

| Name   | Type             | Comment                                                                        | Address                                                                                                                                                                                                 |
|--------|------------------|--------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Google | Hosting Provider | Google Servers host the data. Servers are all within Europe.                   | Google Ireland Limited<br>Gordon House<br>Barrow Street<br>Dublin 4<br>IRELAND<br><a href="https://cloud.google.com/security/gdpr">https://cloud.google.com/security/gdpr</a>                           |
| OVH    | Hosting Provider | OVH Servers are used to host the data. Servers are all within Europe.          | OVH GmbH<br>St. Johanner Str. 41-4<br>66111 Saarbrücken<br>GERMANY<br><a href="https://www.ovh.de/schutz-personenbezogener-daten/faq.xml">https://www.ovh.de/schutz-personenbezogener-daten/faq.xml</a> |
| Websms | SMS Sending      | Used to send customer invites or alerts over SMS.                              | sms.at mobile internet services gmbh<br>Brauquartier 5/Top 13<br>8055 Graz<br>AUSTRIA<br><a href="https://websms.at/de-at/sicherheit/">https://websms.at/de-at/sicherheit/</a>                          |
| Amazon | E-Mail Sending   | Used to send transactional E-mails for alerts or to communicate with the user. | Amazon Web Services EMEA SARL<br>38 avenue John F. Kennedy<br>L-1855<br>LUXEMBOURG<br><a href="https://aws.amazon.com/de/compliance/gdpr-center/">https://aws.amazon.com/de/compliance/gdpr-center/</a> |

|            |                  |                                                                                                                                           |                                                                                                                                                                                                                |
|------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Telematica | SIP Provider     | Used for phone calls if our SIP Server is used.                                                                                           | Telematica Internet Service Provider GmbH<br>Münzgrabenstraße 84b/5<br>8010 Graz<br>AUSTRIA<br><a href="https://www.telematica.at/telematica/datenschutz">https://www.telematica.at/telematica/datenschutz</a> |
| Twilio     | SIP Provider     | Used for phone calls if our SIP Server is used. Two different providers are used to have redundancy.                                      | Twilio Inc<br>Block D, Harcourt Rd, Saint Kevin's,<br>Dublin 2<br>IRELAND<br><a href="https://www.twilio.com/legal/data-protection-addendum">https://www.twilio.com/legal/data-protection-addendum</a>         |
| Hubspot    | Support Tool     | Used for support with end customer.                                                                                                       | HubSpot Germany GmbH<br>Am Postbahnhof 17<br>10243 Berlin<br>GERMANY<br><a href="https://legal.hubspot.com/privacy-policy">https://legal.hubspot.com/privacy-policy</a>                                        |
| Adyen      | Payment Provider | Used for payment processing (online payment and POS payment) of the end customer. Only applies if charged are done with the Arivo system. | Adyen N.V<br>Simon Carmiggeltstraat 6,<br>1011 DJ, Amsterdam<br>NETHERLANDS<br><br><a href="https://www.adyen.com/privacy-policy">https://www.adyen.com/privacy-policy</a>                                     |

|          |                         |                                                                                                       |                                                                                                                                                                                                               |
|----------|-------------------------|-------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Easypark | Parking System          | System for managing parking and other related services.                                               | <p>EasyPark Austria GmbH<br/>Gertrude-Fröhlich-Sandner-Straße 2<br/>1100 Wie<br/>AUSTRIA</p> <p><a href="https://www.easypark.com/en-de/privacy-policy">https://www.easypark.com/en-de/privacy-policy</a></p> |
| Parkster | Parking System          | Pay for parking tickets cashlessly via mobile phone.                                                  | <p>Parkster GmbH<br/>Lyonel-Feininger-Straße 28<br/>80807 München<br/>GERMANY</p> <p><a href="https://www.parkster.com/at/company/privacy/">https://www.parkster.com/at/company/privacy/</a></p>              |
| EFSTA    | Fiscalization           | To securely store cash register data in a tamper-proof manner and transmit it to the tax authorities. | <p>efsta IT Services GmbH<br/>Pachergasse 17 / Top 11<br/>4400 Steyr<br/>AUSTRIA</p> <p><a href="https://www.efsta.eu/">https://www.efsta.eu/</a></p>                                                         |
| ETI      | Debt Collection Service | Used for vehicle registration research.                                                               | <p>ETI experts GmbH<br/>Amsterdamer Straße 133 b<br/>50735 Köln<br/>GERMANY</p> <p><a href="https://www.eti-experts.de/datenschutzerklaerung/">https://www.eti-experts.de/datenschutzerklaerung/</a></p>      |

|                                                 |                               |                                                                                                                                |                                                                                                                                                                                                                                                                           |
|-------------------------------------------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Azure OpenAI (Microsoft Foundry)                | First Level E-Mail Responding | Used for categorizing and first level e-mail communication.                                                                    | <p>Microsoft Ireland Operations Limited<br/>One Microsoft Place<br/>South County Business Park<br/>Dublin D18 P521<br/>Ireland</p> <p><a href="https://www.microsoft.com/de-de/privacy/privacystatement">https://www.microsoft.com/de-de/privacy/privacystatement</a></p> |
| N8N                                             | Workflow Automation Tool      | Used for categorizing and first level e-mail communication.                                                                    | <p>n8n GmbH<br/>Novalisstr. 10<br/>10115, Berlin<br/>GERMANY</p> <p><a href="https://n8n.io/legal/privacy/">https://n8n.io/legal/privacy/</a></p>                                                                                                                         |
| Stripe<br><br>(nur für Verträge vor 01.01.2026) | Payment Provider              | Used for payment processing (only online payment) of the end customer. Only applies if charged are done with the Arivo system. | <p>Stripe Payments Europe, Limited<br/>C/O A &amp; L Goodbody, Ifsc, North Wall Quay Dublin 1.<br/>Dublin 1<br/>IRELAND</p> <p><a href="https://stripe.com/docs/security/stripe">https://stripe.com/docs/security/stripe</a></p>                                          |



## Datenschutzerklärung EasyPark

Letzte Aktualisierung: 6. Februar 2023

### 1 Einleitung

Die EasyPark Gruppe ist in verschiedenen Ländern tätig. In dieser Datenschutzerklärung (die "**Datenschutzerklärung**") bezeichnet "**EasyPark**", "**wir**" und "**uns**" die Easypark GmbH, Luegallee 116, 40545 Düsseldorf, [post@easypark.de](mailto:post@easypark.de), die den EasyPark Park-Service und damit verbundene Dienstleistungen, darunter Abonnements und Pay-per-Use-Dienste, (die "**Dienste**") erbringt. EasyPark fungiert zusammen mit seiner in Schweden ansässigen Muttergesellschaft [EasyPark AB](#) als gemeinsame Verantwortliche für die Verarbeitung personenbezogener Daten, beispielsweise in Bezug auf die Bereitstellung, Entwicklung und Wartung der Dienste, Marketingkommunikation und Kundenservice-Angelegenheiten.

Als Teil der Vereinbarung zwischen EasyPark und EasyPark AB ist EasyPark dafür verantwortlich sicherzustellen, dass Sie die Möglichkeit haben, diese Informationen zur Verarbeitung personenbezogener Daten zu lesen. Bei Fragen in Bezug auf die gemeinsame Verantwortlichkeit oder diese Datenschutzerklärung wenden Sie sich gerne an EasyPark über die in Abschnitt 10 unten aufgeführten Kontaktdaten. Bitte beachten Sie Abschnitt 5.3 unten, um mehr über die Verarbeitung personenbezogener Daten zu erfahren, die innerhalb der EasyPark-Gruppe stattfindet.

In dieser Datenschutzerklärung erläutern wir, welche Kategorien von personenbezogenen Daten EasyPark erhebt, warum EasyPark diese Daten erhebt und wofür EasyPark diese personenbezogenen Daten im Zusammenhang mit den Diensten, der App für Mobilgeräte von EasyPark (die "**App**") oder der Website von EasyPark (die "**Website**") nutzt. Dies tun wir, um Sie in die Lage zu versetzen, Ihre Datenschutz-Rechte auszuüben.

EasyPark verarbeitet personenbezogene Daten im Einklang mit den geltenden Datenschutzgesetzen.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

EasyPark erbringt die Dienste sowohl gegenüber Privatkunden (B2C) als auch gegenüber Geschäftskunden, deren Mitarbeiter die Dienste nutzen (B2B). Diese Datenschutzerklärung gilt für beide Arten von Kunden.

### 2 Quellen personenbezogener Daten

#### 2.1 Von Ihnen erhobene personenbezogene Daten

Die gegebenenfalls verarbeiteten personenbezogenen Daten sind in erster Linie solche Daten, die Sie selbst EasyPark unmittelbar oder mittelbar zur Verfügung stellen. EasyPark erhebt Ihre personenbezogenen Daten beispielsweise, wenn Sie:

- einen Antrag auf Eröffnung eines Accounts bei EasyPark stellen;
- die Dienste, die App und die Website nutzen; und

- wenn Sie EasyPark kontaktieren.

## **2.2 Von Informationsdiensteanbietern erhobene personenbezogene Daten**

Gegebenenfalls erheben wir personenbezogene Daten von Informationsdiensteanbietern, um unsere Kundendaten mit öffentlichen Registern abzugleichen, um sicherzustellen, dass wir über aktuelle und richtige Informationen verfügen, wie beispielsweise das richtige KFZ-Kennzeichen und Fahrzeugmodell.

## **2.3 Von Auskunftgebern erhobene personenbezogene Daten**

Wenn Sie eine Zahlung auf Rechnung beantragen, rufen wir eine Personen-/Bonitätsauskunft von entsprechenden Stellen ab.

## **2.4 Von übernommenen Unternehmen erhobene personenbezogene Daten**

Wenn die EasyPark-Gruppe Unternehmen erwirbt, können personenbezogene Daten im Zusammenhang mit der Übertragungen und Migrationen von Kundendatenbanken der erworbenen Unternehmen zur EasyPark-Gruppe zum Zweck der Integration der erworbenen Unternehmen in die EasyPark-Gruppe verarbeitet werden auf Grundlage unseres berechtigten Interesses neue Unternehmen zu erwerben und in die EasyPark-Gruppe zu integrieren.

## **2.5 Personenbezogene Daten, die von öffentlichen und privaten Betreibern erhoben werden**

Wir können personenbezogene Daten von öffentlichen und privaten Betreibern von Parkplätzen wie Gemeinden, Bahnhöfen, Flughäfen, Krankenhäusern und Universitäten erheben, die uns die Angaben Ihrer Parktransaktionen zur Verfügung stellen, wenn Sie sich für unseren Service entschieden haben, damit wir Ihre Parktransaktionen entsprechend verarbeiten können. Diese Informationen bestehen aus Ihrem Kfz-Kennzeichen, soweit für den Stellplatz erforderlich, dem Stellplatz, der Parkgebühr sowie der Start- und Endzeit Ihres Parkvorgangs.

## **2.6 Von Parkkontrollstellen erhobene personenbezogene Daten**

Wir können personenbezogene Daten von Stellen der Parkkontrolle, wie z.B. Kommunen, privaten Parkraumbetreibern und ihren Vollstreckungspartnern zum Zwecke der Parkvollstreckung gemäß den geltenden Parkvorschriften erheben. Diese Informationen bestehen aus Ihrem Kfz-Kennzeichen, soweit dies für den Parkbereich erforderlich ist, und der Start- und Endzeit Ihres Parkvorgangs.

## **2.7 Personenbezogene Daten, die von Betreibern von Parkeinrichtungen erhoben werden**

Wir können personenbezogene Daten von Betreibern von Parkeinrichtungen (z.B. Parkuhren) und Kennzeichenerkennungssystemen (z.B. in Parkhäusern) erheben, damit Ihr Parkvorgang identifiziert und registriert werden kann. Bitte beachten Sie, dass solche Automatischen Nummernschild-Erkennungsdienste (ANSED) nicht standardmäßig aktiviert sind; diese müssen über unsere App oder über unsere Website eingeschaltet werden.

## **2.8 Personenbezogene Daten, die von Partnern der automatischen Zahlung erhoben werden**

Wir können personenbezogene Daten von Partnern erfassen, die die Möglichkeit der automatischen Zahlung ermöglichen, damit Sie nach einem Parkvorgang automatisch auf der Grundlage von ANPR, RFID (Radio Frequency Identification)-Tag, Bluetooth, UHF (Ultra High Frequency)-Tag oder Fahrzeugsignal bezahlen können. Wir erhalten diese Informationen nur, wenn Sie entweder über unsere App

oder über unsere Website oder vor Ort diese Zahlungsoption aktiviert haben.

## 2.9 Vom öffentlichen und privaten Sektor erhobene personenbezogene Daten

Wir können personenbezogene Daten von unseren Kunden aus dem öffentlichen und privaten Sektor erfassen, die unseren Service nutzen, um ihren Mitarbeitern/Mitarbeiterinnen das Parken zu erleichtern. Wenn Sie als Mitarbeiter/Mitarbeiterin Teil einer solchen Vereinbarung sind, erhalten wir von Ihrem Arbeitgeber Ihren Namen oder Ihre Personalnummer, E-Mail-Adresse, Telefonnummer und das Kfz-Kennzeichen, wonach Sie Ihr Konto mit dem Konto Ihres Arbeitgebers verknüpfen können.

## 2.10 Personenbezogene Daten, die von Flottenmanagementunternehmen erhoben werden

Wir können personenbezogene Daten von Flottenmanagementunternehmen (betrifft ausschließlich Geschäftskonten) erfassen, die uns, Fahrzeugstatusinformationen (z.B. den Zeitstempel der Parktransaktion) zur Verfügung stellen. Diese Informationen können verwendet werden, um Dienste wie die automatische Stoppfunktion bereitzustellen.

## 3 Zwecke und Rechtsgrundlagen der Verarbeitung von personenbezogenen Daten

EasyPark verarbeitet Ihre personenbezogenen Daten zu den folgenden Zwecken und auf Basis der folgenden Rechtsgrundlagen. Die nachstehenden Tabellen enthalten auch Informationen zu den Kategorien der von uns verarbeiteten personenbezogenen Daten sowie die Speicherdauer.

### 3.1 Erbringung der Dienste

EasyPark verarbeitet Ihre personenbezogenen Daten zur Erbringung der Dienste.

| Personenbezogene Daten                                                                                                                 | Rechtsgrundlage für die Verarbeitung                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> , bspw. Name, Kundenidentifikationsnummer, persönliche Identifikationsnummer, Mobilnummer, Kfz-Kennzeichen | <i>Vertrag</i> . Wenn Sie einen Account bei EasyPark eröffnen, wird EasyPark Ihre personenbezogenen Daten verarbeiten, um auf Ihre Anfrage vorvertragliche Maßnahmen vor Abschluss eines Vertrags (d.h. der Allgemeinen Geschäftsbedingungen) durchzuführen.                                                                                                                                                                                                                                        |
| <b>Kontaktdaten</b> , bspw. Adresse, E-Mail, Telefonnummer                                                                             | Wenn Sie unsere Dienste nutzen und Mitteilungen im Zusammenhang mit den Diensten erhalten, wird EasyPark personenbezogene Daten verarbeiten, um unseren Pflichten Ihnen gegenüber nach unserer Allgemeinen Geschäftsbedingungen zu erfüllen. Wenn Sie sich für Automatic CameraPark, d.h. eine automatische Kennzeichenerkennung ( <i>Automatic Number Plate Recognition</i> – ANPR), angemeldet haben, wird Ihr Kfz-Kennzeichen zum Starten und Beenden des Parkvorgangs von einer Kamera erkannt. |
| <b>Parkdaten</b> , bspw. Ankunfts-/Abfahrtszeit und Zonencode zum Parkvorgang                                                          | Diese Verarbeitung personenbezogener Daten ist notwendig, damit EasyPark seine vertraglichen Verpflichtungen Ihnen gegenüber entsprechend den                                                                                                                                                                                                                                                                                                                                                       |
| <b>Transaktionsdaten</b> , bspw. entrichtete Parkgebühr und Dienstgebühren                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Technische Daten</b> , bspw. welches Gerät genutzt wurde sowie die eindeutige Identifikationsnummer eines Mobiltelefons             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Standortdaten</b>, bspw. der Standort, an dem Sie sich laut der Position Ihres Mobiltelefons während eines bestimmten Zeitraums aufhalten, die Ausgangsposition, der gewählte Bestimmungsort und die Route.</p> <p>Wenn Sie der App den Zugriff auf Ortungsdienste gestattet haben, erhebt EasyPark Informationen über den geographischen Standort Ihres Mobiltelefons zur Erbringung der Dienste.</p>                                                                                                                                                                                                                                                                                                                                                                                                      | <p>Allgemeinen Geschäftsbedingungen erfüllen kann.</p> <p>Wenn Sie darüber hinaus unseren Ladeservice für Elektrofahrzeuge wählen, verarbeiten wir personenbezogene Daten zur Erbringung dieses Dienstes. Diese Verarbeitung ist notwendig, damit EasyPark seine vertraglichen Verpflichtungen Ihnen gegenüber entsprechend den Allgemeinen Geschäftsbedingungen erfüllen kann.</p> <p>Wenn Sie die Dienste über Ihren Arbeitgeber nutzen, der ein Geschäftskunde von EasyPark ist, verarbeiten wir Ihre personenbezogenen Daten auf der Grundlage unseres <i>berechtigten Interesses</i> zur Erfüllung unserer Verpflichtungen gegenüber unseren Geschäftskunden entsprechend unserer Vereinbarung mit diesen Kunden. Dazu gehören Mitteilungen im Zusammenhang mit den Diensten, die wir Ihnen ggf. übersenden.</p>                                                                                                                                                                        |
| <p><b>Zahlungsdetails</b>, bspw. Zahlungsweise und relevante Daten<sup>1</sup></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <p>Wenn Sie per Rechnung bezahlen, wird Ihre persönliche Identifikationsnummer verarbeitet, um sicherzustellen, dass Sie sicher identifiziert werden können.</p> <p>Wenn Sie eine Zahlung auf Rechnung beantragen, verarbeiten wir Ihre personenbezogenen Daten auch zur Durchführung einer Bonitätsprüfung auf der Grundlage unseres <i>berechtigten Interesses</i> an der Überprüfung, dass die finanziellen Voraussetzungen für eine Genehmigung dieser Zahlungsweise vorliegen.</p> <p>Die Verarbeitung von Standortdaten basiert – sofern die Verarbeitung nicht für den in Rede stehenden Dienst erforderlich ist – auf Ihrer <i>Einwilligung</i>, die Sie uns durch die Aktivierung der Standortdaten in der App auf Ihrem Mobiltelefon erteilt haben. Sie können Ihre Einwilligung zur Erhebung, Nutzung und Weitergabe dieser Standortdaten durch EasyPark jederzeit widerrufen, indem Sie die Funktion "Zugriff auf Standortdaten erlauben" an Ihrem Mobiltelefon ausschalten.</p> |
| <p><b>Verarbeitungszeitraum:</b> Wir speichern Ihre personenbezogenen Daten nur so lange, wie es für die Zwecke, für die die personenbezogenen Daten erhoben wurden, oder gemäß den gesetzlichen Bestimmungen erforderlich ist.</p> <p>Wenn Sie unsere Pay-per-Use-Dienste länger als 18 Monate nicht nutzen, archivieren wir Ihren Account als inaktiv für die Dauer von 24 Monaten ab Ihrer letzten Pay-per-Use-Transaktion, für den Fall, dass Sie unsere Dienste in der Zukunft erneut verwenden und somit Ihren Account leicht reaktivieren möchten. Danach entfernen oder anonymisieren wir Ihre Account-Daten mit Ausnahme von Informationen, zu deren Speicherung wir gesetzlich verpflichtet sind bzw. zur Wahrung unseres berechtigten Interesses an der Verteidigung gegen bzw. der Geltendmachung</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

<sup>1</sup> EasyPark verwaltet keine Kartendetails. Kartendetails werden durch unsere PCI-zertifizierten Dienstleister bearbeitet.

oder Ausübung von Rechtsansprüche(n) nach Maßgabe dieser Datenschutzerklärung. Danach werden personenbezogene Daten entfernt oder anonymisiert.

Sofern Sie ein Abonnement haben, werden personenbezogene Daten nach Maßgabe dieser Datenschutzerklärung für die Dauer des Abonnements und nach Beendigung des Abonnements, soweit dies gemäß den gesetzlichen Bestimmungen erforderlich ist, gespeichert.

Wenn Sie Ihren Account kündigen möchten, kontaktieren Sie bitte den Kundendienst. Bei einer Kündigung löschen wir unverzüglich Ihre personenbezogenen Informationen, einschließlich der Daten Ihres Parkverlaufs, mit Ausnahme von Informationen, zu deren Speicherung wir gesetzlich verpflichtet sind.

Wenn Sie Geschäftskunde sind, werden Ihre gespeicherten Parkvorgänge zwölf (12) Monate nach dem entsprechenden Parkvorgang gelöscht oder anonymisiert, mit Ausnahme von Informationen, zu deren Speicherung wir gesetzlich verpflichtet sind.

Personenbezogene Daten können in Fällen, in denen eine Speicherung aufgrund gesetzlicher Bestimmungen erforderlich ist oder diese im Zusammenhang mit Rechtsansprüchen, wie in dieser Datenschutzerklärung angegeben, verwendet werden, für eine längere Dauer gespeichert werden.

### 3.2 Werbemitteilungen und Angebote

EasyPark verarbeitet Ihre personenbezogenen Daten im Rahmen der die Dienste betreffenden Kommunikation mit Ihnen und zur Unterbreitung von Angeboten hinsichtlich der Dienste und Produkte von EasyPark. Nach Maßgabe des § 7 Absatz 3 Gesetz gegen den unlauteren Wettbewerb (UWG) können wir unseren bestehenden Kunden auf elektronischem Weg Werbung zu unseren ähnlichen Produkten und Diensten zusenden.

In dem Fall, dass EasyPark eine Zusammenarbeit oder Partnerschaft eingeht, die mit der Versendung von Werbung in Bezug auf eine solche Zusammenarbeit oder Partnerschaft mit Dritten an Sie verbunden wäre, stellen wir sicher, dass wir vorab Ihre Einwilligung zum Erhalt solcher Werbung einholen.

Sie können sich jederzeit von unserer Mailing-Liste abmelden, indem Sie die in der E-Mail enthaltenen Anweisungen zur Abmeldung befolgen. Wenn Sie nicht länger Push-Mitteilungen der App erhalten möchten, können Sie dies direkt in den Einstellungen der App ändern. Sie können SMS-Mitteilungen abbestellen, indem Sie die Anweisungen in den SMS-Mitteilungen befolgen.

EasyPark stellt sicher, dass an Sie gerichtete Direktwerbung mit den geltenden Gesetzen, Bestimmungen, Verhaltensregeln und ethischen Leitlinien im Zusammenhang mit Werbemaßnahmen im Einklang steht.

EasyPark sendet Ihnen Werbemitteilungen nur innerhalb von 18 Monaten ab Ihrem letzten Parkvorgang oder solange Sie ein aktives Abonnement haben, sofern Sie sich nicht bereits zuvor gegen solche Mitteilungen entschieden haben.

Wenn Sie einen Social Media Account haben, kann Ihnen dort Werbung von EasyPark angezeigt werden.

EasyPark kann auf der Website Social-Media-Plugins zur Förderung seiner Kommunikationskanäle verwenden. EasyPark ist mit dem jeweiligen Dritten gemeinsam Verantwortlicher, soweit die Plugins von dem Dritten Inhalte anfordern

und personenbezogene Daten an den Dritten übermitteln. Sie können über die entsprechenden Icons überall auf der Website auf die Social-Media-Dienste zugreifen. Wenn Sie auf diese Webseiten Dritter zugreifen und die Website von EasyPark verlassen, sind die jeweiligen Dritten Verantwortliche für jegliche Verarbeitung personenbezogener Daten auf diesen Webseiten.

| Personenbezogene Daten                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Rechtsgrundlage für die Verarbeitung                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> , bspw. Name, Kundenidentifikationsnummer, Mobilnummer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <i>Berechtigtes Interesse.</i> Die Verarbeitung von personenbezogenen Daten ist für die Wahrung des berechtigten Interesses von EasyPark an der Kommunikation mit Ihnen über die Dienste und die Unterbreitung von Angeboten erforderlich.                                     |
| <b>Kontaktdaten</b> , bspw. Adresse, E-Mail, Telefonnummer                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Die Verarbeitung bestimmter personenbezogener Daten erfolgt über Cookies im Einklang mit unserer Cookie-Richtlinie zur Darstellung relevanter Werbung. Diese Verarbeitung erfolgt mit Ihrer <i>Einwilligung</i> gemäß der Cookie-Richtlinie, die auf der Website abrufbar ist. |
| <b>Technische Daten</b> , bspw. welches Gerät genutzt wurde sowie Webbrowser, die eindeutige Identifikations-nummer eines Mobiltelefons, IP-Adresse                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                                |
| <p><b>Verarbeitungszeitraum:</b> Personenbezogene Daten werden während der Dauer der Kundenbeziehung verarbeitet, bspw. während der Dauer Ihres aktiven Abonnements oder Ihrer aktiven Nutzung unsere Pay-per-Use-Dienste.</p> <p>Wenn Sie unsere Pay-per-Use-Dienste länger als 18 Monate nicht genutzt haben oder Ihr Abonnement gekündigt haben, wird EasyPark Ihnen nicht länger aktiv Werbemitteilungen oder Angebote zusenden, sofern Sie sich nicht bereits zuvor gegen solche Mitteilungen entschieden haben, sondern Ihren Account archivieren und, falls erforderlich, Mitteilungen im Zusammenhang mit den Diensten übersenden.</p> <p>Die Speicherdauer für die jeweiligen Informationen im Zusammenhang mit Cookies ist in unserer Cookie-Richtlinie angegeben.</p> |                                                                                                                                                                                                                                                                                |

### 3.3 Durchführung von Umfragen

EasyPark verarbeitet Ihre personenbezogenen Daten für die Durchführung von Umfragen über EasyPark, die App und die Dienste, beispielsweise in Form einer Bitte um Feedback und Bewertungen über die App, per SMS oder per E-Mail. Bitte beachten Sie, dass Sie keine personenbezogenen Daten teilen sollten, wenn Sie Ihr Feedback im Freitextfeld eintragen. Sollte dies unvermeidbar sein, geben Sie bitte nur personenbezogene Daten an, die für das Feedback, das Sie abgeben möchten, erforderlich sind.

| Personenbezogene Daten                                                | Rechtsgrundlage für die Verarbeitung                                                                                                                                                    |
|-----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> , bspw. Name, Kundenidentifikationsnummer | <i>Berechtigtes Interesse.</i> Die Verarbeitung von personenbezogenen Daten ist für die Wahrung des berechtigten Interesses von EasyPark an der Durchführung von Umfragen erforderlich. |

|                                                                                                                                                                                                                                                                                                                  |  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <b>Kontakt</b> daten, bspw. Adresse, E-Mail, Telefonnummer                                                                                                                                                                                                                                                       |  |
| <b>Kommunikation</b> , bspw. Daten hinsichtlich Ihrer Fragen und unserer Antworten.                                                                                                                                                                                                                              |  |
| <b>Verarbeitungszeitraum:</b> Die personenbezogenen Daten werden für diesen Zweck für einen Zeitraum von drei (3) Monaten gespeichert, beginnend mit dem Datum des Beginns der Umfrage. Allgemeine Berichte, die keine personenbezogenen Daten enthalten, können für einen längeren Zeitraum gespeichert werden. |  |

### 3.4 Nachbereitung und Bewertung

EasyPark verarbeitet Ihre personenbezogenen Daten im Rahmen der Erstellung verschiedener Berichte und Statistiken, um die Dienste und unsere Interaktionen mit Ihnen nachzubereiten und zu bewerten.

| Personenbezogene Daten                                                                                                                                                                                                                                                                                                                                             | Rechtsgrundlage für die Verarbeitung                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> ,<br>bspw. KFZ-Kennzeichen                                                                                                                                                                                                                                                                                                             | <i>Berechtigtes Interesse.</i> Die Verarbeitung von personenbezogenen Daten ist für die Wahrung des berechtigten Interesses von EasyPark an der Nachbereitung und Bewertung unserer Dienste, der Website und der App sowie von Interaktionen mit Ihnen erforderlich. |
| <b>Kontakt</b> daten, bspw.<br>Adresse, E-Mail,<br>Telefonnummer                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                      |
| <b>Park</b> daten, bspw.<br>Ankunfts-/Abfahrtszeit und<br>Zonencode zum<br>Parkvorgang                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                      |
| <b>Technische Daten</b> , bspw.<br>welches Gerät genutzt wurde<br>sowie Webbrowser, die<br>eindeutige<br>Identifikationsnummer eines<br>Mobiltelefons                                                                                                                                                                                                              |                                                                                                                                                                                                                                                                      |
| <b>Nutzung</b> , bspw. wie Sie die<br>App verwenden oder auf<br>unserer Website navigieren<br>(einschließlich Log-in-<br>Modus)                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                      |
| <b>Verarbeitungszeitraum:</b> Personenbezogene Daten werden für diesen Zweck so lange wie erforderlich zur Nachbereitung und Bewertung beispielsweise durch Berichte und zur Erstellung von Statistiken auf aggregierter Ebene gespeichert. Diese Statistiken enthalten keine personenbezogenen Daten und werden generell für einen längeren Zeitraum gespeichert. |                                                                                                                                                                                                                                                                      |

### 3.5 Bearbeitung von Anfragen und Kundendienstangelegenheiten

EasyPark verarbeitet personenbezogene Daten zur Bearbeitung Ihrer Anfragen über verschiedene Kanäle, beispielsweise wenn Sie mit unserem Kundendienst Kontakt aufnehmen.

*Privatkunden*

| Personenbezogene Daten                                                                                                                                                                                                                                                                                               | Rechtsgrundlage für die Verarbeitung                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> , bspw. Name, Kundenidentifikationsnummer, Mobilnummer, KFZ-Kennzeichen                                                                                                                                                                                                                  | <i>Berechtigtes Interesse.</i> Die Verarbeitung von personenbezogenen Daten ist für die Wahrung des berechtigten Interesses von EasyPark an der Bearbeitung Ihrer Anfragen und zur Erbringung des Kundendienstes erforderlich. |
| <b>Kontaktdaten</b> , bspw. Adresse, E-Mail, Telefonnummer                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                |
| <b>Parkdaten</b> , bspw. Ankunfts-/Abfahrtszeit und Zonencode zum Parkvorgang                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                |
| <b>Technische Daten</b> , bspw. welches Gerät genutzt wurde sowie Webbrowser und die eindeutige Identifikationsnummer eines Mobiltelefons                                                                                                                                                                            |                                                                                                                                                                                                                                |
| <b>Transaktionsdaten</b> , bspw. entrichtete Parkgebühr und Dienstgebühren                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                |
| <b>Finanzinformationen</b> , bspw. Kontonummer                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                |
| <b>Kommunikation</b> , bspw. Daten hinsichtlich Ihrer Fragen und unserer Antworten.                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                |
| <b>Verarbeitungszeitraum:</b> Die personenbezogenen Daten werden für diesen Zweck für einen Zeitraum von sechs (6) Monaten gespeichert, beginnend mit dem Datum der Kommunikation. Personenbezogene Daten in unserem Kundendienstmanagementsystem werden danach anonymisiert und E-Mail-Kommunikation wird gelöscht. |                                                                                                                                                                                                                                |
| Personenbezogene Daten können in Fällen, in denen eine Speicherung aufgrund gesetzlicher Bestimmungen erforderlich ist oder diese im Zusammenhang mit Rechtsansprüchen, wie in dieser Datenschutzerklärung angegeben, verwendet werden, für eine längere Dauer gespeichert werden.                                   |                                                                                                                                                                                                                                |

*Geschäftskunden*

| Personenbezogene Daten                                                                                                                                                                                                            | Rechtsgrundlage für die Verarbeitung                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> , bspw. Name, Kundenidentifikationsnummer                                                                                                                                                             | <i>Berechtigtes Interesse.</i> Die Verarbeitung von personenbezogenen Daten ist für die Wahrung des berechtigten Interesses von EasyPark an der Bearbeitung Ihrer Anfragen erforderlich. |
| <b>Kontaktdaten</b> , bspw. Adresse, E-Mail, Telefonnummer                                                                                                                                                                        |                                                                                                                                                                                          |
| <b>Kommunikation</b> , bspw. Daten hinsichtlich Ihrer Fragen und unserer Antworten                                                                                                                                                |                                                                                                                                                                                          |
| <b>Verarbeitungszeitraum:</b> Die personenbezogenen Daten werden für diesen Zweck für einen Zeitraum von sechs (6) Monaten gespeichert, beginnend mit dem Datum der Kommunikation. E-Mail-Kommunikation wird danach anonymisiert. |                                                                                                                                                                                          |



Personenbezogene Daten können in Fällen, in denen eine Speicherung aufgrund gesetzlicher Bestimmungen erforderlich ist oder diese im Zusammenhang mit Rechtsansprüchen, wie in dieser Datenschutzerklärung angegeben, verwendet werden, für eine längere Dauer gespeichert werden.

### 3.6 Aufzeichnung von Telefongesprächen

EasyPark verarbeitet personenbezogene Daten im Zusammenhang mit der Aufzeichnung von Telefongesprächen mit dem Kundendienst zum Zweck der Sicherung der Qualität, zu Schulungszwecken und zu Ihrer und unserer Sicherheit, wenn Sie den Kundendienst telefonisch kontaktieren.

| Personenbezogene Daten                                                                                                                                                           | Rechtsgrundlage für die Verarbeitung                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> , bspw. Name, Kundenidentifikationsnummer, Mobilnummer, KFZ-Kennzeichen                                                                              | <i>Einwilligung.</i> Die Telefongespräche werden ausschließlich mit Ihrer vorherigen Einwilligung aufgezeichnet und zu Schulungszwecken oder zum Zweck der Sicherung der Qualität und aus Sicherheitsgründen weiter verarbeitet. |
| <b>Kontaktdaten</b> , bspw. Adresse, E-Mail, Telefonnummer                                                                                                                       |                                                                                                                                                                                                                                  |
| <b>Parkdaten</b> , bspw. Ankunfts-/Abfahrtszeit und Zonencode zum Parkvorgang                                                                                                    |                                                                                                                                                                                                                                  |
| <b>Technische Daten</b> , bspw. welches Gerät genutzt wurde sowie die eindeutige Identifikationsnummer eines Mobiltelefons                                                       |                                                                                                                                                                                                                                  |
| <b>Transaktionsdaten</b> , bspw. entrichtete Parkgebühr und Dienstgebühren                                                                                                       |                                                                                                                                                                                                                                  |
| <b>Kommunikation</b> , bspw. Daten hinsichtlich Ihrer Fragen und unserer Antworten.                                                                                              |                                                                                                                                                                                                                                  |
| <b>Verarbeitungszeitraum:</b> Die personenbezogenen Daten werden für diesen Zweck für einen Zeitraum von drei (3) Monaten gespeichert, beginnend mit dem Datum der Aufzeichnung. |                                                                                                                                                                                                                                  |

### 3.7 Erfüllung rechtlicher Verpflichtungen

EasyPark verarbeitet personenbezogene Daten zur Erfüllung rechtlicher Verpflichtungen, denen EasyPark unterliegt, beispielsweise Rechnungslegungspflichten.

| Personenbezogene Daten                                                                              | Rechtsgrundlage für die Verarbeitung                                                                                                                                                                     |
|-----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> , bspw. Name, Kundenidentifikationsnummer, Mobilnummer, KFZ-Kennzeichen | <i>Rechtliche Verpflichtung.</i> Die Verarbeitung von personenbezogenen Daten ist erforderlich, damit EasyPark seine rechtlichen Verpflichtungen gemäß den geltenden Gesetzen oder anderen Bestimmungen, |

|                                                                                                                                                               |                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Kontaktdaten</b> , bspw. Adresse, E-Mail, Telefonnummer                                                                                                    | beispielsweise aus dem Handelsgesetzbuch (HGB) oder der Abgabenordnung (AO), erfüllen kann. |
| <b>Parkdaten</b> , bspw. Ankunfts-/Abfahrtszeit und Zonencode zum Parkvorgang                                                                                 |                                                                                             |
| <b>Technische Daten</b> , bspw. welches Gerät genutzt wurde sowie die eindeutige Identifikationsnummer eines Mobiltelefons                                    |                                                                                             |
| <b>Transaktionsdaten</b> , bspw. entrichtete Parkgebühr und Dienstgebühren                                                                                    |                                                                                             |
| <b>Kommunikation</b> , bspw. Daten hinsichtlich Ihrer Fragen und unserer Antworten.                                                                           |                                                                                             |
| <b>Verarbeitungszeitraum:</b> Die personenbezogenen Daten werden für den zur Erfüllung aller rechtlichen Verpflichtungen erforderlichen Zeitraum gespeichert. |                                                                                             |

### 3.8 Geltendmachung und Ausübung von sowie Verteidigung gegen Rechtsansprüche(n)

EasyPark verarbeitet personenbezogene Daten zur Geltendmachung und Ausübung von bzw. zur Verteidigung gegen Rechtsansprüche(n), beispielsweise im Zusammenhang mit einer außergerichtlichen Streitigkeit oder einem gerichtlichen Verfahren.

| Personenbezogene Daten                                                                                                                 | Rechtsgrundlage für die Verarbeitung                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> , bspw. Name, Kundenidentifikationsnummer, persönliche Identifikationsnummer, Mobilnummer, KFZ-Kennzeichen | <p><i>Berechtigtes Interesse.</i> Die Verarbeitung von personenbezogenen Daten ist für die Wahrung des berechtigten Interesses von EasyPark an der Geltendmachung und Ausübung von bzw. der Verteidigung gegen Rechtsansprüche(n) erforderlich.</p> <p>Die persönliche Identifikationsnummer wird verarbeitet, um sicherzustellen, dass Sie sicher identifiziert werden können.</p> |
| <b>Kontaktdaten</b> , bspw. Adresse, E-Mail, Telefonnummer                                                                             |                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Parkdaten</b> , bspw. Ankunfts-/Abfahrtszeit und Zonencode zum Parkvorgang                                                          |                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Technische Daten</b> , bspw. welches Gerät genutzt wurde sowie die eindeutige Identifikationsnummer eines Mobiltelefons             |                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Transaktionsdaten</b> , bspw. entrichtete Parkgebühr und Dienstgebühren                                                             |                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Kommunikation</b> , bspw. Daten hinsichtlich Ihrer Fragen und unserer Antworten.                                                    |                                                                                                                                                                                                                                                                                                                                                                                     |

**Verarbeitungszeitraum:** Die personenbezogenen Daten werden für diesen Zweck zur Wahrung des berechtigten Interesses von EasyPark an der Geltendmachung und Ausübung von bzw. der Verteidigung gegen Rechtsansprüche(n) während der Dauer unserer Vertragsbeziehung und danach für einen Zeitraum von 36 Monaten.

### 3.9 Wartung, Schutz und Entwicklung der Dienste

EasyPark verarbeitet personenbezogene Daten zum Zweck der Wartung, des Schutzes und der Entwicklung der Dienste, der App und der Website, beispielsweise zur Dokumentation, Entwicklung, Prüfung und Verbesserung unserer Dienste.

| Personenbezogene Daten                                                                                                                                                                                                                                                                                                                                                                         | Rechtsgrundlage für die Verarbeitung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> , bspw. Name, Kundenidentifikationsnummer, persönliche Identifikationsnummer, Mobilnummer, KFZ-Kennzeichen.                                                                                                                                                                                                                                                        | <i>Berechtigtes Interesse.</i> Die Verarbeitung von personenbezogenen Daten ist für die Wahrung des berechtigten Interesses von EasyPark an der Wartung, dem Schutz und der Entwicklung der Dienste und der App erforderlich.<br><br>Die persönliche Identifikationsnummer wird verarbeitet, um sicherzustellen, dass Sie sicher identifiziert werden können.<br><br>Die Verarbeitung bestimmter personenbezogener Daten über Cookies im Einklang mit unserer auf der Website abrufbaren Cookie-Richtlinie erfolgt zum Zweck der Sicherstellung der Leistung und Funktionalität der Website und zur Erkennung von Fehlern. Die Verarbeitung der personenbezogenen Daten erfolgt auf der Grundlage unseres <i>berechtigten Interesses</i> an der Sicherstellung der Funktionalität und Leistung der Website durch die Verarbeitung von personenbezogenen Daten, wie beispielsweise technischen Daten. |
| <b>Kontaktdaten</b> , bspw. Adresse, E-Mail, Telefonnummer                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Parkdaten</b> , bspw. Ankunfts-/Abfahrtszeit und Zonencode zum Parkvorgang                                                                                                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Transaktionsdaten</b> , bspw. entrichtete Parkgebühr und Dienstgebühren                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Technische Daten</b> , bspw. welches Gerät genutzt wurde sowie Webbrowser, die eindeutige Identifikationsnummer eines Mobiltelefons, IP-Adresse                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Standortdaten</b> , bspw. der Standort, an dem Sie sich laut der Position Ihres Mobiltelefons während eines bestimmten Zeitraums aufhalten, die Ausgangsposition, der gewählte Bestimmungsort und die Route                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Kommunikation</b> , bspw. Daten hinsichtlich Ihrer Fragen und unserer Antworten.                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Verarbeitungszeitraum:</b> Die personenbezogenen Daten werden zu dem Zweck der Wartung und des Schutzes der Dienstleistungen jeweils für die Dauer der Privatkundenbeziehung bzw. Geschäftskundenbeziehung gespeichert. Für die Entwicklung der Dienste werden personenbezogene Daten lediglich verwendet, um sie anonymisiert zu Testzwecken in der Testumgebung von EasyPark einzusetzen. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

## 4 Sicherheit

EasyPark nimmt die Sicherheit Ihrer personenbezogenen Daten sehr ernst. EasyPark setzt angemessene technische und organisatorische Maßnahmen um, um Ihre

personenbezogenen Daten vor unbefugtem Zugriff, Änderung oder Zerstörung zu schützen. Der Zugriff auf die Informationen ist in verschiedener Hinsicht begrenzt (bspw. durch Benutzerberechtigungen und Passwörter, die abgefragt werden und nur Mitarbeitern zugewiesen werden, die Zugriff auf solche Informationen benötigen, um ihre Arbeitsaufgaben ausüben zu können). Andere Sicherheitsmaßnahmen umfassen Verschlüsselung, Firewalls und physische Begrenzungen und Einschränkungen beim Zugang zu Gebäuden und Zugriff auf Dateien.

## 5 Empfänger personenbezogener Daten

EasyPark teilt erhobene personenbezogene Daten mit den folgenden Empfängern zu den nachstehenden Zwecken. Der Empfänger ist der Verantwortliche für die eigene Verarbeitung der personenbezogenen Daten, die wir mit ihm teilen, sofern dies nicht nachstehend anderweitig geregelt ist.

### 5.1 Parkplatzbetreiber

Wir teilen Daten mit Parkplatzbetreibern, um die Dienste zu erbringen und die Parkplatzbetreiber in die Lage zu versetzen, die Kontrolle über Parkvorgänge auf ihrem Gelände auszuüben und diese zu überprüfen. Der Parkplatzbetreiber ist berechtigt, anonymisierte Standortdaten für statistische Zwecke zu verwenden.

*Durchführungskontrolle und Überwachung von Parkvorgängen*

| Personenbezogene Daten                                                                                                                                                                             | Rechtsgrundlage für die Verarbeitung                                                                                                                                                                                                                                                                                                            |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> , bspw. KFZ-Kennzeichen                                                                                                                                                | <i>Berechtigtes Interesse.</i> Die Verarbeitung von personenbezogenen Daten ist für die Wahrung des berechtigten Interesses von EasyPark an der Einhaltung des Vertrags mit den entsprechenden Parkplatzbetreibern und dem Interesse der Parkplatzbetreiber an der Überprüfung und Überwachung der Parkvorgänge auf ihrem Gelände erforderlich. |
| <b>Parkdaten</b> , bspw. Ankunfts-/Abfahrtszeit und Zonencode zum Parkvorgang                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                 |
| <b>Standortdaten</b> , in Fällen, in denen eine Kenntnis des Standorts des Fahrzeugs erforderlich ist, um den Parkplatz zu prüfen, werden Standortdaten mit dem Betreiber der Parkdienste geteilt. |                                                                                                                                                                                                                                                                                                                                                 |

*Erbringung der Dienste*

Wenn Sie in einem Parkhaus parken, wird Ihr KFZ-Kennzeichen oder die eindeutige Identifikationsnummer der RFID-Karte mit uns und dem Parkplatzbetreiber geteilt, damit der Parkvorgang bei EasyPark beginnen bzw. enden kann.

| Personenbezogene Daten                                                                             | Rechtsgrundlage für die Verarbeitung                                                                                                                                             |
|----------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> , KFZ-Kennzeichen und eindeutige Identifikationsnummer von RFID-Karten | <i>Vertrag.</i> Die Verarbeitung ist erforderlich, damit EasyPark seine vertraglichen Pflichten Ihnen gegenüber entsprechend den Allgemeinen Geschäftsbedingungen erfüllen kann. |
| <b>Parkdaten</b> , bspw. Ankunfts-/Abfahrtszeit und Zonencode zum Parkvorgang                      |                                                                                                                                                                                  |

## 5.2 Zahlungsempfänger und Zahlungsdienstleister

Werden Zahlungen per Rechnung geleistet, werden personenbezogene Daten mit Zahlungsdienstleistern, um unsere Verpflichtungen Ihnen gegenüber gemäß den Allgemeinen Geschäftsbedingungen der Dienste bei Zahlung auf Rechnung zu erfüllen und in einigen Fällen mit Inkassounternehmen zur Erfüllung Ihrer Zahlungspflichten uns gegenüber.

Findet die Zahlung über ein Leasingunternehmen statt, werden personenbezogene Daten und Informationen über Ihre Parkvorgänge mit dem Leasingunternehmen geteilt, um die mit Ihrem über dieses Unternehmen geleasten Fahrzeug in Zusammenhang stehenden Zahlungen zu ermöglichen.

| Personenbezogene Daten                                                                                                                 | Rechtsgrundlage für die Verarbeitung                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> , bspw. Name, Kundenidentifikationsnummer, persönliche Identifikationsnummer, Mobilnummer, KFZ-Kennzeichen | <i>Vertrag.</i> Die Verarbeitung ist erforderlich, damit EasyPark seine vertraglichen Pflichten Ihnen gegenüber entsprechend der Allgemeinen Geschäftsbedingungen erfüllen kann.<br><br>Die persönliche Identifikationsnummer wird verarbeitet, um sicherzustellen, dass Sie sicher identifiziert werden können. |
| <b>Kontaktdaten</b> , bspw. Adresse, E-Mail, Telefonnummer                                                                             |                                                                                                                                                                                                                                                                                                                  |
| <b>Parkdaten</b> , bspw. Ankunfts-/Abfahrtszeit und Zonencode zum Parkvorgang                                                          |                                                                                                                                                                                                                                                                                                                  |
| <b>Transaktionsdaten</b> , bspw. entrichtete Parkgebühr und Dienstgebühren                                                             |                                                                                                                                                                                                                                                                                                                  |

Werden die Zahlungen beispielsweise über eine Zahlkarte oder digitale Zahlungsmethoden (bspw. ApplePay und MobilePay) geleistet, teilen wir nur die Rechnungsnummer und den Rechnungsbetrag für den Abschluss der Zahlung mit.

| Personenbezogene Daten                        | Rechtsgrundlage für die Verarbeitung                                                                                                                                             |
|-----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Identifikationsdaten</b> , Rechnungsnummer | <i>Vertrag.</i> Die Verarbeitung ist erforderlich, damit EasyPark seine vertraglichen Pflichten Ihnen gegenüber entsprechend den Allgemeinen Geschäftsbedingungen erfüllen kann. |

## 5.3 EasyPark-Konzerngesellschaften

Die Technikplattform von EasyPark wird durch Konzerngesellschaften in Schweden bereitgestellt, die personenbezogene Daten verarbeiten, damit EasyPark Ihnen gegenüber die Dienste erbringen kann.

Alle Konzerngesellschaften haben eine interne Datenschutzvereinbarung unterzeichnet, deren Zweck darin besteht, Ihre personenbezogenen Daten zu schützen, wenn sie innerhalb der EasyPark Gruppe ausgetauscht werden.

## 5.4 Dienstleister

Zur Erfüllung des Zwecks der Verarbeitung Ihrer personenbezogenen Daten kann EasyPark personenbezogene Daten mit Dienstleistern teilen. Diese Dienstleister erbringen unter anderem die folgenden Dienstleistungen für EasyPark: Informationsdienste, Telefondienste (PSMS), Support- und IT-Dienste, wie Marketing, Support, Betrieb, Verbesserung, Entwicklung und Dienste für die Bearbeitung von Mailings und die Herstellung von Karten. Diesen Dienstleistern ist die Verarbeitung Ihrer personenbezogenen Daten nur gemäß ausdrücklichen Weisungen durch EasyPark gestattet und sie können diese nicht für eigene Zwecke nutzen. Weiterhin sind sie dazu verpflichtet, Ihre Daten gemäß geltenden Gesetzen und Vereinbarungen zu schützen.

## 5.5 Andere Empfänger

Über die voranstehend genannten Empfänger hinaus kann EasyPark, sofern erforderlich, Ihre personenbezogenen Daten mit den folgenden Empfängern teilen:

| Empfänger                                          | Zweck                                                                                                                                                                                                                                                                                   | Rechtsgrundlage für die Weitergabe                                                                                                                                                                                                                                                                       |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Behörden</b>                                    | Wir teilen Ihre personenbezogenen Daten mit Behörden zur Erfüllung rechtlicher Verpflichtungen, zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder um mit Behörden zu kooperieren.                                                                                | Die Verarbeitung ist für die Erfüllung rechtlicher Verpflichtungen oder zur Erfüllung der berechtigten Interessen von EasyPark erforderlich.<br><br>Die berechtigten Interessen sind insbesondere die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder die Kooperation mit Behörden. |
| <b>Gerichte, externe Berater und Gegenparteien</b> | Im Fall von Streitigkeiten übermitteln wir gegebenenfalls Daten an andere Parteien zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.                                                                                                                                 | Die Verarbeitung ist für die Wahrung unseres berechtigten Interesses an der Durchsetzung und Ausübung von Rechtsansprüchen und der Verteidigung gegen Rechtsansprüche erforderlich.                                                                                                                      |
| <b>Vollzugsbehörden, bspw. die Polizei</b>         | Gegebenenfalls teilen wir personenbezogene Daten mit den Vollzugsbehörden, bspw. der Polizei, wenn wir gesetzlich dazu verpflichtet sind oder um zu einer laufenden strafrechtlichen Untersuchung beizutragen oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. | Die Verarbeitung ist für die Erfüllung rechtlicher Verpflichtungen <i>oder</i> zur Wahrung unseres berechtigten Interesses an einem Beitrag zu einer laufenden strafrechtlichen Untersuchung auf Verlangen oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich.        |

|                                                                             |                                                                                                                                                                                    |                                                                                                                                          |
|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Potentielle Käufer und Verkäufer sowie jeweils deren externe Berater</b> | Gegebenenfalls teilen wir Informationen mit potentiellen Käufern und Verkäufern, sollten wir unser Geschäft insgesamt oder teilweise übertragen oder wenn eine Fusion stattfindet. | Die Verarbeitung ist für die Wahrung unseres berechtigten Interesses an der Durchführung einer Übernahme oder einer Fusion erforderlich. |
|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|

## 6 **Wo werden meine personenbezogenen Daten gespeichert?**

Soweit EasyPark Ihre personenbezogenen Daten verarbeitet, werden diese Daten auf Servern in der Europäischen Union ("EU") gespeichert. In Fällen, in den sich unsere Dienstleister außerhalb der EU oder des Europäischen Wirtschaftsraums ("EWR") befinden, können wir personenbezogene Daten an Dritte übermitteln, die außerhalb der EU / des EWR ansässig sind oder personenbezogene Daten anderweitig außerhalb der EU / des EWR verarbeiten. In solchen Fällen werden wir sicherstellen, dass diese Übermittlungen den anwendbaren datenschutzrechtlichen Bestimmungen entsprechen, unter anderem durch Einrichtung angemessener Schutzmechanismen wie beispielsweise die Standardvertragsklauseln der Europäischen Kommission und ergänzende Maßnahmen, je nach Erforderlichkeit.

Sie können Informationen über Datenübermittlungen außerhalb der EU / des EWR sowie eine Kopie der Sicherheitsmaßnahmen, die EasyPark ergreift, um Ihre personenbezogenen Daten zu schützen, anfordern. Wenden Sie sich hierzu bitte an die am Ende dieser Datenschutzerklärung aufgeführten Kontaktdaten.

## 7 **Cookies**

EasyPark verwendet für die Optimierung der Dienste, zur Durchführung von statistischen Auswertungen, für Analysen und zu Marketing-Zwecken Cookies. Ein Cookie ist eine Textdatei, die beispielsweise auf Ihrem Computer oder Mobilgerät gespeichert wird, um so die Identifizierung Ihres Computers oder Mobiltelefons zu ermöglichen. Cookies helfen EasyPark dabei, die App und die Website beispielsweise auf Grundlage Ihrer Nutzeranfragen als Benutzer der Dienste und der Website von EasyPark anzupassen. Weiterführende Informationen finden Sie in unserer auf der Website abrufbaren Cookie-Richtlinie.

## 8 **Ihre Rechte**

Gemäß den geltenden Datenschutzgesetzen haben Sie eine Reihe von Rechten im Zusammenhang mit der Verarbeitung Ihrer personenbezogenen Daten. Um Ihre Rechte auszuüben, kontaktieren Sie bitte den Kundendienst von EasyPark unter den am Ende dieser Datenschutzerklärung aufgeführten Kontaktdaten.

### 8.1 **Auskunftsrecht**

Sie haben das Recht, eine Bestätigung von uns zu erhalten, ob wir personenbezogenen Daten verarbeiten, die Sie betreffen, und können eine Kopie Auskunft Ihre von uns verarbeiteten personenbezogenen Daten verlangen. Auf einige Ihrer von uns gespeicherten Daten können Sie zugreifen, indem Sie sich in Ihrem persönlichen Account in der App oder auf der Website anmelden. Eine Kopie Ihrer Daten können Sie über den Kundendienst anfordern.

## 8.2 **Recht auf Berichtigung**

Wenn Ihre von EasyPark verarbeiteten personenbezogene Daten unrichtig oder unvollständig sind, sind Sie berechtigt, von EasyPark Berichtigung der personenbezogenen Daten zu verlangen. Einige personenbezogene Daten können Sie selbst berichtigen, indem Sie sich in Ihrem persönlichen Account in der App oder auf der Website anmelden.

## 8.3 **Recht auf Widerspruch gegen Direktwerbung**

**Sie sind zu jeder Zeit ohne Weiteres berechtigt, der Verarbeitung Ihrer personenbezogenen Daten durch EasyPark zum Zweck der Direktwerbung zu widersprechen und sich von zukünftigen Werbemitteilungen abzumelden.**

Kontaktieren Sie hierzu bitte unseren Kundendienst unter den am Ende dieser Datenschutzerklärung angegebenen Kontaktdaten.

## 8.4 **Recht auf Widerspruch gegen die Verarbeitung auf Grundlage unseres berechtigten Interesses**

Sie sind berechtigt, der Verarbeitung auf Grundlage unseres berechtigten Interesses jederzeit aus Gründen, die sich aus Ihrer besonderen Situation ergeben, zu widersprechen. Gegebenenfalls setzen wir die Verarbeitung Ihrer personenbezogenen Daten fort, auch wenn Sie der Verarbeitung widersprochen haben, sofern zwingende schutzwürdige Gründe für die Verarbeitung bestehen, die Ihre Rechte auf Schutz Ihrer Daten überwiegen.

## 8.5 **Recht auf Löschung ("Recht auf Vergessenwerden")**

Unter bestimmten Umständen haben Sie das Recht auf die Löschung Ihrer personenbezogenen Daten, wenn Sie beispielsweise der Verarbeitung widersprochen haben und keine vorrangigen berechtigten Gründe für EasyPark für die weitere Verarbeitung der Daten vorliegen. Dies gilt nicht, wenn wir beispielsweise laut Gesetz zur Speicherung der Daten verpflichtet sind.

## 8.6 **Recht auf Einschränkung der Verarbeitung**

Unter bestimmten Umständen haben Sie das Recht, eine Einschränkung der Verarbeitung Ihrer personenbezogenen Daten zu verlangen. Wenn Sie eine solche Einschränkung verlangen, ist EasyPark in dem Zeitraum, in dem die Verarbeitung Ihrer personenbezogenen Daten eingeschränkt ist, gegebenenfalls nicht in der Lage, seine Verpflichtungen Ihnen gegenüber zu erfüllen.

## 8.7 **Recht auf Datenübertragbarkeit**

Außerdem haben Sie das Recht auf Erhalt einer Kopie der Sie betreffenden personenbezogenen Daten in einem strukturierten Format und, soweit dies technisch machbar ist, auf Übertragung dieser Daten an einen Dritten (Datenübertragbarkeit). Das Recht auf Datenübertragbarkeit umfasst im Vergleich zum Recht auf Auskunft nur Daten, die Sie selbst zur Verfügung gestellt haben und die wir auf Basis bestimmter Rechtsgrundlagen verarbeiten, beispielsweise des Vertrags mit Ihnen (den Allgemeinen Geschäftsbedingungen).

## 8.8 **Widerruf der Einwilligung**

Beruhet die Verarbeitung auf Ihrer Einwilligung, haben Sie das Recht, Ihre Einwilligung jederzeit zu widerrufen. Kontaktieren Sie hierzu bitte unseren Kundendienst unter den am Ende dieser Datenschutzerklärung angegebenen



Kontaktdaten. Bitte beachten Sie, dass die Rechtmäßigkeit der vor dem Widerruf erfolgten Verarbeitung durch den Widerruf der Einwilligung nicht berührt wird.

## 8.9 Beschwerden

Sollten Sie Beschwerden über die Verarbeitung personenbezogener Daten durch EasyPark haben, können Sie sich selbstverständlich gerne an uns wenden, damit wir diesen nachgehen können.

Darüber hinaus haben Sie auch ein Recht auf Beschwerde bei einer Aufsichtsbehörde. Die für EasyPark zuständige Aufsichtsbehörde in Deutschland ist die Landesbeauftragte für den Datenschutz Niedersachsen. Die Kontaktdaten der Aufsichtsbehörde finden Sie im Internet unter [https://lfd.niedersachsen.de/startseite/wir\\_uber\\_uns/die\\_landesbeauftragte/die-landesbeauftragte-fuer-den-datenschutz-niedersachsen-130186.html](https://lfd.niedersachsen.de/startseite/wir_uber_uns/die_landesbeauftragte/die-landesbeauftragte-fuer-den-datenschutz-niedersachsen-130186.html).

Die Kontaktdaten der Aufsichtsbehörde lauten:

Die Landesbeauftragte für den Datenschutz Niedersachsen  
Prinzenstraße 5  
30159 Hannover  
Telefon 0511-120 4500

## 9 Änderungen der Datenschutzerklärung bei EasyPark

EasyPark kann die Datenschutzerklärung von Zeit zu Zeit ändern. Im Fall von Änderungen der Datenschutzerklärung bei EasyPark, die zu einer Änderung der Art und Weise führen, wie EasyPark Ihre personenbezogenen Daten verarbeitet, beispielsweise der Erhebung zusätzlicher personenbezogener Daten für die genannten Zwecke oder der Verarbeitung von Daten für neue Zwecke, informiert EasyPark Sie über derartige Änderungen beispielsweise über die Website, die App oder per E-Mail. EasyPark empfiehlt, dass Sie die Datenschutzerklärung regelmäßig daraufhin überprüfen, wie EasyPark Ihre personenbezogenen Daten verarbeitet.

## 10 Kontaktdaten

Sollten Sie Fragen oder Anmerkungen zu dieser Datenschutzerklärung haben, wenden Sie sich bitte an den Kundendienst von EasyPark unter [post@easypark.de](mailto:post@easypark.de).

Telefonnummer: +49 (0)221 260 1899

E-Mail-Adresse des Datenschutzbeauftragten: [dpo@easypark.net](mailto:dpo@easypark.net)

Wenn Sie uns zur Geltendmachung Ihrer Datenschutz-Rechte kontaktieren, geben Sie bitte Ihren vollständigen Namen sowie Ihre Kontaktdaten an, unter denen wir Sie erreichen können. Bitte beachten Sie, dass wir Ihre Identität unter Umständen überprüfen müssen, bevor wir Ihr Anliegen bearbeiten können.

\* \* \*

# Microsoft Products and Services Data Protection Addendum

Last updated May 22, 2026

Published in English on May 22, 2026. Translations will be published by Microsoft when available. These commitments are binding on Microsoft as of May 22, 2026.

## Contents

---

|                                                   |    |
|---------------------------------------------------|----|
| Summary of Changes.....                           | 2  |
| Introduction .....                                | 2  |
| Applicable DPA Terms and Updates.....             | 3  |
| Electronic Notices .....                          | 4  |
| Prior Versions.....                               | 4  |
| Definitions.....                                  | 4  |
| General Terms.....                                | 7  |
| Compliance with Laws.....                         | 7  |
| Data Protection Terms .....                       | 7  |
| Scope.....                                        | 7  |
| Nature of Data Processing; Ownership.....         | 8  |
| Disclosure of Processed Data.....                 | 10 |
| Processing of Personal Data; GDPR.....            | 10 |
| Data Security .....                               | 13 |
| Security Incident Notification.....               | 16 |
| Data Transfers and Location.....                  | 16 |
| Data Retention and Deletion.....                  | 18 |
| EU Data Act.....                                  | 18 |
| Processor Confidentiality Commitment .....        | 19 |
| Notice and Controls on use of Subprocessors ..... | 19 |

---

|                                                                                               |    |
|-----------------------------------------------------------------------------------------------|----|
| Previews .....                                                                                | 20 |
| Educational Institutions.....                                                                 | 21 |
| CJIS Customer Agreement .....                                                                 | 21 |
| HIPAA Business Associate.....                                                                 | 21 |
| Telecommunication Data .....                                                                  | 22 |
| California Consumer Privacy Act (CCPA).....                                                   | 22 |
| Biometric Data.....                                                                           | 22 |
| Supplemental Professional Services .....                                                      | 23 |
| How to Contact Microsoft .....                                                                | 23 |
| Appendix A – Security Measures.....                                                           | 25 |
| Domain .....                                                                                  | 25 |
| Practices .....                                                                               | 25 |
| Appendix B – Data Subjects and Categories of Personal Data.....                               | 30 |
| Appendix C – Additional Safeguards Addendum .....                                             | 33 |
| Appendix D – Challenges to Order or Binding Legal Obligation Suspending Online Services ..... | 35 |
| Attachment 1 – European Union General Data Protection Regulation Terms.....                   | 36 |
| Relevant GDPR Obligations: Articles 5, 28, 32, and 33.....                                    | 36 |

## Summary of Changes

---

05/22/2026 – Added clarification of subprocessors that support artificial intelligence functionality in the Notice and Controls on use of Subprocessors section.

## Introduction

---

The parties agree that this Microsoft Products and Services Data Protection Addendum (“DPA”) sets forth their obligations with respect to the processing and security of Customer Data, Professional Services Data, and Personal Data in connection with the Products and Services. The DPA is incorporated by reference into the Product Terms and other Microsoft agreements. The parties also agree that, unless a separate Professional Services agreement exists, this DPA

governs the processing and security of Professional Services Data. Separate terms, including different privacy and security terms, govern Customer's use of Non-Microsoft Products.

In the event of any conflict or inconsistency between the DPA Terms and any other terms in Customer's volume licensing agreement or other applicable agreements in connection with the Products and Services ("Customer's agreement"), the DPA Terms shall prevail. The provisions of the DPA Terms supersede any conflicting provisions of the Microsoft Privacy Statement that otherwise may apply to processing of Customer Data, Professional Services Data, or Personal Data, as defined herein.

Microsoft makes the commitments in this DPA to all Customers with an existing Customer's agreement. These commitments are binding on Microsoft with regard to Customer regardless of (1) the Product Terms that are otherwise applicable to any given Product subscription or license, or (2) any other agreement that references the Product Terms.

## Applicable DPA Terms and Updates

### Limits on Updates

When Customer renews or purchases a new subscription to a Product or enters into a work order for a Professional Service, the then-current DPA Terms will apply and will not change during Customer's subscription for that Product or term for that Professional Service. When Customer obtains a perpetual license to Software, the then-current DPA Terms will apply (following the same provision for determining the applicable then-current Product Terms for that Software in Customer's agreement) and will not change during Customer's license for that Software.

### New Features, Supplements, or Related Software

Notwithstanding the foregoing limits on updates, when Microsoft introduces features, offerings, supplements or related software that are new (i.e., that were not previously included with the Products or Services), Microsoft may provide terms or make updates to the DPA that apply to Customer's use of those new features, offerings, supplements or related software. If those terms include any material adverse changes to the DPA Terms, Microsoft will provide Customer a choice to use the new features, offerings, supplements, or related software, without loss of existing functionality of a generally available Product or Professional Service. If Customer does not install or use the new features, offerings, supplements, or related software, the corresponding new terms will not apply.

## Government Regulation and Requirements

Notwithstanding the foregoing limits on updates, Microsoft may modify or terminate a Product or Professional Service in any country or jurisdiction where there is any current or future government requirement or obligation that (1) subjects Microsoft to any regulation or requirement not generally applicable to businesses operating there, (2) presents a hardship for Microsoft to continue operating the Product or offering the Professional Service without modification, and/or (3) causes Microsoft to believe the DPA Terms or the Product or Professional Service may conflict with any such requirement or obligation.

## Electronic Notices

Microsoft may provide Customer with information and notices about Products and Services electronically, including via email, through the portal for an Online Service, or through a web site that Microsoft identifies. Notice is given as of the date it is made available by Microsoft.

## Prior Versions

The DPA Terms provide terms for Products and Services that are currently available. For earlier versions of the DPA Terms, Customer may refer to <https://aka.ms/licensingdocs> or contact its reseller or Microsoft Account Manager.

## Definitions

---

Capitalized terms used but not defined in this DPA will have the meanings provided in Customer's agreement. The following defined terms are used in this DPA:

"Customer Data" means all data, including all text, sound, video, or image files, and software, that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service. Customer Data does not include Professional Services Data.

"Data Protection Requirements" means the GDPR, Local EU/EEA Data Protection Laws, and any applicable laws, regulations, and other legal requirements relating to (a) privacy and data security; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

"DPA Terms" means the terms in the DPA and any Product-specific terms in the Product Terms that specifically supplement or modify the privacy and security terms in the DPA for a specific Product (or feature of a Product). In the event of any conflict or inconsistency between the DPA

and such Product-specific terms, the Product-specific terms shall prevail as to the applicable Product (or feature of that Product).

"EU Customer" means a Customer that has a European Economic Area ("EEA") billing address.

"EU Data Act" means Regulation (EU) 2023/2854 of the European Parliament and Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2020/1828 (Data Act).

"EU Data Act Service" means an Online Service licensed to an EU Customer, excluding an Online Service for which the EU Customer has elected to store Customer Data outside of the EEA.

"Exportable Data and Digital Assets" (EDDA) means Customer Data. For clarity, EDDA does not include Microsoft trade secret(s) or intellectual property, or data that could compromise the security or integrity of the Online Services.

"GDPR" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

"Local EU/EEA Data Protection Laws" means any subordinate legislation and regulation implementing the GDPR.

"GDPR Terms" means the terms in [Attachment 1](#), under which Microsoft makes binding commitments regarding its processing of Personal Data as required by Article 28 of the GDPR.

"Personal Data" means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Preview Data" means Customer Data and Personal Data provided to Microsoft by, or on behalf of, Customer through use of a Preview or generated through Customer's use of a Preview.

"Product" has the meaning provided in the volume license agreement. For ease of reference, "Product" includes Online Services and Software, each as defined in the volume license agreement.

“Products and Services” means Products and Professional Services. Product and Professional Service availability may vary by region and applicability of this DPA to specific Products and Professional Services is subject to the limitations in the Scope section in this DPA.

“Professional Services” means the following services: (a) Microsoft’s consulting services, consisting of planning, advice, guidance, data migration, deployment and solution/software development services provided under a Microsoft Enterprise Services Work Order or, when agreed to in the Project Description, under a Cloud Workload Acceleration Agreement that incorporates this DPA by reference; and (b) technical support services provided by Microsoft that help customers identify and resolve issues affecting Products, including technical support provided as part of Microsoft Unified Support or Premier Support Services, and any other commercial technical support services. The Professional Services do not include the Products or, for purposes of the DPA only, Supplemental Professional Services.

“Professional Services Data” means all data, including all text, sound, video, image files or software, that are provided to Microsoft, by or on behalf of a Customer (or that Customer authorizes Microsoft to obtain from a Product) or otherwise obtained or processed by or on behalf of Microsoft through an engagement with Microsoft to obtain Professional Services.

“2021 Standard Contractual Clauses” means the standard data protection clauses (processor-to-processor module) between Microsoft Ireland Operations Limited and Microsoft Corporation for the transfer of personal data from processors in the EEA to processors established in third countries which do not ensure an adequate level of data protection, as described in Article 46 of the GDPR and approved by the European Commission in decision 2021/914/EC, dated 4 June 2021.

“Subprocessor” means other processors used by Microsoft to process Customer Data, Professional Services Data, and Personal Data, as described in Article 28 of the GDPR.

“Supplemental Professional Services” means support requests escalated from support to a Product engineering team for resolution and other consulting and support from Microsoft provided in connection with Products or a volume license agreement that are not included in the definition of Professional Services.

“Switching” means an EU Customer’s one-time transfer of EDDA out of an EU Data Act Service to a non-Microsoft cloud service provider identified by the EU Customer and whose information EU Customer provides to Microsoft, or to the EU Customer’s on-premises ICT environment, when the EU Customer is terminating their subscription and ending their use of the EU Data Act Service.

Lower case terms used but not defined in this DPA, such as “personal data breach”, “processing”, “controller”, “processor”, “profiling”, “personal data”, and “data subject” will have the same meaning as set forth in Article 4 of the GDPR, irrespective of whether GDPR applies.

## General Terms

---

### Compliance with Laws

Microsoft will comply with all laws and regulations applicable to its providing the Products and Services, including security breach notification law and Data Protection Requirements. However, Microsoft is not responsible for compliance with any laws or regulations applicable to Customer or Customer’s industry that are not generally applicable to information technology service providers. Microsoft does not determine whether Customer’s data includes information subject to any specific law or regulation. All Security Incidents are subject to the Security Incident Notification terms below.

Customer must comply with all laws and regulations applicable to its use of Products and Services, including laws related to biometric data, confidentiality of communications, and Data Protection Requirements. Customer is responsible for determining whether the Products and Services are appropriate for storage and processing of information subject to any specific law or regulation and for using the Products and Services in a manner consistent with Customer’s legal and regulatory obligations. Customer is responsible for responding to any request from a third party regarding Customer’s use of Products and Services, such as a request to take down content under the U.S. Digital Millennium Copyright Act or other applicable laws.

## Data Protection Terms

---

### Scope

The DPA Terms apply to all Products and Services except as described in this section.

The DPA Terms will not apply to any Products or Professional Services specifically identified as excluded, or to the extent identified as excluded, in the Product Terms or applicable work order, which are governed by the privacy and security terms in the applicable Product-specific or work order specific terms.

For clarity, the DPA Terms apply only to the processing of data in environments controlled by Microsoft and Microsoft's subprocessors. This includes data sent to Microsoft by Products and



Services but does not include data that remains on Customer's premises or in any Customer selected third party operating environments.

For Supplemental Professional Services, Microsoft only makes the commitments in the Supplemental Professional Services section below.

## Nature of Data Processing; Ownership

Microsoft will use and otherwise process Customer Data, Professional Services Data, and Personal Data only as described and subject to the limitations provided below (a) to provide Customer the Products and Services in accordance with Customer's documented instructions and (b) for business operations incident to providing the Products and Services to Customer. As between the parties, Customer retains all right, title and interest in and to Customer Data and Professional Services Data. Microsoft acquires no rights in Customer Data or Professional Services Data, other than the rights Customer grants to Microsoft in this section. This paragraph does not affect Microsoft's rights in software or services Microsoft licenses to Customer.

## Processing to Provide Customer the Products and Services

For purposes of this DPA, "to provide" a Product consists of:

- Delivering functional capabilities as licensed, configured, and used by Customer and its users, including providing personalized user experiences;
- Troubleshooting (preventing, detecting, and repairing problems); and
- Keeping Products up to date and performant, and enhancing user productivity, reliability, efficacy, quality, and security.

For purposes of this DPA, "to provide" Professional Services consists of:

- Delivering the Professional Services, including providing technical support, professional planning, advice, guidance, data migration, deployment, and solution/software development services.
- Troubleshooting (preventing, detecting, investigating, mitigating, and repairing problems, including Security Incidents and problems identified in the Professional Services or relevant Product(s) during delivery of Professional Services); and
- Enhancing delivery, efficacy, quality, and security of Professional Services and the underlying Product(s) based on issues identified while providing Professional Services, including fixing software defects and otherwise keeping Products and Services up to date and performant.

In each case, providing the Products and Services is conducted in view of security obligations under Data Protection Requirements.

When providing Products and Services, Microsoft will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) market research aimed at creating new functionalities, services, or products or any other purpose, unless such use or processing is in accordance with Customer's documented instructions.

## Processing for Business Operations Incident to Providing the Products and Services to Customer

For purposes of this DPA, "business operations" means the processing operations authorized by customer in this section.

Customer authorizes Microsoft:

- to create aggregated statistical, non-personal data from data containing pseudonymized identifiers (such as usage logs containing unique, pseudonymized identifiers); and
- to calculate statistics related to Customer Data or Professional Services Data

in each case without accessing or analyzing the content of Customer Data or Professional Services Data and limited to achieving the purposes below, each as incident to providing the Products and Services to Customer.

Those purposes are:

- billing and account management;
- compensation such as calculating employee commissions and partner incentives;
- internal reporting and business modeling, such as forecasting, revenue, capacity planning, and product strategy; and
- financial reporting.

When processing for these business operations, Microsoft will apply principles of data minimization and will not use or otherwise process Customer Data, Professional Services Data, or Personal Data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) any other purpose, other than for the purposes set out in this section. In addition, as with all processing under this DPA, processing for business operations remains subject to Microsoft's confidentiality obligations and commitments under Disclosure of Processed Data.

## Disclosure of Processed Data

Microsoft will not disclose or provide access to any Processed Data except: (1) as Customer directs; (2) as described in this DPA; or (3) as required by law. For purposes of this section, "Processed Data" means: (a) Customer Data; (b) Professional Services Data; (c) Personal Data; and (d) any other data processed by Microsoft in connection with the Products and Services that is Customer's confidential information under Customer's agreement. All processing of Processed Data is subject to Microsoft's obligation of confidentiality under Customer's agreement.

Microsoft will not disclose or provide access to any Processed Data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for Processed Data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from Customer. If compelled to disclose or provide access to any Processed Data to law enforcement, Microsoft will promptly notify Customer and provide a copy of the demand unless legally prohibited from doing so.

Upon receipt of any other third-party request for Processed Data, Microsoft will promptly notify Customer unless prohibited by law. Microsoft will reject the request unless required by law to comply. If the request is valid, Microsoft will attempt to redirect the third party to request the data directly from Customer.

Microsoft will only disclose or provide access to any Processed Data as required by law provided that the laws and practices respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society and, as applicable, to safeguard one of the objectives listed in Article 23(1) of GDPR.

Microsoft will not provide any third party: (a) direct, indirect, blanket, or unfettered access to Processed Data; (b) platform encryption keys used to secure Processed Data or the ability to break such encryption; or (c) access to Processed Data if Microsoft is aware that the data is to be used for purposes other than those stated in the third party's request.

In support of the above, Microsoft may provide Customer's basic contact information to the third party.

## Processing of Personal Data; GDPR

All Personal Data processed by Microsoft in connection with providing the Products and Services is obtained as part of either (a) Customer Data, (b) Professional Services Data, or (c) data generated, derived or collected by Microsoft, including data sent to Microsoft as a result of a Customer's use of service-based capabilities or obtained by Microsoft from locally installed

software. Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Online Service is also Customer Data. Personal Data provided to Microsoft by, or on behalf of, Customer through use of the Professional Services is also Professional Services Data.

Pseudonymized identifiers may be included in data processed by Microsoft in connection with providing the Products and are also Personal Data. Any Personal Data pseudonymized, or de-identified but not anonymized, or Personal Data derived from Personal Data is also Personal Data.

To the extent Microsoft is a processor or subprocessor of Personal Data subject to the GDPR, the GDPR Terms in [Attachment 1](#) govern, and the language in the sub-section ("Processing of Personal Data; GDPR") shall be deemed supplemental:

## Processor and Controller Roles and Responsibilities

Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except (a) when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor; or (b) as stated otherwise in the Product-specific terms or this DPA. When Microsoft acts as the processor or subprocessor of Personal Data, it will process Personal Data only on documented instructions from Customer. Customer agrees that Customer's agreement (including the DPA Terms and any applicable updates), along with the product documentation and Customer's use and configuration of features in the Products, are Customer's complete documented instructions to Microsoft for the processing of Personal Data, or the Professional Services documentation and Customer's use of the Professional Services.

Information on use and configuration of the Products can be found at <https://docs.microsoft.com> (or a successor location) or other agreement incorporating this DPA. Any additional or alternate instructions must be agreed to according to the process for amending Customer's agreement. In any instance where the GDPR applies and Customer is a processor, Customer warrants to Microsoft that Customer's instructions, including appointment of Microsoft as a processor or subprocessor, have been authorized by the relevant controller.

To the extent Microsoft uses or otherwise processes Personal Data subject to the GDPR for business operations incident to providing the Products and Services to Customer, Microsoft will comply with the obligations of an independent data controller under GDPR for such use.

Microsoft is accepting the added responsibilities of a data "controller" under GDPR for such processing to: (a) act consistent with regulatory requirements, to the extent required under GDPR; and (b) provide increased transparency to Customers and confirm Microsoft's accountability for such processing. Microsoft employs safeguards to protect Customer Data, Professional Services Data, and Personal Data in such processing, including those identified in this DPA and those contemplated in Article 6(4) of the GDPR. With respect to processing of

Personal Data under this paragraph, Microsoft makes the commitments set forth in the Additional Safeguards section; for those purposes, (i) any Microsoft disclosure of Personal Data, as described in the Additional Safeguards section, that has been transferred in connection with business operations is deemed a “Relevant Disclosure” and (ii) the commitments in the Additional Safeguards section apply to such Personal Data.

## Processing Details

The parties acknowledge and agree that:

- **Subject Matter.** The subject-matter of the processing is limited to Personal Data within the scope of the section of this DPA entitled “Nature of Data Processing; Ownership” above and the GDPR.
- **Duration of the Processing.** The duration of the processing shall be in accordance with Customer instructions and the terms of the DPA.
- **Nature and Purpose of the Processing.** The nature and purpose of the processing shall be to provide the Products and Services pursuant to Customer’s agreement and for business operations incident to providing the Products and Services to Customer (as further described in the section of this DPA entitled “Nature of Data Processing; Ownership” above).
- **Categories of Data.** The types of Personal Data processed by Microsoft when providing the Products and Services include: (i) Personal Data that Customer elects to include in Customer Data and Professional Services Data; and (ii) those expressly identified in Article 4 of the GDPR that may be generated, derived or collected by Microsoft, including data sent to Microsoft as a result of a Customer’s use of service-based capabilities or obtained by Microsoft from locally installed software. The types of Personal Data that Customer elects to include in Customer Data and Professional Services Data may be any categories of Personal Data identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of Personal Data set forth in Appendix B.
- **Data Subjects.** The categories of data subjects are Customer’s representatives and end users, such as employees, contractors, collaborators, and customers, and may include any other categories of data subjects as identified in records maintained by Customer acting as controller pursuant to Article 30 of the GDPR, including the categories of data subjects set forth in Appendix B.

## Data Subject Rights; Assistance with Requests

Microsoft will make available to Customer, in a manner consistent with the functionality of the Products and Services and Microsoft’s role as a processor of Personal Data of data subjects, the

ability to fulfill data subject requests to exercise their rights under the GDPR. If Microsoft receives a request from Customer's data subject to exercise one or more of its rights under the GDPR in connection with the Products and Services for which Microsoft is a data processor or subprocessor, Microsoft will redirect the data subject to make its request directly to Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Products and Services. Microsoft shall comply with reasonable requests by Customer to assist with Customer's response to such a data subject request.

## Records of Processing Activities

To the extent the GDPR requires Microsoft to collect and maintain records of certain information relating to Customer, Customer will, where requested, supply such information to Microsoft and keep it accurate and up-to-date. Microsoft may make any such information available to the supervisory authority if required by the GDPR.

## Data Security

### Security Practices and Policies

Microsoft will implement and maintain appropriate technical and organizational measures to protect Customer Data, Professional Services Data, and Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. Those measures shall be set forth in a Microsoft Security Policy. Microsoft will make that policy available to Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies.

In addition, those measures shall comply with the requirements set forth in ISO 27001, ISO 27002, and ISO 27018. A description of the security controls for these requirements is available to Customers.

Each Core Online Service also complies with the control standards and frameworks shown in the table in the Product Terms. Each Core Online Service and Professional Service implements and maintains the security measures set forth in Appendix A for the protection of Customer Data and Professional Services Data.

Microsoft implements and maintains the security measures set forth in Annex II of the 2021 Standard Contractual Clauses for the protection of Personal Data within the scope of the GDPR.

Microsoft may add industry or government standards at any time. Microsoft will not eliminate ISO 27001, ISO 27002, ISO 27018 or any standard or framework in the table for Core Online

Services in the Product Terms, unless it is no longer used in the industry and it is replaced with a successor (if any).

## Data Encryption

Customer Data and Professional Services Data (each including any Personal Data therein) in transit over public networks between Customer and Microsoft, or between Microsoft data centers, is encrypted by default.

Microsoft also encrypts Customer Data stored at rest in Online Services and Professional Services Data stored at rest. In the case of Online Services on which Customer or a third-party acting on Customer's behalf may build applications (e.g., certain Azure Services), encryption of data stored in such applications may be employed at the discretion of Customer, using either capabilities provided by Microsoft or obtained by Customer from third parties.

## Data Access

Microsoft employs least privilege access mechanisms to control access to Customer Data and Professional Services Data (including any Personal Data therein). Role-based access controls are employed to ensure that access to Customer Data and Professional Services Data required for service operations is for an appropriate purpose and approved with management oversight. For Core Online Services and Professional Services, Microsoft maintains Access Control mechanisms described in the table entitled "Security Measures" in Appendix A; and there is no standing access by Microsoft personnel to Customer Data, and any required access is for a limited time.

## Customer Responsibilities

Customer is solely responsible for making an independent determination as to whether the technical and organizational measures for Products and Services meet Customer's requirements, including any of its security obligations under applicable Data Protection Requirements.

Customer acknowledges and agrees that (taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing of its Personal Data as well as the risks to individuals) the security practices and policies implemented and maintained by Microsoft provide a level of security appropriate to the risk with respect to its Personal Data. Customer is responsible for implementing and maintaining privacy protections and security measures for components that Customer provides or controls (such as devices enrolled with Microsoft Intune or within a Microsoft Azure customer's virtual machine or application).



## Auditing Compliance

Microsoft will conduct audits of the security of the computers, computing environment, and physical data centers that it uses in processing Customer Data, Professional Service Data, and Personal Data, as follows:

- Where a standard or framework provides for audits, an audit of such control standard or framework will be initiated at least annually.
- Each audit will be performed according to the standards and rules of the regulatory or accreditation body for each applicable control standard or framework.
- Each audit will be performed by qualified, independent, third party security auditors at Microsoft's selection and expense.

Each audit will result in the generation of an audit report ("Microsoft Audit Report"), which Microsoft will make available at <https://servicetrust.microsoft.com/> or another location identified by Microsoft. The Microsoft Audit Report will be Microsoft's Confidential Information and will clearly disclose any material findings by the auditor. Microsoft will promptly remediate issues raised in any Microsoft Audit Report to the satisfaction of the auditor. If Customer requests, Microsoft will provide Customer with each Microsoft Audit Report. The Microsoft Audit Report will be subject to non-disclosure and distribution limitations of Microsoft and the auditor.

To the extent Customer's audit requirements under the Data Protection Requirements cannot reasonably be satisfied through audit reports, documentation or compliance information Microsoft makes generally available to its customers, Microsoft will promptly respond to Customer's additional audit instructions. Before the commencement of an audit, Customer and Microsoft will mutually agree upon the scope, timing, duration, control and evidence requirements, and fees for the audit, provided that this requirement to agree will not permit Microsoft to unreasonably delay performance of the audit. To the extent needed to perform the audit, Microsoft will make the processing systems, facilities and supporting documentation relevant to the processing of Customer Data, Professional Services Data, and Personal Data by Microsoft, its Affiliates, and its Subprocessors available. Such an audit will be conducted by an independent, accredited third-party audit firm, during regular business hours, with reasonable advance notice to Microsoft, and subject to reasonable confidentiality procedures. Neither Customer nor the auditor shall have access to any data from Microsoft's other customers or to Microsoft systems or facilities not involved in providing the applicable Products and Services. Customer is responsible for all costs and fees related to such audit, including all reasonable costs and fees for any and all time Microsoft expends for any such audit, in addition to the rates for services performed by Microsoft. If the audit report generated as a result of Customer's audit



includes any finding of material non-compliance, Customer shall share such audit report with Microsoft and Microsoft shall promptly cure any material non-compliance.

Nothing in this section of the DPA varies or modifies the GDPR Terms or affects any supervisory authority's or data subject's rights under the Data Protection Requirements. Microsoft Corporation is an intended third-party beneficiary of this section.

## Security Incident Notification

If Microsoft becomes aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data, Professional Services Data, or Personal Data while processed by Microsoft (each a "Security Incident"), Microsoft will promptly and without undue delay (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident; (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident.

Notification(s) of Security Incidents will be delivered to Customer by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer maintains accurate contact information with Microsoft for each applicable Product and Professional Service. Customer is solely responsible for complying with its obligations under incident notification laws applicable to Customer and fulfilling any third-party notification obligations related to any Security Incident.

Microsoft shall make reasonable efforts to assist Customer in fulfilling Customer's obligation under GDPR Article 33 or other applicable law or regulation to notify the relevant supervisory authority and data subjects about such Security Incident.

Microsoft's notification of or response to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to the Products and Services.

## Data Transfers and Location

### Data Transfers

Customer Data, Professional Services Data, and Personal Data that Microsoft processes on Customer's behalf may not be transferred to, or stored and processed in a geographic location except in accordance with the DPA Terms and the safeguards provided below in this section.

Taking into account such safeguards, Customer appoints Microsoft to transfer Customer Data, Professional Services Data, and Personal Data to the United States or any other country in which Microsoft or its Subprocessors operate and to store and process Customer Data, and Personal Data to provide the Products, except as described elsewhere in the DPA Terms.

All transfers of Customer Data, Professional Services Data, and Personal Data out of the European Union, European Economic Area, United Kingdom, and Switzerland to provide the Products and Services are subject to the terms of the 2021 Standard Contractual Clauses implemented by Microsoft. In addition, transfers from the United Kingdom are subject to the terms of the IDTA implemented by Microsoft. For purposes of this DPA, the "IDTA" means the International data transfer addendum to the European Commission's standard contractual clauses for international data transfers issued by the UK Information Commissioner's Office under S119A(1) of the UK Data Protection Act 2018. Microsoft will abide by the requirements of European Economic Area, United Kingdom, and Swiss data protection law regarding the collection, use, transfer, retention, and other processing of Personal Data from the European Economic Area, United Kingdom, and Switzerland. All transfers of Personal Data to a third country or an international organization will be subject to appropriate safeguards as described in Article 46 of the GDPR and such transfers and safeguards will be documented according to Article 30(2) of the GDPR.

In addition, Microsoft is certified to the EU-U.S. and Swiss-U.S. Data Privacy Frameworks, the UK Extension to the EU-U.S. Data Privacy Framework and the commitments they entail. Microsoft agrees to notify Customer if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the principles of the Data Privacy Frameworks.

## Location of Customer Data

For the Core Online Services, Microsoft will store Customer Data at rest within certain major geographic areas (each, a Geo) as set forth in the Product Terms.

For EU Data Boundary Services, Microsoft will store and process Customer Data, Personal Data, and store Professional Services Data at rest within the European Union and the European Free Trade Association (EFTA) as set forth in the Product Terms.

Microsoft does not control or limit the regions from which Customer or Customer's end users may access or move Customer Data.

## Data Retention and Deletion

At all times during the term of Customer's subscription or the applicable Professional Services engagement, Customer will have the ability to access, extract and delete Customer Data stored in each Online Service and Professional Services Data.

Except for free trials and LinkedIn services, Microsoft will retain Customer Data that remains stored in Online Services in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data and Personal Data stored in Online Services within an additional 90 days, unless authorized under this DPA to retain such data.

For Personal Data in connection with the Software and for Professional Services Data, Microsoft will delete all copies after the business purposes for which the data was collected or transferred have been fulfilled or earlier upon Customer's request, unless authorized under this DPA to retain such data.

The Online Service may not support retention or extraction of software provided by Customer. Microsoft has no liability for the deletion of Customer Data, Professional Services Data, or Personal Data as described in this section.

## EU Data Act

Switching is permitted at any time at no additional cost beyond the fees and other amounts otherwise due pursuant to EU Customer's agreement. EU Customer may access, export, and delete EDDA at any time, including accessing and exporting EDDA up to 90 days after subscription termination, as set forth in the Data Retention and Deletion provision. EU Customer decides when to start exporting EDDA and on what timeline. More than 30 days may be required for actual extraction and export of EDDA by EU Customer depending on the customer's specific configuration, quantity of data, the Switching destination, and other circumstances outside of Microsoft's control. EU Customer should complete Switching prior to termination of the EU Data Act Service, which EU Customer may do with 60 days' notice to Microsoft and payment of any amount still owed pursuant to EU Customer's agreement. Microsoft will provide reasonable assistance for Switching and will act with due care as set forth in the Data Security and other sections of the DPA and under Customer's agreement in providing the EU Data Act Services during Switching and in parallel use. An EU Customer may obtain a reduction in data egress fees associated with Switching and in parallel use as provided under the law. These EU Data Act terms do not apply to Previews.

Supporting materials on data export and methods and information related to Microsoft ICT infrastructure used to provide EU Data Act Services and how Microsoft responds to government data access requests can be found in the Product Terms.

## Processor Confidentiality Commitment

Microsoft will ensure that its personnel engaged in the processing of Customer Data, Professional Services Data, and Personal Data (i) will process such data only on instructions from Customer or as described in this DPA, and (ii) will be obligated to maintain the confidentiality and security of such data even after their engagement ends. Microsoft shall provide periodic and mandatory data privacy and security training and awareness to its employees with access to Customer Data, Professional Services Data, and Personal Data in accordance with applicable Data Protection Requirements and industry standards.

## Notice and Controls on use of Subprocessors

Microsoft may hire Subprocessors to provide certain limited or ancillary services on its behalf. Customer consents to this engagement and to Microsoft Affiliates as Subprocessors. The above authorizations will constitute Customer's prior written consent to the subcontracting by Microsoft of the processing of Customer Data, Professional Services Data, and Personal Data if such consent is required under the Standard Contractual Clauses or the GDPR Terms.

Microsoft is responsible for its Subprocessors' compliance with Microsoft's obligations in this DPA. Microsoft makes available information about Subprocessors on a Microsoft website. When engaging any Subprocessor, Microsoft will ensure via a written contract that the Subprocessor may access and use Customer Data, Professional Services Data, or Personal Data only to deliver the services Microsoft has retained them to provide and is prohibited from using Customer Data, Professional Services Data, or Personal Data for any other purpose. Microsoft will ensure that Subprocessors are bound by written agreements that require them to provide at least the level of data protection required of Microsoft by the DPA, including the limitations on disclosure of Processed Data. Microsoft agrees to oversee the Subprocessors to ensure that these contractual obligations are met.

From time to time, Microsoft may engage new Subprocessors. Microsoft will give Customer notice and, as applicable, update the website and provide Customer with a mechanism to obtain notice of that update of any new Subprocessor at least 6 months in advance of providing that Subprocessor with access to Customer Data or for subprocessors that support artificial intelligence functionality, 30 days' notice with the ability to disable use of that subprocessor until at least 6 months after notice. Additionally, Microsoft will give Customer notice and, as

applicable, update the website and provide Customer with a mechanism to obtain notice of that update of any new Subprocessor at least 30 days in advance of providing that Subprocessor with access to Professional Services Data or Personal Data other than that which is contained in Customer Data. If Microsoft engages a new Subprocessor for a new Product or Professional Service that processes Customer Data, Professional Services Data, or Personal Data, Microsoft will give Customer notice prior to availability of that Product or Professional Service.

If Customer does not approve of a new Subprocessor for an Online Service or Professional Services, then Customer may terminate any subscription for the affected Online Service or the applicable Statements of Service for the applicable Professional Service, respectively, without penalty or termination fee by providing, before the end of the relevant notice period, written notice of termination. If Customer does not approve of a new Subprocessor for Software, and Customer cannot reasonably avoid use of the Subprocessor by restricting Microsoft from processing data as set forth in the documentation or this DPA, then Customer may terminate any license for the affected software product without penalty by providing, before the end of the relevant notice period, written notice of termination. Customer may also include an explanation of the grounds for non-approval together with the termination notice, in order to permit Microsoft to re-evaluate any such new Subprocessor based on the applicable concerns. If the affected Product is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for any subscriptions or other applicable unpaid work for the terminated Products or Services from subsequent invoices to Customer or its reseller.

## Previews

Previews may employ lesser or different privacy and security measures than those typically present in the Products and Services. Unless otherwise noted, Customer should not use Previews to process Personal Data or other data that is subject to legal or regulatory compliance requirements. Except for Previews that allow Personal Data Processing, for Products, the following terms in this DPA do not apply to Previews: Processing of Personal Data; GDPR, Data Security, and HIPAA Business Associate. For Professional Services, offerings designated as Previews or Limited Release only meet the terms of the Supplemental Professional Services.

For Previews that allow Personal Data processing, all terms in this DPA apply subject to following:

- Preview Data may be transferred to, and stored and processed in, the United States or any other country in which Microsoft or its Subprocessors operate. Accordingly, Location

of Customer Data does not apply to Previews insofar as it would restrict the countries where Microsoft can transfer, store, or process Preview Data.

- Previews may not retain Preview Data beyond the duration of a Preview. When a Preview ends or Customer otherwise ceases participation in a Preview, Microsoft may delete Preview Data, even if the Preview is subsequently made generally commercially available. Accordingly, Data Retention and Deletion does not apply to Previews insofar as it would restrict Microsoft's right to delete Preview Data.

Previews may be subject to additional terms provided separately as part of those Previews.

## Educational Institutions

If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA), apply, Microsoft acknowledges that for the purposes of the DPA, Microsoft is a "school official" with "legitimate educational interests" in the Customer Data and Professional Services Data, as those terms have been defined under FERPA and its implementing regulations, and Microsoft agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials.

Customer understands that Microsoft may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer will be responsible for obtaining any parental consent for any end user's use of the Products and Services that may be required by applicable law and to convey notification on behalf of Microsoft to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data and Professional Services Data in Microsoft's possession as may be required under applicable law.

## CJIS Customer Agreement

Microsoft provides certain government cloud services ("Covered Services") in accordance with the FBI Criminal Justice Information Services ("CJIS") Security Policy ("CJIS Policy"). The CJIS Policy governs the use and transmission of criminal justice information. All Microsoft CJIS Covered Services shall be governed by the terms and conditions in the CJIS Management Agreement.

## HIPAA Business Associate

If Customer is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data or Professional Services Data, as those terms are defined under

the Health Insurance Portability and Accountability Act of 1996, as amended, and the regulations promulgated thereunder (collectively, "HIPAA"), execution of Customer's agreement includes execution of the HIPAA Business Associate Agreement ("BAA"). The full text of the BAA identifies the Online Services or Professional Services to which it applies and is available at <http://aka.ms/BAA>. Customer may opt out of the BAA by sending the following information to Microsoft in a written notice (under the terms of the Customer's agreement):

- the full legal name of the Customer and any Affiliate that is opting out; and
- if Customer has multiple agreements, Customer's agreement to which the opt out applies.

## Telecommunication Data

To the extent Microsoft is processing traffic, content and other Personal Data in the provision of Products and Services that qualify as telecommunication services under applicable law, specific statutory obligations may apply. Microsoft will comply with all telecommunication specific laws and regulations applicable to its providing the Products and Services, including security breach notification, Data Protection Requirements, and telecommunication secrecy. Customer is responsible for obtaining any appropriate consent from end users in connection with use of Products and Services that qualify as telecommunication services.

## California Consumer Privacy Act (CCPA)

If Microsoft is processing Personal Data within the scope of the CCPA, Microsoft makes the following additional commitments to Customer. Microsoft will process Customer Data, Professional Services Data, and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in the DPA Terms and as permitted under the CCPA, including under any "sale" exemption. In no event will Microsoft sell any such data. These CCPA terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the DPA Terms, Product Terms, or other agreement between Microsoft and Customer.

## Biometric Data

If Customer uses Products and Services to process Biometric Data, Customer is responsible for: (i) providing notice to data subjects, including with respect to retention periods and destruction; (ii) obtaining consent from data subjects; and (iii) deleting the Biometric Data, all as appropriate and required under applicable Data Protection Requirements. Microsoft will process that Biometric Data following Customer's documented instructions (as described in the "Processor and Controller Roles and Responsibilities" section above) and protect that Biometric Data in



accordance with the data security and protection terms under this DPA. For purposes of this section, "Biometric Data" will have the meaning set forth in Article 4 of the GDPR and, if applicable, equivalent terms in other Data Protection Requirements.

## Supplemental Professional Services

When used in the sections listed below, the defined term "Professional Services" includes Supplemental Professional Services, and the defined term "Professional Services Data" includes data obtained for Supplemental Professional Services.

For Supplemental Professional Services, the following sections of the DPA apply in the same manner as they apply to Professional Services: "Introduction", "Compliance with Laws", "Nature of Processing; Ownership", "Disclosure of Processed Data", "Processing of Personal Data; GDPR", the first paragraph of "Security Practices and Policies", "Customer Responsibilities", "Security Incident Notification", "Data Transfer" (including the terms regarding the 2021 Standard Contractual Clauses), the third paragraph of "Data Retention and Deletion", "Processor Confidentiality Commitment", "Notice and Controls on use of Subprocessors", "HIPAA Business Associate" (to the extent applicable in the BAA), "California Consumer Privacy Act (CCPA)", "Biometric Data", "How to Contact Microsoft", "Appendix B – Data Subjects and Categories of Personal Data", and "Appendix C – Additional Safeguards Addendum".

## How to Contact Microsoft

If Customer believes that Microsoft is not adhering to its privacy or security commitments, Customer may contact customer support or use Microsoft's Privacy web form, located at <http://go.microsoft.com/?linkid=9846224>. Microsoft's mailing address is:

### **Microsoft Enterprise Service Privacy**

Microsoft Corporation  
One Microsoft Way  
Redmond, Washington 98052 USA

Microsoft Ireland Operations Limited is Microsoft's data protection representative for the European Economic Area and Switzerland. The privacy representative of Microsoft Ireland Operations Limited can be reached at the following address:

### **Microsoft Ireland Operations, Ltd.**

Attn: Data Protection  
One Microsoft Place  
South County Business Park  
Leopardstown



Dublin 18, D18 P521, Ireland

## Appendix A – Security Measures

Microsoft has implemented and will maintain for Customer Data in the Core Online Services and Professional Services Data the following security measures, which in conjunction with the security commitments in this DPA (including the GDPR Terms), are Microsoft's only responsibility with respect to the security of that data.

| Domain                               | Practices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Organization of Information Security | <p><b>Security Ownership.</b> Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures.</p> <p><b>Security Roles and Responsibilities.</b> Microsoft personnel with access to Customer Data or Professional Services Data are subject to confidentiality obligations.</p> <p><b>Risk Management Program.</b> Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service and before processing Professional Service Data or launching the Professional Services.</p> <p>Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.</p>                                                                                                                                                                                                     |
| Asset Management                     | <p><b>Asset Inventory.</b> Microsoft maintains an inventory of all media on which Customer Data or Professional Services Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access.</p> <p><b>Asset Handling</b></p> <ul style="list-style-type: none"> <li>• Microsoft classifies Customer Data and Professional Services Data to help identify it and to allow for access to it to be appropriately restricted.</li> <li>• Microsoft imposes restrictions on printing Customer Data and Professional Services Data and has procedures for disposing of printed materials that contain such data.</li> <li>• Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data or Professional Services Data on portable devices, remotely accessing such data, or processing such data outside Microsoft's facilities.</li> </ul> |

| Domain                                   | Practices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Human Resources Security                 | <p><b>Security Training.</b> Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will only use anonymous data in training.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Physical and Environmental Security      | <p><b>Physical Access to Facilities.</b> Microsoft limits access to facilities where information systems that process Customer Data or Professional Services Data are located to identified authorized individuals.</p> <p><b>Physical Access to Components.</b> Microsoft maintains records of the incoming and outgoing media containing Customer Data or Professional Services Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of such data they contain.</p> <p><b>Protection from Disruptions.</b> Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference.</p> <p><b>Component Disposal.</b> Microsoft uses industry standard processes to delete Customer Data and Professional Services Data when it is no longer needed.</p>                                                                                                                                                                                                                           |
| Communications and Operations Management | <p><b>Operational Policy.</b> Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data or Professional Services Data.</p> <p><b>Data Recovery Procedures</b></p> <ul style="list-style-type: none"> <li>On an ongoing basis, but in no case less frequently than once a week (unless no updates have occurred during that period), Microsoft maintains multiple copies of Customer Data and Professional Services Data from which such data can be recovered.</li> <li>Microsoft stores copies of Customer Data and Professional Services Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data and Professional Services Data are located.</li> <li>Microsoft has specific procedures in place governing access to copies of Customer Data and Professional Services Data.</li> <li>Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Professional</li> </ul> |

| Domain         | Practices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                | <p>Services and for Azure Government Services, which are reviewed every twelve months.</p> <ul style="list-style-type: none"> <li>• Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.</li> <li>• Malicious Software. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data and Professional Services Data, including malicious software originating from public networks.</li> </ul> <p><b>Data Beyond Boundaries</b></p> <ul style="list-style-type: none"> <li>• Microsoft encrypts, or enables Customer to encrypt, Customer Data and Professional Services Data that is transmitted over public networks.</li> <li>• Microsoft restricts access to Customer Data and Professional Services Data in media leaving its facilities.</li> </ul> <p><b>Event Logging.</b> Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data or Professional Services Data, registering the access ID, time, authorization granted or denied, and relevant activity.</p> |
| Access Control | <p><b>Access Policy.</b> Microsoft maintains a record of security privileges of individuals having access to Customer Data or Professional Services Data.</p> <p><b>Access Authorization</b></p> <ul style="list-style-type: none"> <li>• Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data or Professional Services Data.</li> <li>• Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months.</li> <li>• Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources.</li> <li>• Microsoft ensures that where more than one individual has access to systems containing Customer Data or Professional Services Data, the individuals have separate identifiers/log-ins.</li> </ul> <p><b>Least Privilege</b></p>                                                                                                                                                                                                                                                                                                                                                                |

| Domain                                   | Practices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                          | <ul style="list-style-type: none"> <li>• Technical support personnel are only permitted to have access to Customer Data and Professional Services Data when needed.</li> <li>• Microsoft restricts access to Customer Data and Professional Services Data to only those individuals who require such access to perform their job function.</li> </ul> <p><b>Integrity and Confidentiality</b></p> <ul style="list-style-type: none"> <li>• Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended.</li> <li>• Microsoft stores passwords in a way that makes them unintelligible while they are in force.</li> </ul> <p><b>Authentication</b></p> <ul style="list-style-type: none"> <li>• Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems.</li> <li>• Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly.</li> <li>• Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long.</li> <li>• Microsoft ensures that de-activated or expired identifiers are not granted to other individuals.</li> <li>• Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password.</li> <li>• Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed.</li> <li>• Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.</li> </ul> <p><b>Network Design.</b> Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data or Professional Services Data they are not authorized to access.</p> |
| Information Security Incident Management | <p><b>Incident Response Process</b></p> <ul style="list-style-type: none"> <li>• Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Domain                         | Practices                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | <p>breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data.</p> <ul style="list-style-type: none"> <li>• For each security breach that is a Security Incident, notification by Microsoft (as described in the “Security Incident Notification” section above) will be made without undue delay and, in any event, within 72 hours.</li> <li>• Microsoft tracks, or enables Customer to track, disclosures of Customer Data and Professional Services Data, including what data has been disclosed, to whom, and at what time.</li> </ul> <p><b>Service Monitoring.</b> Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.</p> |
| Business Continuity Management | <ul style="list-style-type: none"> <li>• Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data or Professional Services Data are located.</li> <li>• Microsoft’s redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data and Professional Services Data in its original or last-replicated state from before the time it was lost or destroyed.</li> </ul>                                                                                                                                                                                                                                             |

## Appendix B – Data Subjects and Categories of Personal Data

---

**Data subjects:** Data subjects include the Customer's representatives and end-users including employees, contractors, collaborators, and customers of the Customer. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by Microsoft. Microsoft acknowledges that, depending on Customer's use of the Products and Services, Customer may elect to include personal data from any of the following types of data subjects in the personal data:

- Employees, contractors and temporary workers (current, former, prospective) of Customer;
- Dependents of the above;
- Customer's collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of Customer's services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the Customer and/or use communication tools such as apps and websites provided by the Customer;
- Stakeholders or individuals who passively interact with Customer (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the Customer);
- Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

**Categories of data:** The personal data that is included in e-mail, documents and other data in an electronic form in the context of the Products and Services. Microsoft acknowledges that, depending on Customer's use of the Products and Services, Customer may elect to include personal data from any of the following categories in the personal data:

- Basic personal data (for example place of birth, street name and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last

- name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
  - Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
  - Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver's license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
  - Pseudonymous identifiers;
  - Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);
  - Commercial Information (for example history of purchases, special offers, subscription information, payment history);
  - Biometric Information (for example DNA, fingerprints and iris scans);
  - Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
  - Photos, video and audio;
  - Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
  - Device identification (for example IMEI-number, SIM card number, MAC address);
  - Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
  - HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location and organizations);
  - Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
  - Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);



- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions or offences); or
- Any other personal data identified in Article 4 of the GDPR.

## Appendix C – Additional Safeguards Addendum

---

By this Additional Safeguards Addendum to the DPA (this “Addendum”), Microsoft provides additional safeguards to Customer for the processing of personal data, within the scope of the GDPR, by Microsoft on behalf of Customer and additional redress to the data subjects to whom that personal data relates.

This Addendum supplements and is made part of, but is not in variation or modification of, the DPA.

1. **Challenges to Orders.** In the event Microsoft receives an order from any third party for compelled disclosure of any personal data processed under this DPA, Microsoft shall:
  - a. use every reasonable effort to redirect the third party to request data directly from Customer;
  - b. promptly notify Customer, unless prohibited under the law applicable to the requesting third party, and, if prohibited from notifying Customer, use all lawful efforts to obtain the right to waive the prohibition in order to communicate as much information to Customer as soon as possible; and
  - c. use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the laws of the requesting party or any relevant conflicts with applicable law of the European Union or applicable Member State law.

If, after the steps described in a. through c. above, Microsoft or any of its affiliates remains compelled to disclose personal data, Microsoft will disclose only the minimum amount of that data necessary to satisfy the order for compelled disclosure.

For purpose of this section, lawful efforts do not include actions that would result in civil or criminal penalty such as contempt of court under the laws of the relevant jurisdiction.

2. **Indemnification of Data Subjects.** Subject to Sections 3 and 4, Microsoft shall indemnify a data subject for any material or non-material damage to the data subject caused by Microsoft’s disclosure of personal data of the data subject that has been transferred in response to an order from a non-EU/EEA government body or law enforcement agency in violation of Microsoft’s obligations under Chapter V of the GDPR (a “Relevant Disclosure”). Notwithstanding the foregoing, Microsoft shall have no obligation to indemnify the data subject under this Section 2 to the extent the data subject has already received compensation for the same damage, whether from Microsoft or otherwise.

3. **Conditions of Indemnification.** Indemnification under Section 2 is conditional upon the data subject establishing, to Microsoft's reasonable satisfaction, that:
- a. Microsoft engaged in a Relevant Disclosure;
  - b. the Relevant Disclosure was the basis of an official proceeding by the non-EU/EEA government body or law enforcement agency against the data subject; and
  - c. the Relevant Disclosure directly caused the data subject to suffer material or non-material damage.

The data subject bears the burden of proof with respect to conditions a. through c.

Notwithstanding the foregoing, Microsoft shall have no obligation to indemnify the data subject under Section 2 if Microsoft establishes that the Relevant Disclosure did not violate its obligations under Chapter V of the GDPR.

4. **Scope of Damages.** Indemnification under Section 2 is limited to material and non material damages as provided in the GDPR and excludes consequential damages and all other damages not resulting from Microsoft's infringement of the GDPR.
5. **Exercise of Rights.** Rights granted to data subjects under this Addendum may be enforced by the data subject against Microsoft irrespective of any restriction in Clauses 3 or 6 of the Standard Contractual Clauses. The data subject may only bring a claim under this Addendum on an individual basis, and not part of a class, collective, group or representative action. Rights granted to data subjects under this Addendum are personal to the data subject and may not be assigned.
6. **Notice of Change.** Microsoft agrees and warrants that it has no reason to believe that the legislation applicable to it or its sub-processors, including in any country to which personal data is transferred either by itself or through a sub-processor, prevents it from fulfilling the instructions received from the Customer and its obligations under this Addendum or the 2021 Standard Contractual Clauses and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by this Addendum or the Standard Contractual Clauses, it will promptly notify the change to Customer as soon as it is aware, in which case Customer is entitled to suspend the transfer of data and/or terminate the contract.

## Appendix D – Challenges to Order or Binding Legal Obligation Suspending Online Services

---

By this Appendix, Microsoft provides the following commitments to National, Federal, and Regional Government Customer entities of the European Union (“EU”) Member States, as well as EU accession countries, members of the European Free Trade Association, the United Kingdom, Monaco, the Vatican, and the European Commission (“Protected Government Customer”).

1. In the event that Microsoft receives an order or is otherwise subject to a binding legal obligation from any government, agency, commission, or quasi-governmental body requiring Microsoft to suspend or cease the provision, in whole or in part, of Online Services (including, but not limited to, the provision of Microsoft Azure Services, Microsoft Dynamics 365 Services, or Office 365 Services) to the Protected Government Customer – Microsoft, on behalf of itself and its Affiliates, shall:
  - a. use available means to secure the voluntary withdrawal, revocation, or rescission of such order; and
  - b. use all lawful efforts to challenge the order in the courts of the country whose government issued the order on the basis of any legal deficiencies under the laws of the ordering party or any relevant conflicts with applicable law of the European Union or applicable law of the countries listed above.

Microsoft will seek permanent and interim injunctive relief if needed to ensure the continuous and uninterrupted provision of the relevant Online Services pending the full and final adjudication of lawful efforts to challenge the order or other binding legal obligation referred to above.

2. Rights granted to Customer under this provision are personal to the Protected Government Customer and may not be assigned.

# Attachment 1 – European Union General Data Protection Regulation Terms

---

Microsoft makes the commitments in these GDPR Terms, to all customers effective May 25, 2018. These commitments are binding upon Microsoft with regard to Customer regardless of (1) the version of the Product Terms and DPA that is otherwise applicable to any given Product subscription or license, or (2) any other agreement that references this attachment.

For purposes of these GDPR Terms, Customer and Microsoft agree that Customer is the controller of Personal Data and Microsoft is the processor of such data, except when Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor. These GDPR Terms apply to the processing of Personal Data, within the scope of the GDPR, by Microsoft on behalf of Customer. These GDPR Terms do not limit or reduce any data protection commitments Microsoft makes to Customer in the Product Terms or other agreement between Microsoft and Customer. These GDPR Terms do not apply where Microsoft is a controller of Personal Data.

## Relevant GDPR Obligations: Articles 5, 28, 32, and 33

1. Microsoft supports Customer's accountability obligations via this DPA and the product documentation provided to Customer, and will continue to do so during the term of the term of Customer's subscription or the applicable Professional Services engagement pursuant to subsection 3(h) below. (Article 5(2))
2. Microsoft shall not engage another processor without prior specific or general written authorisation of Customer. In the case of general written authorisation, Microsoft shall inform Customer of any intended changes concerning the addition or replacement of other processors, thereby giving Customer the opportunity to object to such changes. (Article 28(2))
3. Processing by Microsoft shall be governed by these GDPR Terms under European Union (hereafter "Union") or Member State law and are binding on Microsoft with regard to Customer. The subject-matter and duration of the processing, the nature and purpose of the processing, the type of Personal Data, the categories of data subjects and the obligations and rights of the Customer are set forth in the Customer's licensing agreement, including these GDPR Terms. In particular, Microsoft shall:
  - a. process the Personal Data only on documented instructions from Customer, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by Union or Member State law to which

Microsoft is subject; in such a case, Microsoft shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

- b. ensure that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- c. take all measures required pursuant to Article 32 of the GDPR;
- d. respect the conditions referred to in paragraphs 2 and 4 for engaging another processor;
- e. taking into account the nature of the processing, assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Customer's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;
- f. assist Customer in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, taking into account the nature of processing and the information available to Microsoft;
- g. at the choice of Customer, delete or return all the Personal Data to Customer after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the Personal Data;
- h. make available to Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR and allow for and contribute to audits, including inspections, conducted by Customer or another auditor mandated by Customer.

Microsoft shall immediately inform Customer if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. (Article 28(3))

- 4. Where Microsoft engages another processor for carrying out specific processing activities on behalf of Customer, the same data protection obligations as set out in these GDPR Terms shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. Where that other processor fails to fulfil its data protection obligations, Microsoft shall remain fully liable to the Customer for the performance of that other processor's obligations. (Article 28(4))
- 5. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Customer and Microsoft shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- a. the pseudonymisation and encryption of Personal Data;
  - b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
  - c. the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
  - d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. (Article 32(1))
6. In assessing the appropriate level of security, account shall be taken of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. (Article 32(2))
7. Customer and Microsoft shall take steps to ensure that any natural person acting under the authority of Customer or Microsoft who has access to Personal Data does not process them except on instructions from Customer, unless he or she is required to do so by Union or Member State law. (Article 32(4))
8. Microsoft shall notify Customer without undue delay after becoming aware of a Personal Data breach. (Article 33(2)). Such notification will include that information a processor must provide to a controller under Article 33(3) to the extent such information is reasonably available to Microsoft.

# Data Processing Agreement

Where you are not a consumer, you confirm that you have authority to bind the business on behalf of which you are accepting the terms of this agreement.

Please read these terms carefully, as they contain legal obligations and important terms which we will rely upon.

## BACKGROUND

The Customer and n8n entered into a set of terms and conditions for the provision of the n8n workflow automation platform ("**Terms of Service**") that may require n8n to process Personal Data on behalf of the Customer.

This Data Processing Agreement ("**Agreement**"):

- sets out the additional terms, requirements and conditions on which n8n will process Personal Data on behalf of the Customer;
- contains the mandatory clauses required by Article 28(3) of the General Data Protection Regulation ((EU) 2016/679) for contracts between Controllers and Processors; and
- contains the SCCs (available in full here [https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers\\_en](https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en)) and completed as described in Annex I, as well as additional supplementary measures in connection with the SCCs which the parties have included to take account of the recommendations provided by the European Data Protection Board in June 2021.

## AGREED TERMS

### 1 DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this Agreement.

#### 1.1 Definitions:

**"Authorised Persons"** the persons or categories of persons identified in Appendix A.

**"Business Purposes"** means the services described in the Terms of Service or any other purpose specifically identified in Appendix A.

**"Controller" and "Processor"** as defined in the Data Protection Legislation.

**"Customer"** means you, the person or business entering into this Agreement.

**"Data Protection Legislation"** means the General Data Protection Regulation ((EU) 2016/679); the UK GDPR; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) and all other legislation and





regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data;

**"Data Subject"** means an individual who is the subject of Personal Data.

**"n8n"** means N8N GMBH trading as **n8n** incorporated and registered in Germany with company number HRB 212509 B whose registered office is at Novalisstraße 10 10115 Berlin, Germany.

**"Personal Data"** means any information relating to an identified or identifiable natural person that is processed by n8n as a result of, or in connection with, the provision of the services under the Terms of Service; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**"Personal Data Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.

**"Processing, processes and process"** means either any activity that involves the use of Personal Data or as the Data Protection Legislation may otherwise define processing, processes or process. It includes any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Processing also includes transferring Personal Data to third parties.

**"Sensitive Personal Data"** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data processed for uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, as defined in Article 9 of the GDPR.

**"Standard Contractual Clauses (SCC)"** means the Standard Contractual Clauses issued pursuant to the EU Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at [https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers\\_en](https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en) and completed as described in Annex I.

**"UK GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

- 1.2 This Agreement is subject to the Terms of Service and is incorporated into the Terms of Service. Interpretations and defined terms set forth in the Terms of Service apply to the interpretation of this Agreement.
- 1.3 The Annexes form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Annexes.



- 1.4 A reference to writing or written includes email but not fax.
- 1.5 In the case of conflict or ambiguity between:
  - 1.5.1 any provision contained in the body of this Agreement and any provision contained in the Appendices, the provision in the body of this Agreement will prevail;
  - 1.5.2 the terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Appendices, the provision contained in the Appendices will prevail;
  - 1.5.3 any of the provisions of this Agreement and the provisions of the Terms of Service, the provisions of this Agreement will prevail; and
  - 1.5.4 any of the provisions of this Agreement and any executed SCC, the provisions of the executed SCC will prevail.

## **2 PERSONAL DATA TYPES AND PROCESSING PURPOSES**

- 2.1 The Customer and n8n intend that the Customer is the Controller and n8n is the Processor.
- 2.2 The Customer retains control of the Personal Data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to n8n.
- 2.3 The Customer warrants and represents that n8n's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Customer will comply with the Data Protection Legislation.
- 2.4 Appendix A describes the subject matter, duration, nature and purpose of processing and the Personal Data categories and Data Subject types in respect of which n8n may process to fulfil the Business Purposes of the Terms of Service. This Agreement only applies to such Processing. If the Customer intends to process Sensitive Personal Data using the n8n platform, the Customer must provide written notice to n8n and ensure that any such processing complies with applicable Data Protection Legislation. The Customer is solely responsible for providing specific processing instructions for such data.

## **3 N8N'S OBLIGATIONS**

- 3.1 n8n will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Customer's written instructions from Authorised Persons. n8n will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation. n8n must immediately notify the Customer if, in its opinion, the Customer's instruction would not comply with the Data Protection Legislation.
- 3.2 n8n must promptly comply with any Customer request or instruction from Authorised Persons requiring n8n to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.
- 3.3 n8n will maintain the confidentiality of all Personal Data and will not disclose Personal Data to third parties unless the Customer or this Agreement specifically authorises the disclosure, or as required by law. If a law, court, regulator or supervisory authority requires n8n to process or disclose Personal Data, n8n must first inform the Customer of the legal or regulatory requirement and give the Customer an opportunity to object or challenge the requirement, unless the law prohibits such notice.



3.4 n8n will reasonably assist the Customer with meeting the Customer's compliance obligations under the Data Protection Legislation, taking into account the nature of n8n's processing and the information available to n8n, including in relation to Data Subject rights, data protection impact assessments and reporting to and consulting with supervisory authorities under the Data Protection Legislation.

3.5 n8n must promptly notify the Customer of any changes to Data Protection Legislation that may adversely affect n8n's performance of the Terms of Service.

#### **4 N8N'S EMPLOYEES**

4.1 n8n will ensure that all employees:

4.1.1 are informed of the confidential nature of the Personal Data and are bound by confidentiality obligations and use restrictions in respect of the Personal Data;

4.1.2 have undertaken training on the Data Protection Legislation relating to handling Personal Data and how it applies to their particular duties; and

4.1.3 are aware both of n8n's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

#### **5 SECURITY**

5.1 n8n must at all times implement appropriate technical and organisational measures against unauthorised or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data including, but not limited to, the security measures set out in Annex II. n8n must document those measures in writing and periodically review them to ensure they remain current and complete, at least annually.

5.2 n8n must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

5.2.1 the pseudonymisation and encryption of personal data;

5.2.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.2.3 the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

5.2.4 a process for regularly testing, assessing and evaluating the effectiveness of security measures.

#### **6 PERSONAL DATA BREACH**

6.1 n8n will promptly and without undue delay notify the Customer if any Personal Data is lost or destroyed or becomes damaged, corrupted, or unusable. n8n will restore such Personal Data at its own expense.

6.2 n8n will notify the Customer without undue delay and, where feasible, no later than 72 hours after becoming aware of:

6.2.1 any accidental, unauthorised or unlawful processing of the Personal Data; or

6.2.2 any Personal Data Breach.



- 6.3 Where n8n becomes aware of an event within the scope of clause 6.2, it shall, without undue delay, also provide the Customer with the following information:
- 6.3.1 a description of the nature of such event, including the categories and approximate number of both Data Subjects and Personal Data records concerned;
  - 6.3.2 the likely consequences of the event; and
  - 6.3.3 a description of the measures taken or proposed to be taken to address such event, including measures to mitigate its possible adverse effects.
- 6.4 Immediately following any unauthorised or unlawful Personal Data processing or Personal Data Breach, the parties will co-ordinate with each other to investigate the matter. n8n will reasonably co-operate with the Customer in the Customer's handling of the matter, including:
- 6.4.1 assisting with any investigation;
  - 6.4.2 making available all relevant records, logs, files, data reporting and other materials required to comply with all Data Protection Legislation or as otherwise reasonably required by the Customer; and
  - 6.4.3 taking reasonable and prompt steps to mitigate the effects and to minimise any damage resulting from the Personal Data Breach or unlawful Personal Data processing.
- 6.5 n8n will not inform any third party of any Personal Data Breach without first obtaining the Customer's prior written consent, except when required to do so by law.
- 6.6 n8n agrees that the Customer has the sole right to determine:
- 6.6.1 whether to provide notice of the Personal Data Breach to any Data Subjects, supervisory authorities, regulators, law enforcement agencies or others, as required by law or regulation or in the Customer's discretion, including the contents and delivery method of the notice; and
  - 6.6.2 whether to offer any type of remedy to affected Data Subjects, including the nature and extent of such remedy.
- 6.7 n8n will cover all reasonable expenses associated with the performance of its obligations under clause 6.2 and clause 6.4 unless the matter arose from the Customer's specific instructions, negligence, wilful default or breach of this Agreement, in which case the Customer will cover all reasonable expenses of both parties.

## 7 CROSS-BORDER TRANSFERS OF PERSONAL DATA

- 7.1 If an adequate protection measure for the international transfer of Personal Data is required under applicable data protection legislation (and has not otherwise been arranged by the parties) the SCCs as shown at [https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers\\_en](https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en) shall be considered a part of this Agreement as if they had been set out in full. For data transfers subject to UK GDPR, the parties shall incorporate the UK Addendum to the SCCs issued by the UK Information Commissioner's Office. Where applicable, the Addendum shall be deemed appended to this Agreement.



- 7.2 The Customer consents to n8n (and its subcontractors) transferring Personal Data outside the European Economic Area ("EEA"). Provided that where such Processing occurs, n8n:
- 7.2.1 is processing Personal Data in a territory which is subject to a current finding by the European Commission under the Data Protection Legislation that the territory provides adequate protection for the privacy rights of individuals; or
  - 7.2.2 participates in a valid cross-border transfer mechanism under the Data Protection Legislation, so that n8n (and, where appropriate, the Customer) can ensure that appropriate safeguards are in place to ensure an adequate level of protection with respect to the privacy rights of individuals as required by Article 46 of the General Data Protection Regulation ((EU) 2016/679). n8n must identify in Appendix A the transfer mechanism that enables the parties to comply with these cross-border data transfer provisions and n8n must immediately inform the Customer of any change to that status; or
  - 7.2.3 ensures that the transfer otherwise complies with the Data Protection Legislation, in particular Art. 44 and subsequent of the GDPR.
- 7.3 The Customer consents to appointment by n8n of a subcontractor located outside of the EEA in compliance with clause 7.2 and authorises n8n to enter into SCCs with the subcontractor. n8n will make the executed SCCs available to the Customer on request.
- 8 SUBCONTRACTORS**
- 8.1 The Customer consents to n8n appointing subcontractors for the purposes of providing the Platform, the current list of which can be found [here](#). n8n shall inform the Customer of any intended changes concerning the addition or replacement of any subcontractor therefore giving the Customer the opportunity to object in accordance with clause 8.3 below.
- 8.2 When appointing subcontractors n8n shall:
- 8.2.1 enter into a written contract with the subcontractor that contains terms similar to those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request and at the Customer's expense, provides the Customer with copies of such contracts (subject to redaction of any confidential information);
  - 8.2.2 maintain control over all Personal Data it entrusts to the subcontractor; and
  - 8.2.3 ensure the subcontractor's contract terminates automatically on termination of this Agreement for any reason.
- 8.3 In the event the Customer objects to the appointment or replacement of a subcontractor, the Customer may terminate their account on the Platform or where possible agree with n8n to terminate access to the relevant part of the Service affected by the addition of the new subcontractor. For the avoidance of doubt this will be the Customer's sole and exclusive remedy.
- 8.4 Where the subcontractor fails to fulfil its obligations under such written agreement, n8n remains fully liable to the Customer for the subcontractor's performance of its agreement obligations.



## **9 COMPLAINTS, DATA SUBJECT REQUESTS AND THIRD-PARTY RIGHTS**

9.1 n8n must, at no additional cost, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Customer as the Customer may reasonably require, to enable the Customer to comply with:

9.1.1 the rights of Data Subjects under the Data Protection Legislation, including subject access rights, the rights to rectify and erase personal data, object to the processing and automated processing of personal data, and restrict the processing of personal data; and

9.1.2 information or assessment notices served on the Customer by any supervisory authority under the Data Protection Legislation.

9.2 n8n must notify the Customer immediately if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 n8n must notify the Customer without undue delay if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their related rights under the Data Protection Legislation.

9.4 n8n will give the Customer its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request.

9.5 n8n must not disclose the Personal Data to any Data Subject or to a third party other than at the Customer's request or instruction, as provided for in this Agreement or as required by law.

## **10 TERM AND TERMINATION**

10.1 This Agreement will remain in full force and effect so long as:

10.1.1 the Terms of Service remain in effect; or

10.1.2 n8n retains any Personal Data related to the Terms of Service in its possession or control ("**Term**").

10.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Terms of Service in order to protect Personal Data will remain in full force and effect.

10.3 If a change in any Data Protection Legislation prevents either party from fulfilling all or part of its Terms of Service obligations, the parties will suspend the processing of Personal Data until that processing complies with the new requirements. If the parties are unable to bring the Personal Data Processing into compliance with the Data Protection Legislation within 30 days, they may terminate the Terms of Service on written notice to the other party.

## **11 DATA RETURN AND DESTRUCTION**

11.1 At the Customer's request, n8n will give the Customer a copy of or access to all or part of the Customer's Personal Data in its possession or control in a commonly accessible and electronic format determined by n8n.

11.2 On termination of the Terms of Service for any reason or expiry of its term, n8n will promptly securely delete or destroy or, if directed in writing by the Customer, return and not retain, all or any Personal Data related to this Agreement in its possession or control. This requirement shall not apply to Personal Data which n8n has archived on its backup systems which are not reasonably accessible, provided that such Personal Data is





deleted promptly in the event such backups become reasonably accessible (such as by n8n using those backups to restore its systems).

- 11.3 Clause 11.2 shall not apply to the extent any law, regulation, or government or regulatory body requires n8n to retain any documents or materials that n8n would otherwise be required to return or destroy.

## **12 RECORDS**

- 12.1 n8n will keep detailed, accurate and up-to-date written records regarding any processing of Personal Data it carries out for the Customer, including but not limited to, the access, control and security of the Personal Data, approved subcontractors and affiliates, the processing purposes, categories of processing, any transfers of personal data to a third country and related safeguards, and a general description of the technical and organisational security measures referred to in clause 5.1 ("**Records**").

- 12.2 n8n will ensure that the Records are sufficient to enable the Customer to verify n8n's compliance with its obligations under this Agreement and n8n will provide the Customer with copies of the Records upon request.

## **13 AUDIT**

- 13.1 No more than once during any consecutive 12 month period, on request from the Customer n8n will carry out an audit (whether by itself or its third-party representatives) to audit its compliance with this Agreement and provide the results to the Customer. Customer shall be entitled to ask questions of n8n related to compliance with Data Protection Legislation in advance of the audit, with n8n shall use its reasonable endeavours to respond to adequately when providing the audit results.

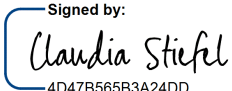
- 13.2 On the Customer's written request and at the Customer's cost, n8n will exercise relevant audit rights it has in connection with its subcontractors' compliance with their obligations regarding the Customer's Personal Data and provide the Customer with the audit results.

- 13.3 The audit rights set out at clauses 13.1 – 13.2 are the Customer's only contractual rights (and n8n's only obligations) in connection with the auditing of n8n's Processing of Personal Data. Save that nothing in this Agreement shall prevent or is intended to undermine the rights and powers granted to Data Subjects or Supervisory Authorities, and accordingly n8n shall submit to any audits required by a Supervisory Authority or Data Protection Law.



The parties' authorized signatories have duly executed this Agreement.

ON BEHALF OF N8N:

|                          |                                                                                                                                 |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| NAME                     | claudia stiefel, VP operations                                                                                                  |
| COMPANY NAME AND ADDRESS | n8n GmbH, Novalisstr. 10, 10115 Berlin                                                                                          |
| SIGNED                   | <div>Signed by:<br/><br/>4D47B565B3A24DD</div> |

ON BEHALF OF THE CUSTOMER:

|                          |  |
|--------------------------|--|
| CONTACT PERSON NAME      |  |
| CONTACT PERSON POSITION  |  |
| CONTACT PERSON EMAIL     |  |
| COMPANY NAME AND ADDRESS |  |
| SIGNED                   |  |
| DATE                     |  |



**Appendix A****PERSONAL DATA PROCESSING PURPOSES AND DETAILS****1****DATA PROCESSING PURPOSES AND DETAILS**

|                                                         |                                                                                                                                                                            |
|---------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Subject matter of processing:</b>                    | n8n operates a workflow automation tool which enables customers to sync, transfer and transform data between different third-party services                                |
| <b>Duration of Processing:</b>                          | The processing of personal data shall endure for the duration of the customer's subscription term                                                                          |
| <b>Nature of Processing:</b>                            | n8n provides its service to the Customer to facilitate the automation of workflows                                                                                         |
| <b>Business Purposes:</b>                               | The automation of internal business processes                                                                                                                              |
| <b>Personal Data Categories:</b>                        | Name, email address, password, billing address, credit card information, IP Address, API Key, access token, user identifiers, integration configuration, API logs, cookies |
| <b>Data Subject Types:</b>                              | The data controller may at its discretion submit personal data about subjects including but not limited to: employees, customers, vendors, service providers               |
| <b>Authorised Persons:</b>                              | The holder of the n8n account.                                                                                                                                             |
| <b>n8n's legal basis for Processing outside the EEA</b> | Standard Contractual Clauses                                                                                                                                               |



## ANNEX I

We incorporate the SCCs by reference. Where there is a choice of governing law or a choice of forum and jurisdiction, we use Germany.

### A. LIST OF PARTIES

#### Data exporter

**Name:** The exporter is the Customer specified in the Agreement

**Address:** specified in the Agreement

**Contact person's name, position and contact details:** specified in the Agreement

**Activities relevant to the data transferred under these Clauses:** processing data in relation to n8n's terms of service

**Role:** Controller

**Signed:** \_\_\_\_\_

#### Data importers

**Name:** n8n GmbH

**Address:** Novalisstr. 10, 10115 Berlin

**Contact person's name, position and contact details:** Jan Oberhauser, available at [privacy@n8n.io](mailto:privacy@n8n.io)

**Activities relevant to the data transferred under these Clauses:** processing data in relation to our Terms of Service

**Role:** Processor

**Signed:**  \_\_\_\_\_  
4D47B565B3A24DD...

### B. DESCRIPTION OF TRANSFER

#### MODULE TWO: Controller-to-Processor

#### Categories of data subjects whose personal data is transferred

Data subjects whose Personal Data is uploaded or otherwise provided by the data exporter to n8n.

#### Categories of personal data transferred



Personal Data that is submitted to n8n by the exporter. The categories of Personal Data are determined and controlled by the data exporter in its sole discretion.

**Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.**

None anticipated.

**The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).**

Continuously, for the length of the Agreement between the parties.

#### **Nature of the processing**

Personal Data transferred will be processed to (i) provide the n8n's product to the data exporter and fulfil the data importer's obligations under the Agreement; and (ii) comply with applicable law

#### **Purpose(s) of the data transfer and further processing**

Personal Data transferred will be processed to (i) provide n8n's product to the data exporter and fulfil the data importer's obligations under the Agreement; and (ii) comply with applicable law.

**The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period**

Personal Data will be retained for the length of time necessary to provide n8n's product under the Agreement and in accordance with n8n's data retention processes and as otherwise required by applicable law.

**For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing**

n8n's sub-processors will process Personal Data to assist n8n in providing its product pursuant to the Agreement, for as long as needed for n8n to provide its product.

### **C. COMPETENT SUPERVISORY AUTHORITY**

The Berlin Commissioner for Data Protection and Freedom of Information

## ANNEX II

### **TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

A description of n8n's technical and organisational security measures can be found [here](#). n8n will not materially decrease the overall security of the service during a subscription term, and will notify the Customer of any substantial changes.

Sample

## ANNEX III

### LIST OF SUB-PROCESSORS

A list of sub-processors, together with a form to subscribe to updates about them can be found [here](#).

Sample

## Google Cloud Platform, Workspace, Cloud Identity & Implementation Services: EU Standard Contractual Clauses (Module 3: Processor-to-Processor)

Capitalized terms used but not defined in these Clauses (including the Appendix) have the meanings given to them in the agreement into which these Clauses are incorporated (the "Agreement"). If the Agreement relates to the resale or supply of Google Cloud Platform under a Google Cloud partner or reseller program, then all references in these Clauses to Customer mean Partner.

### STANDARD CONTRACTUAL CLAUSES

#### SECTION I

##### *Clause 1*

##### **Purpose and scope**

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) <sup>(1)</sup> for the transfer of personal data to a third country.

(b) The Parties:

- (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
- (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

## ***Clause 2***

### **Effect and invariability of the Clauses**

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

## ***Clause 3***

### **Third-party beneficiaries**

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
- (ii) Clause 8 – Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
- (iii) Clause 9 – Clause 9(a), (c), (d) and (e);
- (iv) Clause 12 – Clause 12(a), (d) and (f);
- (v) Clause 13;
- (vi) Clause 15.1(c), (d) and (e);
- (vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b);

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

#### ***Clause 4***

##### **Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

#### ***Clause 5***

##### **Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### ***Clause 6***

##### **Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

#### ***Clause 7 – Not used***

## **SECTION II – OBLIGATIONS OF THE PARTIES**

#### ***Clause 8***

##### **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.



## **8.1 Instructions**

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter (<sup>5</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntr5-L\\_2021199EN.01003701-E0005](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntr5-L_2021199EN.01003701-E0005))

).

## **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

## **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

## **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

### **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

### **8.6 Security of processing**

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

## **8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

## **8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (<sup>6</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntr6-L\\_2021199EN.01003701-E0006](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntr6-L_2021199EN.01003701-E0006))

) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

## **8.9 Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical

facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

## **Clause 9**

### **Use of sub-processors**

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. <sup>(9)</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntr9-L\\_2021199EN.01003701-E0009](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntr9-L_2021199EN.01003701-E0009))

) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

## ***Clause 10***

### **Data subject rights**

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

## ***Clause 11***

### **Redress**

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to

Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

## **Clause 12**

### **Liability**

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.



(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### ***Clause 13***

#### **Supervision**

(a) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### **SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### ***Clause 14***

##### **Local laws and practices affecting compliance with the Clauses**

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures



authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards <sup>(12)</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntr12-L\\_2021199EN.01003701-E0012](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntr12-L_2021199EN.01003701-E0012))

);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## ***Clause 15***

### **Obligations of the data importer in case of access by public authorities**

#### **15.1 Notification**

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract,

with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## **15.2 Review of legality and data minimisation**

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## **SECTION IV – FINAL PROVISIONS**

### ***Clause 16***

#### **Non-compliance with the Clauses and termination**

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

## **Clause 17**

## Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

### **Clause 18**

#### **Choice of forum and jurisdiction**

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Ireland.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

(<sup>1</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc1-L\\_2021199EN.01003701-E0001](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc1-L_2021199EN.01003701-E0001))

) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(<sup>2</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc2-L\\_2021199EN.01003701-E0002](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc2-L_2021199EN.01003701-E0002))

) Not applicable

(<sup>3</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc3-L\\_2021199EN.01003701-E0003](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc3-L_2021199EN.01003701-E0003))

) Not applicable

<sup>(4)</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc4-L\\_2021199EN.01003701-E0004](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc4-L_2021199EN.01003701-E0004))

) Not applicable

<sup>(5)</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc5-L\\_2021199EN.01003701-E0005](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc5-L_2021199EN.01003701-E0005))

) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

<sup>(6)</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc6-L\\_2021199EN.01003701-E0006](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc6-L_2021199EN.01003701-E0006))

) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

<sup>(7)</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc7-L\\_2021199EN.01003701-E0007](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc7-L_2021199EN.01003701-E0007))

) Not applicable

<sup>(8)</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc8-L\\_2021199EN.01003701-E0008](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc8-L_2021199EN.01003701-E0008))

) Not applicable

<sup>(9)</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc9-L\\_2021199EN.01003701-E0009](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc9-L_2021199EN.01003701-E0009))

) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

<sup>(10)</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc10-L\\_2021199EN.01003701-E0010](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc10-L_2021199EN.01003701-E0010))

) Not applicable

<sup>(11)</sup>

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc11-L\\_2021199EN.01003701-E0011](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc11-L_2021199EN.01003701-E0011))

) Not applicable

([https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc12-L\\_2021199EN.01003701-E0012](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en#ntc12-L_2021199EN.01003701-E0012))

) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

## **APPENDIX**

### **EXPLANATORY NOTE:**

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

## **ANNEX I**

### **A. LIST OF PARTIES**

#### **Data exporter(s):**

Name: Customer

Address: As specified in the Agreement.

Contact person's name, position and contact details: Contact details for the data exporter are specified in the Agreement. Details about the data exporter's data protection officer are available to the data importer in the Admin Console for Google Cloud Platform, Google Workspace or Cloud Identity (where such details have been provided by the data exporter).

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Agreement. Those Services may include advisory, consulting or implementation services if ordered by the data exporter from the data importer in relation to Google Cloud Platform, Google Workspace or Cloud Identity ("Implementation Services").

Signature and date: The parties agree that execution of the Agreement and certification by the data exporter in relation to Google Cloud Platform, Google Workspace or Cloud Identity under Section 10.3 of the Cloud Data Processing Addendum (Customers) at <https://cloud.google.com/terms/data-processing-addendum> (/terms/data-processing-addendum) ("CDPA (Customers)") or the Cloud Data Processing Addendum (Partners) at <https://cloud.google.com/terms/partners-data-processing-addendum> (/terms/partners-data-processing-addendum) (<https://cloud.google.com/terms/data-processing-terms/partner>) ("CDPA (Partners)"), as applicable, shall constitute execution of these Clauses by both parties.

Role (controller/processor): processor

**Data importer(s):**

Name: Google

Address: As specified in the Agreement.

Contact person's name, position and contact details: Contact details for the data importer are specified in the Agreement. The data importer's data protection team can be contacted as described in the CDPA (Customers) or the CDPA (Partners), as applicable.

Activities relevant to the data transferred under these Clauses: The data importer provides the Services, including any applicable Implementation Services, to the data exporter in accordance with the Agreement.

Signature and date: The parties agree that execution of the Agreement and certification by the data exporter in relation to Google Cloud Platform, Google Workspace or Cloud Identity under Section 10.3 of the CDPA (Customers) or the CDPA (Partners), as applicable, shall constitute execution of these Clauses by both parties.

Role (controller/processor): processor

**B. DESCRIPTION OF TRANSFER**

*Categories of data subjects whose personal data is transferred*



Data subjects are the individuals whose personal data is processed by the data importer under the data exporter's instructions as specified in the Agreement ("Transferred Personal Data"). These individuals may include, for example: employees, other staff such as contractors and temporary workers, customers and clients (including their staff), other end users, suppliers (including their staff), relatives and associates of the above, advisers, consultants and other professional experts, shareholders, members or supporters, and students and pupils.

#### *Categories of personal data transferred*

Transferred Personal Data may include, for example:

- Personal details, including any information that identifies the data subject and their personal characteristics, including: name, address, contact details, age, date of birth, sex, and physical description.
- Employment details, including information relating to the employment of the data subject, including employment and career history, recruitment and termination details, attendance records, performance appraisals, training records, and security records.
- Financial details, including information relating to the financial affairs of the data subject, including income, salary, assets and investments, payments, creditworthiness, loans, benefits, grants, insurance details, and pension information.
- Education and training details, including information which relates to the education and any professional training of the data subject, including academic records, qualifications, skills, training records, professional expertise, student and pupil records.
- Personal details issued as an identifier by a public authority, including passport details, national insurance numbers, identity card numbers, driving licence details.
- Family, lifestyle and social circumstances, including any information relating to the family of the data subject and the data subject's lifestyle and social circumstances, including details of family and other household members, habits, housing, travel details, leisure activities, and membership of charitable or voluntary organisations.

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff*

*having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

Transferred Personal Data may include special categories of personal data (as defined in the GDPR). This may include, for example: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

The restrictions and safeguards specified in Annex II apply to these categories of personal data (if any).

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

Transferred Personal Data may be transferred on a continuous basis until it is deleted in accordance with the terms of the CDPA (Customers) or the CDPA (Partners), as applicable.

*Nature of the processing*

The data importer will process Transferred Personal Data to provide, secure and monitor the Services and any applicable TSS in accordance with the Agreement.

*Purpose(s) of the data transfer and further processing*

The data importer will process Transferred Personal Data to provide, secure and monitor the Services and any applicable TSS in accordance with the Agreement.

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

The data importer will retain Transferred Personal Data until its deletion in accordance with the provisions of the CDPA (Customers) or the CDPA (Partners), as applicable.

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

As above.

## **C. COMPETENT SUPERVISORY AUTHORITY**

*Identify the competent supervisory authority/ies in accordance with Clause 13*

The authority identified by the data exporter as its competent supervisory authority via the Admin Console for Google Cloud Platform, Google Workspace or Cloud Identity.

## **ANNEX II**

### **TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

The data importer will implement and maintain security standards at least as protective as those set out in Appendix 2 of the CDPA (Customers), the CDPA (Partners), or a Data Processing Addendum for any Implementation Services, as applicable.

The technical and organisational measures to be taken by sub-processors are described in the "Subprocessor Security" section of that Appendix.

The technical and organisational measures to be taken by the data importer to assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 are set out in Sections 8 (Impact Assessments and Consultations) and 9 (Access etc.; Data Subject Rights; Data Export) of the CDPA (Customers) or the CDPA (Partners), as applicable.

## **ANNEX III**

### **LIST OF SUB-PROCESSORS**

The controller has authorised the use of the following sub-processors (as applicable):

For Google Cloud Platform Services: the sub-processors at

<https://cloud.google.com/terms/subprocessors>

(<https://cloud.google.com/terms/subprocessors>)

For Google Workspace or Cloud Identity Services: the sub-processors at

<https://workspace.google.com/intl/en/terms/subprocessors.html>

(<https://workspace.google.com/intl/en/terms/subprocessors.html>)

For Implementation Services: (a) those entities listed as subcontractors in an applicable Order Form, Statement of Work, or other confirmation provided to Customer before commencement of the Services; and (b) any other entity whose engagement as a sub-processor has been authorised by Customer in accordance with the Agreement.

## **ANNEX IV**

### **SUPPLEMENTARY TERMS FOR SWISS FDPA TRANSFERS ONLY**

The following terms supplement the Clauses only if and to the extent the Clauses apply with respect to data transfers subject to the Federal Data Protection Act of 19 June 1992 (Switzerland):

1. The term 'Member State' will be interpreted in such a way as to allow data subjects in Switzerland to exercise their rights under the Clauses in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Clauses.
2. If the relevant data transfers are exclusively subject to the Federal Data Protection Act of 19 June 1992 (Switzerland), the competent supervisory authority/ies for purposes of Annex I.C (Competent Supervisory Authority) of the Clauses will be the Federal Data Protection and Information Commissioner in Switzerland (or its replacement or successor).

## **ANNEX V**

### **SUPPLEMENTARY TERMS FOR UK GDPR TRANSFERS ONLY**

The following United Kingdom International Data Transfer Addendum to the European Commission Standard Contractual Clauses supplements the Clauses only if and to the extent the Clauses apply with respect to transfers of personal data subject to the UK GDPR.

#### **International Data Transfer Addendum to the EU Commission Standard Contractual Clauses**

##### **VERSION B1.0, in force 21 March 2022**

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

#### **Part 1: Tables**

**Table 1: Parties**

| <b>Start date</b>                            | (a) 21 September 2022, where the effective date of the Agreement is before 21 September 2022; or<br><br>(b) otherwise, on the effective date of the Agreement.                                     |                                              |                                                 |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-------------------------------------------------|
| <b>The Parties</b>                           | <table><tr><th data-bbox="287 1904 893 2027">Exporter (who sends the Restricted Transfer)</th><th data-bbox="893 1904 1437 2027">Importer (who receives the Restricted Transfer)</th></tr></table> | Exporter (who sends the Restricted Transfer) | Importer (who receives the Restricted Transfer) |
| Exporter (who sends the Restricted Transfer) | Importer (who receives the Restricted Transfer)                                                                                                                                                    |                                              |                                                 |

|                                                              |                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Parties' details</b>                                      | Full legal name: Customer                                                                                                                                                                                                                                                                                                                                            | Full legal name: Google                                                                                                                                                                                                                                                                                          |
|                                                              | Trading name (if different): As specified in the Agreement.                                                                                                                                                                                                                                                                                                          | Trading name (if different): As specified in the Agreement.                                                                                                                                                                                                                                                      |
|                                                              | Main address (if a company registered address): As specified in the Agreement.                                                                                                                                                                                                                                                                                       | Main address (if a company registered address): As specified in the Agreement.                                                                                                                                                                                                                                   |
|                                                              | Official registration number (if any) (company number or similar identifier): As specified in the Agreement.                                                                                                                                                                                                                                                         | Official registration number (if any) (company number or similar identifier): As specified in the Agreement.                                                                                                                                                                                                     |
| <b>Key Contact</b>                                           | Contact details for the data exporter are specified in the Agreement. Details about the data exporter's data protection officer are available to the data importer in the Admin Console for Google Cloud Platform, Google Workspace or Cloud Identity (where such details have been provided by the data exporter).                                                  | Contact details for the data importer are specified in the Agreement. The data importer's data protection team can be contacted as described in the CDPA (Customers) or the CDPA (Partners), as applicable.                                                                                                      |
| <b>Signature (if required for the purposes of Section 2)</b> | The Parties agree that execution of the Agreement and certification by the data exporter in relation to Google Cloud Platform, Google Workspace or Cloud Identity under Section 10.3 of the Cloud Data Processing Addendum (Customers) or the Cloud Data Processing Addendum (Partners), as applicable, shall constitute execution of this Addendum by both Parties. | The Parties agree that execution of the Agreement and certification by the data exporter in relation to Google Cloud Platform, Google Workspace or Cloud Identity under Section 10.3 of the CDPA (Customers) or the CDPA (Partners), as applicable, shall constitute execution of this Addendum by both parties. |

**Table 2: Selected SCCs, Modules and Selected Clauses**

|                         |                                                                                                                             |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <b>Addendum EU SCCs</b> | The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: |
|                         | Date: 4 June 2021                                                                                                           |
|                         | Reference (if any): Module 3: Processor-to-Processor                                                                        |
|                         | Other identifier (if any): N/A                                                                                              |

**Table 3: Appendix Information**

*"Appendix Information"* means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

---

Annex 1A: List of Parties: Annex I(A)

---

Annex 1B: Description of Transfer: Annex I(B)

---

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Annex II

---

Annex III: List of Sub processors (Modules 2 and 3 only): Annex III

---

#### Table 4: Ending this Addendum when the Approved Addendum Changes

---

|                                                         | Which Parties may end this Addendum as set out in Section 19: |
|---------------------------------------------------------|---------------------------------------------------------------|
| Ending this Addendum when the Approved Addendum changes | <input checked="" type="checkbox"/> Importer                  |
|                                                         | <input checked="" type="checkbox"/> Exporter                  |
|                                                         | <input type="checkbox"/> neither Party                        |

---

#### Part 2: Mandatory Clauses

---

|                          |                                                                                                                                                                                                                                                                               |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Mandatory Clauses</b> | Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses. |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

---

#### Part 3: Supplementary Clauses

---

|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Supplementary Clauses</b> | Part 3: Supplementary Clauses of the Approved Addendum, being the following:                                                                                                                                                                                                                                                                                                                                                                       |
|                              | The data importer may not end this Addendum as set out in Section 19 of the Mandatory Clauses unless the data importer has adopted an Alternative Transfer Solution for the Restricted Transfers by the end date. An “Alternative Transfer Solution” for this purpose means a solution, other than Standard Contractual Clauses, that enables the lawful transfer of personal data to a third country in accordance with Chapter V of the UK GDPR. |
|                              | Any written notice provided by the data exporter pursuant to Section 19 of the Mandatory Clauses in order to end this Addendum will be deemed to terminate the Agreement for convenience.                                                                                                                                                                                                                                                          |

---

[April 4, 2022](#)

- (/terms/sccs/eu-p2p/index-20220404)

[September 24, 2021](#)

(/terms/sccs/eu-p2p/index-20210924)

## Data Processing Agreement

[Home](#) | [Terms and Conditions](#) | [Data Processing Agreement](#)

# Data Processing Agreement

*Last Updated: February 14, 2022*

This Data Processing Agreement ("**DPA**") forms part of the OVHcloud Terms of Service (the "**Agreement**") or other written or electronic agreement between **OVH US LLC dba OVHcloud®**, with its principal place of business at

11950 Democracy Drive  
Suite 300  
Reston, VA 20191

("OVHcloud") and **Customer** for the purchase of the OVHcloud Services to reflect the parties' agreement with regard to the Processing of Personal Data and Service Data. All terms not defined herein shall have the meaning ascribed to them in the Agreement.

### 1. **BACKGROUND**

OVHcloud provides certain Services to the Customer in accordance with the Agreement. This DPA sets forth the data protection terms and obligations that apply when OVHcloud Processes Personal Data on behalf of the Customer in the course of providing the OVHcloud Services. The parties have agreed to enter into this DPA to address the rights and obligations that apply to the Customer under the Applicable Data Protection Laws concerning OVHcloud's Processing of Personal Data on behalf of the Customer.

### 2. **DEFINITIONS**

Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:

**"Affiliate"** means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for the purposes of this definition, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity;

**"Applicable Data Protection Laws"** means all applicable legislation relating to the Processing of Personal Data under the Agreement, including without limitation, the United States and its states, the EU Data Protection Directive 95/46/EC and all local laws and regulations which amend or replace any of them, including the GDPR, together with any national implementing laws in any



Member State of the European Union or, to the extent applicable, in any other country, as amended, repealed, consolidated or replaced from time to time;

**"CCPA"** means the California Consumer Privacy Act, Cal. Civ. Code Section 1798.100 et seq., and its implementing regulations.

**"Controller"** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;

**"Data Subject(s)"** means the individual(s) to whom Personal Data relates;

**"EEA"** means the European Economic Area;

**"End Users"** means Customer's customers, prospects, employees, consultants or independent contractors, suppliers and other individuals or third parties;

**"OVHcloud Services"** has the meaning given to it in the Agreement;

**"Personal Data"** means information defined as personal data, personal information, or a similar term by Applicable Data Protection Laws;

**"Processing"** means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction performed upon Personal Data. The terms "Process", "Processes" and "Processed" will be construed accordingly;

**"Processor"** means any natural or legal person which agrees to receive Personal Data from the Controller for the purposes of Processing such data on behalf of the Controller and in accordance with the Controller's written instructions. Any references shall also mean OVHcloud operating as a "service provider," as defined in CCPA Section 1798.140 (v), with respect to the Processing of Service Data;

**"Relationship Data"** means any account-related data provided by the Customer to OVHcloud during the purchase, sign up, use or support of an account. Relationship Data may include Personal Data;

**"Security Breach"** means any accidental or unlawful acquisition, destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data and/or Service Data to the extent it includes Personal Data;

**"Security Measures"** means OVHcloud's technical and organizational measures specified in Section 3(k) of this DPA;

**"Service Data"** means any data (including any Personal Data), the extent of which is determined and controlled by the Customer in its sole discretion, contained in any applications, files, data, information or other content uploaded to or published, displayed or backed up by Customer, or any of its End Users, through the OVHcloud Services, relating to Customer and/or the its employees, customers, suppliers, service providers, business partners, consultants and other End Users. Service Data does not include Usage Data or Relationship Data;

**"Standard Contractual Clauses"** means, (i) with respect to transfers of Personal Data from the EEA and Switzerland, the standard contractual clauses for, as applicable, (a) Controller-to-

Processor or (b) Processor-to-Processor Transfers approved by European Commission Decision of 4 June 2021 and reproduced in Schedules 1 and 2 to this Agreement or, (ii) with respect to transfers of Personal Data from the UK, the standard contractual clauses for the transfer of personal data to processors established in third countries approved by European Commission Decision of 5 February 2010 and reproduced in Schedule 3 to this Agreement;

**"Sub-processor"** means an entity Processing Customer Personal Data on behalf of a Processor;

**"UK"** means the United Kingdom;

**"Usage Data"** means any data (other than Service Data) relating to Customer's use and consumption of the OVHcloud Services, including, without limitation, information about the amount of computing and storage resources purchased or consumed, data relating to the configuration, performance or features of the OVHcloud Services, configuration settings, features accessed, IP addresses, usernames, and performance metrics.

### 3. **PROCESSING OF SERVICE DATA**

- a. **Scope and Role.** The subject-matter of this DPA is the provision of the OVHcloud Services to Customer that involves the Processing of Service Data. The parties acknowledge and agree that with regard to the Processing of Service Data, Customer is the Controller or the Processor, as applicable, and OVHcloud is the Processor or sub-processor, as applicable, and that OVHcloud may engage Sub-processors only pursuant to the requirements set forth in Section 3(m) "Sub-processors" below. OVHcloud will Process Service Data only as a Processor on Customer's behalf and for the purposes of providing the Services as set forth in the Agreement, or as otherwise permitted for processors by Applicable Data Protection Laws. OVHcloud will not disclose Service Data to any third party, except in accordance with this DPA and the Agreement or where required by law.
- b. **Instructions for Data Processing.** OVHcloud will only Process Service Data on Customer's lawful instructions, including with regard to transfers of Service Data to a third country or an international organization, as set forth in this DPA, which Customer agrees constitutes its complete and final instructions to OVHcloud in relation to Processing of Service Data. Processing outside the scope of this DPA (if any) will require the prior written agreement between the parties. To the extent that any change in Customer's instructions for Processing incurs additional fees, Customer agrees to pay to OVHcloud any associated increase in fees for carrying out such instructions, unless the change in the instructions is motivated by a change in the Applicable Data Protection Laws or direct instructions from the competent data protection authority according to the Applicable Data Protection Laws. Upon notice in writing, Customer may terminate this DPA and the Agreement if OVHcloud declines to follow Customer's instructions that are outside the scope of this DPA. If OVHcloud cannot Process the Service Data in accordance with Customer's instructions due to a legal requirement under Applicable Data Protection Laws, OVHcloud shall inform Customer about the legal requirement before Processing the data, unless that law prohibits such information because of important grounds of public interest or an equivalent concept. As a Processor, OVHcloud will Process Service Data only as necessary to perform the Services, and will not collect, use, retain, access, share, sell, transfer, or otherwise Process Service Data for any purpose not related to providing such Services, for any purpose other than as set out in the Agreement, or as otherwise permitted by the CCPA.
- c. **Customer Compliance.** Customer shall, in its use of the Services, Process Service Data, and subsequently issue any Processing instructions to OVHcloud in accordance with the requirements of Applicable Data Protection Laws with respect to Processors, including any applicable requirement to provide notice to Data Subjects and/or End Users of the use of

OVHcloud as a Processor or Sub- Processor.

Customer shall have sole responsibility for the accuracy, quality, and legality of Service Data and the means by which Customer acquired Service Data. This includes obtaining all consents and rights necessary for OVHcloud to Process Service Data in accordance with Applicable Data Protection Laws and this DPA. Customer specifically acknowledges that its use of the Services will not violate the rights of any Data Subject and/or End User that has opted-out from sales or other disclosures of Personal Data, to the extent applicable under Applicable Data Protection Laws.

If Customer is acting as a Processor to a Controller, Customer warrants that Customer's instructions and actions with respect to the relevant Service Data, including Customer's designation of OVHcloud as a Sub-processor, have been authorized by the relevant Controller. Customer shall not instruct OVHcloud to Process or disclose Service Data for any purpose other than as set out in the Agreement, this DPA, or as otherwise agreed in writing between the parties, or as otherwise permitted by Applicable Data Protection Laws.

- d. **Confidentiality.** OVHcloud will ensure that all persons authorized to Process Service Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- e. **Deletion and Retrieval of Service Data.** Before the effective date of the expiration or termination of the Agreement, Customer may retrieve a copy of Service Data and, if Customer elects so, delete Service Data from the OVHcloud Services. For fifteen (15) calendar days following the effective date of the expiration or termination of the Agreement, OVHcloud will enable Customer to retrieve Service Data from OVHcloud's systems, at no additional cost to Customer, provided that (i) prior to the effective date of the expiration or termination of the Agreement Customer notifies OVHcloud via email (directed to [support@corp.ovh.us](mailto:support@corp.ovh.us)) that Customer elects to retrieve the data, and (ii) Customer is in compliance with the Agreement. If Customer does not elect to retrieve Service Data in accordance with the foregoing, OVHcloud is hereby instructed to delete the Service Data promptly upon expiration or termination of the Agreement, unless the applicable law requires storage. If OVHcloud is unable to delete Service Data for technical or other reasons, OVHcloud will apply measures to ensure that Service Data is blocked from any further Processing.
- f. **Third Party Requests for Service Data.** If OVHcloud receives a request from Data Subjects to exercise their rights under Applicable Data Protection Laws with respect to the Service Data (including, but not limited to, the right of access, right to rectification, restriction of Processing, erasure, data portability, object to the Processing, or the right not to be subject to an automated individual decision making), or a Data Subject complaint or request from a competent authority in relation to the Service Data, OVHcloud, to the extent legally permitted, will redirect the third party to the Customer and Customer will be responsible for responding to any such request. OVHcloud will not respond independently to such requests and will provide reasonable assistance to Customer so that Customer can make the information available to the third party. If OVHcloud is required to respond to a court order, warrant, audit or agency action and that occurrence demands that OVHcloud discloses Service Data, OVHcloud will promptly notify Customer in advance and provide Customer with a copy of the demand unless legally prohibited from doing so by applicable law. To the extent that OVHcloud incurs any additional costs associated with third party requests, Customer will reimburse OVHcloud its time and expenses.
- g. **Security Breach.** To the extent OVHcloud becomes aware of a Security Breach, OVHcloud will promptly notify Customer of said Security Breach. OVHcloud will comply with the

Security Breach-related obligations directly applicable to it under the Applicable Data Protection Laws and will provide reasonable assistance to Customer in Customer's compliance with its Security Breach-related obligations.

The obligations herein shall not apply to incidents that are caused by Customer or Customer's End Users.

- h. Data Protection Impact Assessments and Consultations.** OVHcloud will provide reasonable assistance to the Customer during the performance of a data protection impact assessment, and, if applicable, in connection with consultation with the competent data protection authority, if the Customer is required to engage in such activities by Applicable Data Protection Laws and solely to the extent (i) Customer does not otherwise have access to the relevant information, and (ii) such information is available to OVHcloud.
- i. Protected Health Information.** Customer agrees that it will not upload into the OVHcloud Services nor include within Service Data any data which is regulated by the United States Health Insurance Portability and Accountability Act unless Customer has entered into a business associate agreement with OVHcloud.
- j. Data Center Locations.** Customer will select the location where Service Data will be stored. Customer authorizes OVHcloud to store Service Data in the location that it has chosen when purchasing the OVHcloud Services. In the case the Service Data will be Processed in a data center in the EEA or the UK, the Personal Data contained therein will be subject to the GDPR and the complementing EEA member state or UK data protection law, or any other statutory data protection law and regulation applicable to such data that will substitute and repeal such law. By uploading Service Data into the OVHcloud Services, Customer acknowledges and agrees that Service Data may be transferred and accessed from around the world, including to and from the location in which Service Data is maintained.
- k. OVHcloud Security Responsibilities.** OVHcloud is responsible for implementing and maintaining appropriate technical, organizational and security measures, to protect any Service Data processed hereunder against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of Processing. These measures will ensure a level of security appropriate to the risk associated with the Processing activity as required by Applicable Data Protection Laws.
- l. Audit of Technical and Organizational Measures.** Upon request and subject to execution of a non-disclosure agreement in a form acceptable to OVHcloud, OVHcloud will provide an annual examination report issued to it by third-party auditors selected by OVHcloud of its technical and organizational measures. Any further audit will be conducted in accordance with OVHcloud's standard audit procedures as applicable from time to time and at Customer's expense.
- m. Sub-Processing.** Customer agrees that OVHcloud may use Sub-processors to fulfill the contractual obligations under this DPA and the Agreement or to provide certain services on OVHcloud's behalf, such as providing support services. Customer acknowledges and agrees that (a) OVHcloud's Affiliates may be retained as Sub-processors; and, (b) OVHcloud and its Affiliates respectively may engage third-party Sub-processors in connection with the provision of the Services. OVHcloud or its Affiliates have entered into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data and Service Data, should it contain Personal Data, to the extent applicable to the nature of the Services provided by such Sub-processor.

Customer hereby grants OVHcloud general authorization to engage Sub-processors. For the avoidance of doubt, the above authorization constitutes Customer's prior written consent to the Sub-processing by OVHcloud for purposes of Clause 9 of the Standard Contractual Clauses applicable to transfers from the EEA and Switzerland or Clause 11 of the Standard Contractual Clauses applicable to transfers from the UK. A list of the Sub-processors can be found in Annex III of the applicable Standard Contractual Clauses. If OVHcloud engages a Sub-processor to Process any Service Data, OVHcloud will (i) inform Customer of any intended changes concerning the addition or replacement of such Sub-processors, to the greatest extent permitted by applicable law, and Customer will have an opportunity to object to such changes on reasonable grounds within fifteen (15) business days after being notified. If the parties are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party; (ii) keep Customer informed if there is any change to the role or status of the Sub-processor; and (iii) enter into a written agreement with the Sub-processor that imposes on the Sub-processor the same obligations that apply to OVHcloud under the DPA. OVHcloud will be responsible for any breaches of this DPA that are caused by any such Sub-processor.

#### **4. USAGE DATA**

- a. OVHcloud collects and Processes Usage Data: (i) to provide the OVHcloud Services to Customer; (ii) to address technical issues with the OVHcloud Services; (iii) to improve OVHcloud's products and services and provide enhanced customer and technical support services, and personalized customer experience; (iv) as otherwise described in OVHcloud's privacy policy and set out in the Agreement.

#### **5. INTERNATIONAL DATA TRANSFERS**

- a. Customer agrees that OVHcloud may transfer Personal Data to third parties, including third parties established in other jurisdictions, provided that such transfers comply with applicable laws and the provisions of this DPA, including, but not limited to, onward transfer provisions set forth in the Standard Contractual Clauses.
- b. In the case of a transfer of Personal Data from the EEA or Switzerland to a territory outside the EEA or Switzerland which has not been the subject of a finding of an adequate level of protection under Applicable Data Protection Laws, the executed standard contractual clauses attached hereto as Schedule 1 (where Data Exporter acts as a Controller) or Schedule 2 (where Data Exporter acts as a Processor) shall apply.
- c. In the case of a transfer of Personal Data from the UK to a territory outside the UK which has not been the subject of a finding of an adequate level of protection under Applicable Data Protection Laws, the executed Standard Contractual Clauses attached hereto as Schedule 3 shall apply.
- d. In the event the Standard Contractual Clauses referenced in Section 5(b) or 5(c) are amended, replaced, or repealed by the European Commission, the UK, or under Applicable Data Protection Laws, the parties shall work together in good faith to enter into an updated version of the Standard Contractual Clauses (to the extent required), or negotiate in good faith a solution to enable a transfer of Personal Data to be conducted in compliance with Applicable Data Protection Laws.

#### **6. LIABILITY**

- a. Any claims brought under this DPA shall be subject to the terms and conditions, including but not limited to, the exclusions and limitations set forth in the Agreement.
- b. Customer acknowledges that OVHcloud is reliant on the Customer for direction as to the extent to which OVHcloud is entitled to use and Process Service Data on behalf of



Customer in performance of the OVHcloud Services. Consequently, OVHcloud will not be liable under the Agreement for any claim brought by a Data Subject arising from any action or omission by OVHcloud, to the extent that such action or omission resulted directly from the Customer's instructions or from Customer's failure to comply with its obligations under the Applicable Data Protection Laws.

## **7. GENERAL PROVISIONS**

Where applicable, Schedules, Annexes, and Appendices to this DPA will be deemed to be an integral part of this DPA. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control. If there is a conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses will control. In the event the Agreement ends or is terminated, the obligations under this DPA shall cease (save that Sections 3(k) and 3(l) shall continue to apply so long as OVHcloud and/or its Sub-Processors Process Service Data on behalf of Customer).

# **SCHEDULE 1—EEA C-TO-P TRANSFER CLAUSES**

## **SECTION I**

### *Clause 1*

#### **Purpose and scope**

- a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)( ) for the transfer of personal data to a third country.
- b. The Parties:
  - i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A. (hereinafter each 'data exporter'), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each 'data importer').have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

### *Clause 2*

#### **Effect and invariability of the Clauses**

- a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or

additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

- b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### *Clause 3*

#### **Third-party beneficiaries**

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
- i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - ii. Clause 8.1(b), 8.9(a), (c), (d) and (e);
  - iii. Clause 9(a), (c), (d) and (e);
  - iv. Clause 12(a), (d) and (f);
  - v. Clause 13;
  - vi. Clause 15.1(c), (d) and (e);
  - vii. Clause 16(e);
  - viii. Clause 18(a) and (b).
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### *Clause 4*

#### **Interpretation**

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

### *Clause 5*

#### **Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

### *Clause 6*

#### **Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

### *Clause 7 - Optional*

Intentionally left blank.

## **SECTION II - OBLIGATIONS OF THE PARTIES**

### *Clause 8*

## **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

### **a. Instructions**

- i. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- ii. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

### **b. Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

### **c. Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

### **d. Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

### **e. Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

### **f. Security of processing**

- i. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter



'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

- ii. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- iii. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- iv. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

#### **g. Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

#### **h. Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ( ) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

- iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person. Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**i. Documentation and compliance**

- i. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- ii. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- iii. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- iv. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- v. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

*Clause 9*

**Use of sub-processors**

- a. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least fifteen (15) business days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
- b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- c. The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

- e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

#### *Clause 10*

### **Data subject rights**

- a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorized to do so by the data exporter.
- b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

#### *Clause 11*

### **Redress**

- a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - ii. refer the dispute to the competent courts within the meaning of Clause 18.
- d. The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

#### *Clause 12*

### **Liability**

- a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-

processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

- c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

#### *Clause 13*

### **Supervision**

- a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## **SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

**Local laws and practices affecting compliance with the Clauses**

- a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - iii. any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
- f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

**Obligations of the data importer in case of access by public authorities**

## **1. Notification**

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## **2. Review of legality and data minimization**

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
- c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## **SECTION IV – FINAL PROVISIONS**



## **Non-compliance with the Clauses and termination**

- a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - ii. the data importer is in substantial or persistent breach of these Clauses; or
  - iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

### *Clause 17*

## **Governing law**

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of France.

### *Clause 18*

## **Choice of forum and jurisdiction**

- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The Parties agree that those shall be the courts of France.
- c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d. The Parties agree to submit themselves to the jurisdiction of such courts.

Appendix

**ANNEX I**

**A. LIST OF PARTIES**

**[CUSTOMER]**

(the "**data exporter**")

and

**OVH US LLC dba OVHcloud®**

with its principal location at

11950 Democracy Drive  
Suite 300  
Reston, VA 20191

(the "**data importer**")

**B. DESCRIPTION OF TRANSFER**

See Section 3(a), above.

**C. COMPETENT SUPERVISORY AUTHORITY**

Commission nationale de l'informatique et des libertés ("CNIL")

**ANNEX II**

**TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

OVHcloud has taken and will maintain the appropriate administrative, technical, physical and procedural security measures for protection of the security, confidentiality and integrity of the personal data as described on OVHcloud's Data Security webpage, accessible on [us.ovhcloud.com/resources/data-security](https://us.ovhcloud.com/resources/data-security), or otherwise made reasonably available by OVHcloud.

**ANNEX III**

**List of Sub-processors**

**OVHcloud Sub-Processors**

OVHcloud may engage the following entities as Sub-processors to carry out specific data processing activities on behalf of Customers.

| <b>Affiliate Entities</b> | <b>Country</b> |
|---------------------------|----------------|
| OVH SAS                   | France         |
| OVH Hispano               | Spain          |
| OVH SRL                   | Italy          |
| OVH GmbH                  | Germany        |
| OVH Limited               | United Kingdom |



**Affiliate Entities****Country**

|                                              |            |
|----------------------------------------------|------------|
| OVH Hosting Limited                          | Ireland    |
| OVH Hebergement INC                          | Canada     |
| OVH Sp. Zo.o.                                | Poland     |
| OVH Hosting Sistemas Informaticos unipessoal | Portugal   |
| OVH BV                                       | Netherland |
| OVH Singapore PTE Ltd                        | Singapore  |
| OVH Australia PTY Ltd                        | Australia  |
| OVH Tech R&S Private Limited                 | India      |

**Third Party Entities****Country**

|                                  |           |
|----------------------------------|-----------|
| Avalara, Inc.                    | USA       |
| Bigtincan Mobile Pty Ltd.        | Australia |
| Equifax Information Services LLC | USA       |
| FIS                              | USA       |
| Fjord Technologies S.A.S.        | France    |
| Marketo, Inc.                    | USA       |
| Salesforce.com, Inc.             | USA       |
| ServiceNow Inc.                  | USA       |
| Zendesk, Inc.                    | USA       |
| Zuora, Inc.                      | USA       |

## **SCHEDULE 2—EEA P-TO-P TRANSFER CLAUSES**

### **SECTION I**

#### *Clause 1M*

#### **Purpose and scope**

- a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)( ) for the transfer of personal data to a third country.
- b. The Parties:
  - i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A. (hereinafter each 'data exporter'), and
  - ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each 'data importer').

- have agreed to these standard contractual clauses (hereinafter: 'Clauses').
- c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
  - d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

## *Clause 2*

### **Effect and invariability of the Clauses**

- a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
- b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

## *Clause 3*

### **Third-party beneficiaries**

- a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
  - i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - ii. Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
  - iii. Clause 9(a), (c), (d) and (e);
  - iv. Clause 12(a), (d) and (f);
  - v. Clause 13;
  - vi. Clause 15.1(c), (d) and (e);
  - vii. Clause 16(e);
  - viii. Clause 18(a) and (b).
- b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

## *Clause 4*

### **Interpretation**

- a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

## *Clause 5*

### **Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

#### *Clause 6*

##### **Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

#### *Clause 7 - Optional*

Intentionally left blank.

## **SECTION II - OBLIGATIONS OF THE PARTIES**

#### *Clause 8*

##### **Data protection safeguards**

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under these Clauses.

##### **a. Instructions**

- i. The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
- ii. The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
- iii. The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
- iv. The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter( ).

##### **b. Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

##### **c. Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its

content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

**d. Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

**e. Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

**f. Security of processing**

- i. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organizational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- ii. The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorized to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- iii. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including

measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- iv. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

#### **g. Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

#### **h. Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ( ) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;
- iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

#### **i. Documentation and compliance**

- i. The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
- ii. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
- iii. The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
- iv. The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

- v. Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
- vi. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- vii. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

#### *Clause 9*

### **Use of sub-processors**

- a. The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least fifteen (15) business days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).
- b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ( ) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- c. The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

#### *Clause 10*

### **Data subject rights**

- a. The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorized to do so by the controller.
- b. The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organizational measures, taking

into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

- c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

#### *Clause 11*

##### **Redress**

- a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.
- b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
  - i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - ii. refer the dispute to the competent courts within the meaning of Clause 18.
- d. The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
- e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

#### *Clause 12*

##### **Liability**

- a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
- d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the



data subject is entitled to bring an action in court against any of these Parties.

- f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### *Clause 13*

#### **Supervision**

- a. Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behavior is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

## **SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

### *Clause 14*

#### **Local laws and practices affecting compliance with the Clauses**

- a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:



- i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
  - iii. any relevant contractual, technical or organizational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The data exporter shall forward the notification to the controller.
- f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation, if appropriate in consultation with the controller. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## *Clause 15*

### **Obligations of the data importer in case of access by public authorities**

#### **1. Notification**

- a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
  - i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The data exporter shall forward the notification to the controller.

- b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The data exporter shall forward the information to the controller.
- d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

## **2. Review of legality and data minimization**

- a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
- b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. The data exporter shall make the assessment available to the controller.
- c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## **SECTION IV – FINAL PROVISIONS**

### *Clause 16*

#### **Non-compliance with the Clauses and termination**

- a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

- c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
- i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - ii. the data importer is in substantial or persistent breach of these Clauses; or
  - iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.
- e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

#### *Clause 17*

### **Governing law**

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of France.

#### *Clause 18*

### **Choice of forum and jurisdiction**

- a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- b. The Parties agree that those shall be the courts of France.
- c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- d. The Parties agree to submit themselves to the jurisdiction of such courts.

#### Appendix

#### ANNEX I

#### **A. LIST OF PARTIES**

**[CUSTOMER]**

(the "**data exporter**")

and

**OVH US LLC dba OVHcloud®**

with its principal location at

11950 Democracy Drive  
Suite 300  
Reston, VA 20191

(the "**data importer**")

**B. DESCRIPTION OF TRANSFER**

See Section 3(a), above.

**C. COMPETENT SUPERVISORY AUTHORITY**

Commission nationale de l'informatique et des libertés ("CNIL")

ANNEX II

**TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

OVHcloud has taken and will maintain the appropriate administrative, technical, physical and procedural security measures for protection of the security, confidentiality and integrity of the personal data as described on OVHcloud's Data Security webpage, accessible on [us.ovhcloud.com/resources/data-security](https://us.ovhcloud.com/resources/data-security), or otherwise made reasonably available by OVHcloud.

ANNEX III

**List of Sub-processors**

**OVHcloud Sub-Processors**

OVHcloud may engage the following entities as Sub-processors to carry out specific data processing activities on behalf of Customers.

| <b>Affiliate Entities</b>                    | <b>Country</b> |
|----------------------------------------------|----------------|
| OVH SAS                                      | France         |
| OVH Hispano                                  | Spain          |
| OVH SRL                                      | Italy          |
| OVH GmbH                                     | Germany        |
| OVH Limited                                  | United Kingdom |
| OVH Hosting Limited                          | Ireland        |
| OVH Hebergement INC                          | Canada         |
| OVH Sp. Zo.o.                                | Poland         |
| OVH Hosting Sistemas Informaticos unipessoal | Portugal       |
| OVH BV                                       | Netherland     |
| OVH Singapore PTE Ltd                        | Singapore      |
| OVH Australia PTY Ltd                        | Australia      |

**Affiliate Entities****Country**

|                              |       |
|------------------------------|-------|
| OVH Tech R&S Private Limited | India |
|------------------------------|-------|

**Third Party Entities****Country**

|                                  |           |
|----------------------------------|-----------|
| Avalara, Inc.                    | USA       |
| Bigtincan Mobile Pty Ltd.        | Australia |
| Equifax Information Services LLC | USA       |
| FIS                              | USA       |
| Fjord Technologies S.A.S.        | France    |
| Marketo, Inc.                    | USA       |
| Salesforce.com, Inc.             | USA       |
| ServiceNow Inc.                  | USA       |
| Zendesk, Inc.                    | USA       |
| Zuora, Inc.                      | USA       |

## **SCHEDULE 3—UK STANDARD CONTRACTUAL CLAUSES**

*Clause 1***Definitions**

For the purposes of the Clauses:

- a. 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'Commissioner' shall have the same meaning as in the UK GDPR;
- b. 'the data exporter' means the controller who transfers the personal data;
- c. 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system covered by UK adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 of the Data Protection Act 2018;
- d. 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- e. 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the UK;
- f. 'technical and organizational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

*Clause 2*

## **Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

### *Clause 3*

#### **Third-party beneficiary clause**

- a. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
- b. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
- c. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- d. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

### *Clause 4*

#### **Obligations of the data exporter**

The data exporter agrees and warrants:

- a. that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the Commissioner) and does not violate the applicable data protection law;
- b. that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- c. that the data importer will provide sufficient guarantees in respect of the technical and organizational security measures specified in Appendix 2 to this contract;
- d. that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- e. that it will ensure compliance with the security measures;

- f. that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not covered by adequacy regulations issued under Section 17A Data Protection Act 2018 or Paragraphs 4 and 5 of Schedule 21 Data Protection Act 2018;
- g. to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the Commissioner if the data exporter decides to continue the transfer or to lift the suspension;
- h. to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- i. that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- j. that it will ensure compliance with Clause 4(a) to (i).

#### *Clause 5*

### **Obligations of the data importer**

The data importer agrees and warrants:

- a. to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b. that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c. that it has implemented the technical and organizational security measures specified in Appendix 2 before processing the personal data transferred;
- d. that it will promptly notify the data exporter about:
  - i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
  - ii. any accidental or unauthorized access; and
  - iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;
- e. to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the Commissioner with regard to the processing of the data transferred;
- f. at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the Commissioner;



- g. to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- h. that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- i. that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- j. to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

#### *Clause 6*

#### **Liability**

- a. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
- b. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

- c. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

#### *Clause 7*

#### **Mediation and jurisdiction**

- a. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
  - i. to refer the dispute to mediation, by an independent person or, where applicable, by the Commissioner;
  - ii. to refer the dispute to the UK courts.
- b. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.



## *Clause 8*

### **Cooperation with supervisory authorities**

- a. The data exporter agrees to deposit a copy of this contract with the Commissioner if it so requests or if such deposit is required under the applicable data protection law.
- b. The parties agree that the Commissioner has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
- c. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

## *Clause 9*

### **Governing law**

The Clauses shall be governed by the law of the country of the United Kingdom in which the data exporter is established.

## *Clause 10*

### **Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from (i) making changes permitted by Paragraph 7(3) & (4) of Schedule 21 Data Protection Act 2018; or (ii) adding clauses on business related issues where required as long as they do not contradict the Clause.

## *Clause 11*

### **Subprocessing**

- a. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses<sup>2</sup>. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
- b. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- c. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the laws of the country of the UK where the exporter is established.
- d. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a

year. The list shall be available to the Commissioner.

## Clause 12

### Obligation after the termination

- a. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
- b. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the Commissioner, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

## Appendix

### ANNEX I

#### A. LIST OF PARTIES

**[CUSTOMER]**

(the "**data exporter**")

and

**OVH US LLC dba OVHcloud®**

with its principal location at

11950 Democracy Drive  
Suite 300  
Reston, VA 20191

(the "**data importer**")

#### B. DESCRIPTION OF TRANSFER

See Section 3(a), above.

#### C. COMPETENT SUPERVISORY AUTHORITY

Commission nationale de l'informatique et des libertés ("CNIL")

### ANNEX II

#### **TECHNICAL AND organizational MEASURES INCLUDING TECHNICAL AND organizational MEASURES TO ENSURE THE SECURITY OF THE DATA**

OVHcloud has taken and will maintain the appropriate administrative, technical, physical and procedural security measures for protection of the security, confidentiality and integrity of the personal data as described on OVHcloud's Data Security webpage, accessible on [us.ovhcloud.com/resources/data-security](https://us.ovhcloud.com/resources/data-security), or otherwise made reasonably available by OVHcloud.

### ANNEX III

#### **List of Sub-processors**

#### **OVHcloud Sub-Processors**

OVHcloud may engage the following entities as Sub-processors to carry out specific data processing activities on behalf of Customers.

| Affiliate Entities                           | Country        |
|----------------------------------------------|----------------|
| OVH SAS                                      | France         |
| OVH Hispano                                  | Spain          |
| OVH SRL                                      | Italy          |
| OVH GmbH                                     | Germany        |
| OVH Limited                                  | United Kingdom |
| OVH Hosting Limited                          | Ireland        |
| OVH Hebergement INC                          | Canada         |
| OVH Sp. Zo.o.                                | Poland         |
| OVH Hosting Sistemas Informaticos unipessoal | Portugal       |
| OVH BV                                       | Netherland     |
| OVH Singapore PTE Ltd                        | Singapore      |
| OVH Australia PTY Ltd                        | Australia      |
| OVH Tech R&S Private Limited                 | India          |

| Third Party Entities             | Country   |
|----------------------------------|-----------|
| Avalara, Inc.                    | USA       |
| Bigtincan Mobile Pty Ltd.        | Australia |
| Equifax Information Services LLC | USA       |
| FIS                              | USA       |
| Fjord Technologies S.A.S.        | France    |
| Marketo, Inc.                    | USA       |
| Salesforce.com, Inc.             | USA       |
| ServiceNow Inc.                  | USA       |
| Zendesk, Inc.                    | USA       |
| Zuora, Inc.                      | USA       |

Tools

Support

News

## Social Networks



Copyright ©2023 OVH US LLC and affiliated companies all rights reserved. OVHcloud, the OVHcloud logo and all other OVH marks contained herein are registered trademarks of OVH SAS.  
All other marks contained herein are the property of their respective owners.  
[Terms of Service](#) | [Legal](#) | [About OVHcloud](#) | [OVHcloud Careers](#)

## Vereinbarung über die Auftragsverarbeitung gemäß Art. 28 DSGVO (AVV)

**Auftragsverarbeiter**  
gem. Art. 4 Z 8 DSGVO

**LINK Mobility Austria GmbH**  
Brauquartier 5/13  
8055 Graz  
AUSTRIA  
FN: 222236v

im Folgenden kurz „**AUFTRAGNEHMER**“,

**Verantwortlicher**  
gem. Art. 4 Z 7 DSGVO

Arivo Parking Solutions GmbH  
Am Innovationspark 10  
8020 Graz  
Austria  
im Folgenden kurz „**AUFTRAGGEBER**“;

AUFTRAGGEBER und AUFTRAGNEHMER nachfolgend einzeln oder gemeinsam „**PARTEI/EN**“ genannt

### I. Gegenstand der Vereinbarung

- a. Die PARTEIEN haben bezüglich der LINK Mobility Services einen Nutzungsvertrag geschlossen. Die entsprechenden Nutzungsbedingungen sowie die Datenschutzvereinbarung sind jeweils unter [www.websms.com](http://www.websms.com) abrufbar. Die Anmeldung zu websms Services erfolgt über Onlineanmeldung, über die von LINK Mobility zu Verfügung gestellten Onlinetools oder auf direktem Weg über die LINK Mobility Kundenberater.
- b. Der AUFTRAGNEHMER betreibt die LINK Mobility Services inklusive dem Mobile Messaging Gateway über welche der AUFTRAGGEBER elektronische Nachrichten (bspw. SMS, Push Nachrichten, Voice SMS etc.) versenden kann. Der AUFTRAGGEBER kann über die websms Services Kontakte und Nachrichten, sowie seine Accountinformation be- und verarbeiten. Für die Akquise von Kontakten stehen dem AUFTRAGGEBER Opt-in Formulare zur Verfügung.
- c. Der AUFTRAGNEHMER verarbeitet alle erforderlichen Daten,
  - die für den Betrieb,
  - den Versand der Nachrichten,
  - die ordnungsgemäße Verrechnung
  - und die Weiterentwicklung der Services notwendig sind.
- d. Dazu erhebt, verarbeitet der AUFTRAGNEHMER auch personenbezogene Daten im Auftrag des AUFTRAGGEBERS.
- e. Über die Daten und Datenverarbeitungstätigkeiten wird zwischen dem AUFTRAGGEBER und dem AUFTRAGNEHMER Vertraulichkeit vereinbart. Der Begriff Vertraulichkeit umfasst auch die Betriebs- und Geschäftsgeheimnisse sowohl des AUFTRAGGEBERS als auch des AUFTRAGNEHMERS.

### II. Art und Zweck der Datenverarbeitung

- a. Sämtliche Begriffe sind im Sinne der geltenden Rechtslage zu interpretieren und entsprechen den Begriffen der DSGVO sowie des österreichischen Datenschutzrechts.
- b. Daten sind alle personenbezogenen Daten, die über die Onlineinterfaces sowie die LINK Mobility Schnittstellen vom AUFTRAGGEBER an den AUFTRAGNEHMER im Zuge der LINK Mobility Services übermittelt werden.
- c. Gegenstand dieser Auftragsverarbeitungsvereinbarung ist nur die Verarbeitung von personenbezogenen Daten im Sinne der DSGVO in der geltenden Fassung.
- d. Statistische Daten, die der AUFTRAGNEHMER bspw. beim Besuch der Webservices erhebt und nicht direkt mit dem AUFTRAGGEBER in Verbindung gebracht werden können, sowie Firmendaten und andere nicht-personenbezogene Daten sind nicht Teil dieser Vereinbarung.

### III. Betroffene Daten- und Personenkategorien

| Datenkategorie    | Zweck der Verarbeitung                                                           | Dauer der Verarbeitung                                                                                                                                                                                                        | Personenkategorie                                                                         |
|-------------------|----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Stammdaten        | Kontaktadresse der anmel-<br>denden, Vertrag abschlie-<br>ßenden Person          | Dauer des Vertragsverhält-<br>nisses und über die entspre-<br>chenden gesetzlichen Auf-<br>bewahrungsfristen                                                                                                                  | AUFTRAGGEBER, bzw. na-<br>türliche Person, die für die<br>Anmeldung bevollmächtigt<br>ist |
| Verrechnungsdaten | Korrekte Fakturierung der<br>bestellten Services                                 | Dauer des Vertragsverhält-<br>nisses und über die entspre-<br>chenden gesetzlichen Auf-<br>bewahrungsfristen                                                                                                                  | Mitarbeiter des<br>AUFTRAGGEBERS                                                          |
| Kontodaten        | Verrechnung der offenen<br>Rechnungen, sowie SEPA<br>Lastschriftmandate          | Dauer des Vertragsverhält-<br>nisses und über die entspre-<br>chenden gesetzlichen Auf-<br>bewahrungsfristen                                                                                                                  | Mitarbeiter des<br>AUFTRAGGEBERS                                                          |
| Bestelldaten      | Detailinhalte über die<br>Bestellung                                             | Dauer des Vertragsverhält-<br>nisses                                                                                                                                                                                          | AUFTRAGGEBER<br><br>Mitarbeiter des<br>AUFTRAGGEBERS                                      |
| Userdaten         | Zugangsverwaltung zum<br>websms System                                           | Dauer des Vertragsverhält-<br>nisses                                                                                                                                                                                          | Mitarbeiter des<br>AUFTRAGGEBERS                                                          |
| Verkehrsdaten     | Nachrichtenversand,<br>Abrechnung                                                | Dauer des Vertragsverhält-<br>nisses und über die entspre-<br>chenden gesetzlichen Auf-<br>bewahrungsfristen                                                                                                                  | AUFTRAGGEBER<br><br>Endkunden des<br>AUFTRAGGEBERS                                        |
| Endkundendaten    | Alle Daten, die im Rahmen<br>der Erbringung der Leistun-<br>gen generiert werden | Dauer des Vertragsverhält-<br>nisses                                                                                                                                                                                          | Mitarbeiter des AUFTRAG-<br>GEBERS<br><br>Betroffene Endkunden                            |
| Inhaltsdaten      | Inhalte aus den Nachrichten                                                      | Bei Anlieferung via Schnitt-<br>stelle: unmittelbare Lö-<br>schung nach Zustellung<br><br>Bei Aktivierung Chatfunk-<br>tion: Dauer des Vertragsver-<br>hältnisses<br><br>Ausnahme: Chatverlauf wird<br>vom Endkunden gelöscht | Mitarbeiter des AUFTRAG-<br>GEBERS<br><br>Betroffene Endkunden                            |

### IV. Dauer der Verarbeitung

- Dieser Vertrag wird auf unbestimmte Zeit abgeschlossen und ist an die Laufzeit des LINK Mobility Nutzungsvertrages geknüpft und beginnt und endet insofern zeitgleich mit dem LINK Mobility Nutzungsvertrag.
- Eine Kündigung des LINK Mobility Nutzungsvertrages erstreckt sich automatisch auf den Vertrag über die Auftragsverarbeitung.
- Eine vorzeitige Kündigung des Vertrages über die Auftragsverarbeitung wird von beiden Parteien ausgeschlossen.
- Alle notwendigen Maßnahmen zum Datenschutz bestehen entsprechend den geltenden Rechtsvorschriften über die Vertragslaufzeit hinaus.

**V. Ort und Durchführung der Datenverarbeitung**

- a. Alle Datenverarbeitungstätigkeiten des AUFTRAGNEHMERS werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.
- b. Datenverarbeitungstätigkeiten, die nicht vom AUFTRAGNEHMER selbst durchgeführt werden, sind in „Anlage 2 – Subunternehmer“ enthalten. Jede Verlagerung der Leistungserbringung in einen Drittstaat erfolgt nur nach schriftlicher Zustimmung des AUFTRAGGEBERS.

**VI. Subaufträge**

- a. Der AUFTRAGNEHMER ist berechtigt alle in „Anlage 2 – Subunternehmer“ aufgeführten Auftragsverarbeiter als Subauftragsverarbeiter für die Vertragserfüllung zu beauftragen.
- b. Subaufträge sind nur jene Services, die der AUFTRAGNEHMER unmittelbar für die Erbringung seiner Services gemäß der Nutzungsvereinbarung nutzt. Hilfsdienste wie zum Beispiel Telekommunikationsservices, postalische Dienste und/oder solche Dienste, für die AUFTRAGGEBER ein eigenständiges Vertragsverhältnis eingeht, fallen nicht darunter.
- c. Änderungen sowie geplante Änderungen von Subauftragsverhältnissen sind dem AUFTRAGGEBER rechtzeitig und schriftlich bekannt zu geben. Der AUFTRAGGEBER hat das Recht diesen binnen eines Monats ab Bekanntgabe der Änderungen schriftlich zu widersprechen.
- d. Der AUFTRAGNEHMER schließt mit seinen Subauftragsverarbeitern entsprechende Vereinbarungen, um die Einhaltung der Verpflichtungen zwischen AUFTRAGGEBER und AUFTRAGNEHMER gem. Art 28 Abs. 4 DSGVO auch im Falle eines Subauftragsverhältnisses sicherzustellen. Der jeweilige Subauftragsverarbeiter wird ausschließlich aufgrund dieser Vereinbarung tätig.
- e. Kommt der Subauftragnehmer seinen Verpflichtungen nicht nach, haftet der AUFTRAGNEHMER gegenüber dem AUFTRAGGEBER für die Einhaltung der Pflichten des Subauftragsverarbeiters gemäß dieser Auftragsverarbeitungsvereinbarung.

**VII. Technisch organisatorische Maßnahmen**

- a. Die technischen und organisatorischen Maßnahmen gem. Anlage 1 werden Bestandteil dieser Vereinbarung.
- b. Der AUFTRAGNEHMER überprüft seine technischen und organisatorischen Maßnahmen regelmäßig und passt sie erforderlichenfalls dem letzten Stand der Technik an.
- c. Alle Änderungen der technischen und organisatorischen Maßnahmen sind dem AUFTRAGGEBER schriftlich mitzuteilen.

## VIII. Weisungen

- a. Der AUFTRAGGEBER hat das Recht im Zuge dieses Vertrages Weisungen an den AUFTRAGNEHMER zu erteilen.
- b. Weisungen haben schriftlich zu erfolgen. Mündliche Weisungen sind unverzüglich schriftlich zu bestätigen und werden von beiden Vertragsparteien aufbewahrt.
- c. Weisungen sind nur zwischen vereinbarten Weisungsberechtigten und Weisungsempfängern gültig.

Weisungsberechtigte Personen auf Seiten des AUFTRAGGEBERS sind:

Dominik Wieser, Arivo Parking Solutions GmbH, d.wieser@arivo.co

Ines Schnur, Arivo Parking Solutions GmbH, i.schnur@arivo.co

Weisungsempfänger auf Seiten des AUFTRAGNEHMERs sind:

- Josef GRABNER, VP Commercial Operation DACH, josef.grabner@linkmobility.com
- Martin MRVKA, VP Technology, martin.mrvka@linkmobility.com, +43 316 813380
- Jan WIECZORKIEWICZ, Datenschutzverantwortlicher, datenschutz.at@linkmobility.com, +43 316 813380
- Hermann GSTETTNER, Senior Solution & Partner Consultant, hermann.gstettner@linkmobility.com, +43 316 813380

Änderungen bezüglich Weisungsberechtigten und Weisungsempfängern sind unverzüglich und schriftlich der jeweiligen PARTEI mitzuteilen.

## IX. Rechte und Pflichten des AUFTRAGGEBERS

- a. Der AUFTRAGGEBER verpflichtet sich alle Vereinbarungen, die Bestandteil des LINK Mobility Nutzungsvertrages, der Nutzungsbedingungen zum websms Messaging Gateway und der Datenschutzerklärung sind, einzuhalten.
- b. Der AUFTRAGGEBER ist für die Bewertung und Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten, Kundendaten sowie für den Schutz der Rechte der betroffenen Personen alleinig verantwortlich.
- c. Der AUFTRAGGEBER ist für alle personenbezogenen Daten, die er für die Nutzung von LINK Mobility in den Anwendungen verwendet alleinig Verantwortlicher gem. Art. 4 DSGVO Abs. 7 und auch zum Schutz dieser Daten verpflichtet.
- d. Der AUFTRAGGEBER informiert den AUFTRAGNEHMER unverzüglich, wenn er Fehler oder Unrechtmäßigkeiten bei den personenbezogenen Daten feststellt und diese nicht von ihm selbst, über die vom AUFTRAGNEHMER zu Verfügung gestellten Anwendungen behoben werden können.
- e. Der AUFTRAGGEBER hat das Recht Weisungen für folgenden Umfang zu erteilen:
  - Auskunft darüber, welche Daten vom Auftraggeber gespeichert sind
  - Löschung von personenbezogenen Daten
  - Änderung von personenbezogenen Daten
  - Nach Beendigung des Vertragsverhältnisses, die Herausgabe der gespeicherten personenbezogenen Daten
- f. Der AUFTRAGGEBER ist vor Beginn der Datenverarbeitung und nach einer entsprechenden Vorankündigung und Terminvereinbarung berechtigt sich selbst oder durch einen von ihm beauftragten Dritten, von den getroffenen technischen und organisatorischen Maßnahmen zu überzeugen.



## **X. Pflichten des AUFTRAGNEHMERS**

- a. Der AUFTRAGNEHMER verpflichtet sich Daten und Verarbeitungsergebnisse ausschließlich im Rahmen dieser Vereinbarung und der schriftlichen Aufträge (Weisungen) zu verarbeiten. Die Verarbeitung der Daten für eigene Zwecke des AUFTRAGNEHMERS bedarf einer schriftlichen Zustimmung durch den AUFTRAGGEBER. Diese Zustimmung kann vom AUFTRAGGEBER jederzeit widerrufen werden.
- b. Der AUFTRAGNEHMER informiert den AUFTRAGGEBER unverzüglich, falls er der Ansicht ist, eine Weisung des AUFTRAGGEBERS verstößt gegen Datenschutzbestimmungen der Europäischen Union oder der Mitgliedstaaten.
- c. Erhält der AUFTRAGNEHMER den behördlichen Auftrag Daten des AUFTRAGGEBERS herauszugeben, so hat er diesen unverzüglich darüber in Kenntnis zu setzen und die Behörde an ihn zu verweisen.
- d. Der AUFTRAGNEHMER erklärt rechtsverbindlich, dass er mit allen mit der Datenverarbeitung in seinem Unternehmen beauftragten Personen, sowie mit allen Subauftragsverarbeitern und den dort beauftragten Personen Vertraulichkeit vereinbart hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen bleibt auch nach Beendigung ihrer Tätigkeit und auch beim Ausscheiden aus dem Unternehmen des AUFTRAGNEHMERS aufrecht. Der AUFTRAGNEHMER stellt sicher, dass diese Vertraulichkeit auch durch seine Subauftragsverarbeiter gewährleistet wird.
- e. Der AUFTRAGNEHMER erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit und Verarbeitung nach Art 32 DSGVO ergriffen hat (Anlage 1 – technisch, organisatorische Maßnahmen).
- f. Der AUFTRAGNEHMER ergreift die technischen und organisatorischen Maßnahmen gem. Anlage 1 damit der AUFTRAGGEBER die Rechte der betroffenen Personen nach Abschnitt III DSGVO innerhalb der gesetzlichen Fristen erfüllen kann. Dafür überlässt der AUFTRAGNEHMER dem AUFTRAGGEBER alle notwendigen Informationen.
- g. Der AUFTRAGNEHMER setzt den AUFTRAGGEBER unverzüglich über Datenpannen (Data Breach) in Kenntnis und unterstützt den AUFTRAGGEBER bei der Einhaltung der in Art 32 bis Art 36 DSGVO genannten Pflichten.
- h. Erhält der AUFTRAGNEHMER irrtümlich einen Antrag gem. Abschnitt III DSGVO, in dem er für den Verantwortlichen der Datenanwendung gehalten wird, leitet er diesen unverzüglich an den AUFTRAGGEBER weiter und hat dies dem Antragsteller mitzuteilen.
- i. Der AUFTRAGNEHMER führt ein für die vorliegende Auftragsverarbeitung relevantes Verarbeitungsverzeichnis gem. Art 30 DSGVO.
- j. Der AUFTRAGNEHMER räumt dem AUFTRAGGEBER oder einem von ihm beauftragten Dritten, nach einer entsprechenden Vorankündigung und Terminvereinbarung, das Recht ein sich jederzeit, durch Einsichtnahme oder Kontrolle über die vertragskonforme Erfüllung in Kenntnis zu setzen.
- k. Der AUFTRAGNEHMER ist verpflichtet nach Beendigung dieses Vertrages alle Verarbeitungsergebnisse und Unterlagen, welche Daten aus dem Auftrag enthalten, auf Wunsch des AUFTRAGGEBERS herauszugeben oder zu löschen. Ausgenommen davon sind Daten, die zur Erfüllung von gesetzlichen Vorgaben aufbewahrt werden müssen.

## **XI. Löschung und Rückgabe personenbezogener Daten**

- a. Kopien oder Duplikate der Daten dürfen ohne Wissen und Zustimmung des AUFTRAGGEBERS nicht erstellt werden. Ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind.
- b. Ferner ausgenommen sind Daten, die für die Einhaltung der gesetzlichen Aufbewahrungspflichten erforderlich sind. Dies gilt auch für Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen.
- c. Nach Abschluss der vereinbarten Leistungen oder früher, nach Aufforderung durch den AUFTRAGGEBER, hat der AUFTRAGNEHMER sämtliche in seinem Besitz befindlichen Datenbestände, Unterlagen sowie erstellte Verarbeitungs- und Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem AUFTRAGGEBER auszuhändigen.
- d. Auf ausdrücklichen Wunsch des AUFTRAGGEBERS kann anstatt der Herausgabe eine Vernichtung der Daten verlangt werden. Das Protokoll der Löschung ist auf Anforderung des AUFTRAGGEBERS vorzuweisen.

## XII. Haftung

- a. Für den Ersatz von Schäden, die ein Betroffener wegen einer nach den Datenschutzgesetzen unzulässigen oder unrichtigen Datenverarbeitung oder Nutzung im Rahmen der Auftragsverarbeitung erleidet, haften die Parteien gemäß der DSGVO in der geltenden Fassung.
- b. Im Innenverhältnis haftet der AUFTRAGNEHMER nur bei Vorsatz oder grober Fahrlässigkeit, wobei die Haftung des AUFTRAGNEHMERS für jegliche Schäden, dazu zählen unter anderem entgangener Gewinn, verlorene Einsparungen, mittelbare und Folgeschäden, Geldbußen durch Aufsichtsbehörden, sowie Schäden aus Ansprüchen Dritter mit EUR 1.000,00 begrenzt ist.
- c. Die Parteien stellen sich jeweils von der Haftung frei, wenn eine Partei nachweist, dass sie in keinerlei Hinsicht für den Umstand, durch den der Schaden bei einem Betroffenen eingetreten ist, verantwortlich ist.

## XIII. Schlussbestimmungen

- a. Sollten einzelne Bestimmungen dieses Vertrages unwirksam oder undurchführbar sein oder nach Vertragsabschluss unwirksam oder undurchführbar werden, wird die Wirksamkeit der übrigen Bestimmungen nicht davon berührt. Beide Vertragsparteien verpflichten sich, anstelle der unwirksamen Bestimmungen, wirksame und möglichst nahekommende Bestimmungen zu vereinbaren.
- b. Änderungen und Ergänzungen dieser Vereinbarung müssen schriftlich erfolgen.
- c. Weicht diese Vereinbarung vom LINK Mobility Nutzungsvertrag ab, geht diese Vereinbarung vor.
- d. Diese Vereinbarung unterliegt österreichischem Recht unter Ausschluss der kollisionsrechtlichen Rück- und/oder Weiterverweisungsnormen des österreichischen internationalen Privatrechts.
- e. Zur Entscheidung aller Streitigkeiten aus oder in Zusammenhang mit dieser Vereinbarung einschließlich deren Zustandekommen, Verletzung, Auflösung, Gültigkeit oder Nichtigkeit, sind ausschließlich die örtlich und sachlich zuständigen Grazer Gerichte zuständig.

Für den AUFTRAGNEHMER

Für den AUFTRAGGEBER

Graz, am 13.3.2023

Graz ..... am 9/4/22 .....

Josef Grabner  
Managing Direktor

  
Arivo Parking Solutions GmbH  
Am Innovationspark 10, 8020 Graz, Austria  
Tel: +43 316 375 018 FN467497x  
Info@arivo.co www.arivo.co  
.....  
Name und Funktion

## Anlage 1 - technisch, organisatorische Maßnahmen

### 1. Zutrittskontrolle

Schutz vor unbefugten Zutritt zu Datenverarbeitungsanlagen

- Alarmanlage
- Protokollierung der Besucher
- Personenkontrolle beim Portier
- Chipkarten für das Zugangssystem
- Videoüberwachung
- Tragepflicht von Berechtigungsausweisen

### 2. Zugangskontrolle

Maßnahmen, die verhindern, dass Unbefugte Datenverarbeitungssysteme benutzen:

- Zuordnung von Benutzerrechten
- Passwortvergabe auf Basis einer Passwortpolicy
- Authentifizierungen mittels Benutzernamen und Passwort
- Gehäuseverriegelung an den Serverracks
- Benutzerprofile
- Einsatz von VPN Technologie
- Sicherheitsschlösser
- Personenkontrolle beim Portier
- Tragepflicht von Berechtigungsausweisen
- Teilweiser Einsatz von Smartphone-Administrationsservices (Android)
- Einsatz von Antivirensoftware
- Einsatz von Firewalls

### 3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung des Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Beschränkung der Anzahl von Systemadministratoren auf ein notwendiges Minimum
- Passwortrichtlinie (Passwortlänge)

### 4. Pseudonymisierung

Maßnahmen, die sicherstellen, dass, sofern möglich, primäre Identifikationsmerkmale aus personenbezogenen Daten entfernt werden und diese gesondert gespeichert werden:

- Google Analytics IP Pseudonymisierung

### 5. Klassifikationsschema für Daten

Einteilung in geheim, vertraulich, intern und öffentlich.

### 6. Weitergabekontrolle

Maßnahmen, die sicherstellen, dass personenbezogene Daten bei der elektronischen Übertragung oder während des Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Einrichtung von Standleitungen und VPN Tunneln
- Die Durchführung von physischen Transporten von Hardware erfolgt mit persönlicher Begleitung durch qualifiziertes hauseigenes Personal
- Der Transport erfolgt in sicheren Transportbehältern.
- Datenweitergaben erfolgen nur an berechtigte Dritte (Behörden) im Rahmen der gesetzlichen Vorgaben.

**7. Eingabekontrolle**

Maßnahmen, die sicherstellen, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

- Protokollierung mittels Access Logs
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen

**8. Verfügbarkeitskontrolle**

Maßnahmen, die sicherstellen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Unterbrechungsfreie Stromversorgung (USV)
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Alarmierung bei unberechtigten Zutritten
- Testen von Datenwiederherstellung
- Klimaanlage in Serverräumen
- Backups inkl. Recoverykonzept
- Notfallpläne
- Serverräume sind nicht unter sanitären Anlagen
- Schutzsteckdosen in Serverräumen

**9. Trennungsgebot**

Maßnahmen, die sicherstellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt voneinander verarbeitet werden.

- Festlegung von Datenbankrechten
- Logische softwareseitige Mandantentrennung
- Trennung von Entwicklungs-, Test- und Produktivsystem

**10. Wiederherstellbarkeit**

Maßnahmen, die sicherstellen, dass personenbezogene Daten rasch wiederhergestellt werden können:

- Backups
- Recoverykonzept

**11. Lösungsfristen**

Maßnahmen, die sicherstellen, dass personenbezogene Daten und Metadaten entsprechend gelöscht werden können wenn ihre gesetzlichen Aufbewahrungsfristen erloschen sind.

**12. Auftragskontrolle**

Maßnahmen, die sicherstellen, dass keine Auftragsverarbeitung ohne entsprechende Weisung des AUFTRAGGEBERS erfolgt:

- Auftragsverarbeitungsvereinbarung mit Lieferanten inkl. Adressatenkreis von Weisungsgebern und Weisungsempfängern
- Schriftliche Weisungen

## Anlage 2 – Subunternehmer

| Firmenname          | Anschrift                                                                                                                                        | Zweck der Beauftragung                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| InterXion           | Sitz unseres Rechenzentrums ist Louis-Häflinger-Gasse, 1210 Wien; Hauptsitz von InterXion ist Tupolevlaan 24, 1119 NX Schiphol-Rijk, Niederlande | Hosting der websms Services;<br>ISO zertifiziertes Hochsicherheitsrechenzentrum |
| rapidmail GmbH      | Augustinerplatz 2<br>79098 Freiburg i.Br.<br>Deutschland                                                                                         | Newslettersend                                                                  |
| mtms solutions GmbH | Nordstraße 4, 5301 Eugendorf, Österreich                                                                                                         | Betrieb, Wartung und Kundenservice von Spezialapplikationen                     |
| easyname GmbH       | Canettistraße 5/10<br>A-1100 Wien                                                                                                                | Datacenter für die neue Cloud Plattform                                         |

## AWS DATA PROCESSING ADDENDUM

This Data Processing Addendum (“**DPA**”) supplements the AWS Customer Agreement available at <http://aws.amazon.com/agreement>, as updated from time to time between Customer and AWS, or other agreement between Customer and AWS governing Customer’s use of the Services (the “**Agreement**”). This DPA is an agreement between you and the entity you represent (“**Customer**”, “**you**” or “**your**”) and Amazon Web Services, Inc. and the AWS Contracting Party or AWS Contracting Parties (as applicable) under the Agreement (together “**AWS**”). Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 17 of this DPA.

### 1. Data Processing.

- 1.1 **Scope and Roles.** This DPA applies when Customer Data is processed by AWS. In this context, AWS will act as processor to Customer, who can act either as controller or processor of Customer Data.
- 1.2 **Customer Controls.** Customer can use the Service Controls to assist it with its obligations under Applicable Data Protection Law, including its obligations to respond to requests from data subjects. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS would become aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if AWS becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. AWS will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing the Service Controls that Customer can use to erase or rectify Customer Data.
- 1.3 **Details of Data Processing.**
  - 1.3.1 **Subject matter.** The subject matter of the data processing under this DPA is Customer Data.
  - 1.3.2 **Duration.** As between AWS and Customer, the duration of the data processing under this DPA is determined by Customer.
  - 1.3.3 **Purpose.** The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.
  - 1.3.4 **Nature of the processing.** Compute, storage and such other Services as described in the Documentation and initiated by Customer from time to time.
  - 1.3.5 **Type of Customer Data.** Customer Data uploaded to the Services under Customer’s AWS accounts.
  - 1.3.6 **Categories of data subjects.** The data subjects could include Customer’s customers, employees, suppliers and End Users.
- 1.4 **Compliance with Laws.** Each party will comply with all laws, rules and regulations applicable to it and binding on it in the performance of this DPA, including Applicable Data Protection Law.

- 2. **Customer Instructions.** The parties agree that this DPA and the Agreement (including Customer providing instructions via configuration tools such as the AWS management console and APIs made available by AWS for the Services) constitute Customer’s documented instructions regarding AWS’s processing of Customer Data (“**Documented Instructions**”). AWS will process

Customer Data only in accordance with Documented Instructions (which if Customer is acting as a processor, could be based on the instructions of its controllers). Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between AWS and Customer, including agreement on any additional fees payable by Customer to AWS for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if AWS declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. Taking into account the nature of the processing, Customer agrees that it is unlikely AWS can form an opinion on whether Documented Instructions infringe Applicable Data Protection Law. If AWS forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its Documented Instructions.

3. **Confidentiality of Customer Data.** AWS will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends AWS a demand for Customer Data, AWS will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, AWS may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then AWS will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so.
4. **Confidentiality Obligations of AWS Personnel.** AWS restricts its personnel from processing Customer Data without authorization by AWS as described in the Security Standards. AWS imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection and data security.
5. **Security of Data Processing**
  - 5.1 AWS has implemented and will maintain the technical and organizational measures for the AWS Network as described in the Security Standards and this Section. In particular, AWS has implemented and will maintain the following technical and organizational measures:
    - (a) security of the AWS Network as set out in Section 1.1 of the Security Standards;
    - (b) physical security of the facilities as set out in Section 1.2 of the Security Standards;
    - (c) measures to control access rights for authorized personnel to the AWS Network as set out in Section 1.3 of the Security Standards; and
    - (d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by AWS as described in Section 2 of the Security Standards.
  - 5.2 Customer can elect to implement technical and organizational measures to protect Customer Data. Such technical and organizational measures include the following which can be obtained by Customer from AWS as described in the Documentation, or directly from a third-party supplier:
    - (a) pseudonymization and encryption to ensure an appropriate level of security;
    - (b) measures to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services that are operated by Customer;

measures to allow Customer to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and

- (c) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by Customer.

## 6. Sub-processing.

6.1 **Authorized Sub-processors.** Customer provides general authorization to AWS's use of sub-processors to provide processing activities on Customer Data on behalf of Customer ("**Sub-processors**") in accordance with this Section. The AWS website (currently posted at <https://aws.amazon.com/compliance/sub-processors/>) lists Sub-processors that are currently engaged by AWS. At least 30 days before AWS engages a Sub-processor, AWS will update the applicable website and provide Customer with a mechanism to obtain notice of that update. To object to a Sub-processor, Customer can: (i) terminate the Agreement pursuant to its terms; (ii) cease using the Service for which AWS has engaged the Sub-processor; or (iii) move the relevant Customer Data to another Region where AWS has not engaged the Sub-processor.

6.2 **Sub-processor Obligations.** Where AWS authorizes a Sub-processor as described in Section 6.1:

- (i) AWS will restrict the Sub-processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Documentation, and AWS will prohibit the Sub-processor from accessing Customer Data for any other purpose;
- (ii) AWS will enter into a written agreement with the Sub-processor and, to the extent that the Sub-processor performs the same data processing services provided by AWS under this DPA, AWS will impose on the Sub-processor the same contractual obligations that AWS has under this DPA; and
- (iii) AWS will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-processor that cause AWS to breach any of AWS's obligations under this DPA.

7. **AWS Assistance with Data Subject Requests.** Taking into account the nature of the processing, the Service Controls are the technical and organizational measures by which AWS will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under Applicable Data Protection Law. If a data subject makes a request to AWS, AWS will promptly forward such request to Customer once AWS has identified that the request is from a data subject for whom Customer is responsible. Customer authorizes on its behalf, and on behalf of its controllers when Customer is acting as a processor, AWS to respond to any data subject who makes a request to AWS, to confirm that AWS has forwarded the request to Customer. The parties agree that Customer's use of the Service Controls and AWS forwarding data subjects' requests to Customer in accordance with this Section, represent the scope and extent of Customer's required assistance.

8. **Optional Security Features.** AWS makes available many Service Controls that Customer can elect to use. Customer is responsible for (a) implementing the measures described in Section 5.2, as appropriate, (b) properly configuring the Services, (c) using the Service Controls to allow Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (for example backups and routine archiving of Customer Data), and



(d) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorized access and measures to control access rights to Customer Data.

## **9. Security Incident Notification.**

9.1 **Security Incident.** AWS will (a) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (b) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security Incident.

9.2 **AWS Assistance.** To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), AWS will cooperate with and assist Customer by including in the notification under Section 9.1(a) such information about the Security Incident as AWS is able to disclose to Customer, taking into account the nature of the processing, the information available to AWS, and any restrictions on disclosing the information, such as confidentiality. Taking into account the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident.

9.3 **Unsuccessful Security Incidents.** Customer agrees that:

- (i) an unsuccessful Security Incident will not be subject to this Section 9. An unsuccessful Security Incident is one that results in no unauthorized access to Customer Data or to any of AWS's equipment or facilities storing Customer Data, and could include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers) or similar incidents; and
- (ii) AWS's obligation to report or respond to a Security Incident under this Section 9 is not and will not be construed as an acknowledgement by AWS of any fault or liability of AWS with respect to the Security Incident.

9.4 **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means AWS selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the AWS management console and secure transmission at all times.

## **10. AWS Certifications and Audits.**

10.1 **AWS ISO-Certification and SOC Reports.** In addition to the information contained in this DPA, upon Customer's request, and provided that the parties have an applicable NDA in place, AWS will make available the following documents and information:

- (i) the certificates issued for the ISO 27001 certification, the ISO 27017 certification, the ISO 27018 certification, and the ISO 27701 certification (or the certifications or other documentation evidencing compliance with such alternative standards as are substantially equivalent to ISO 27001, ISO 27017, ISO 27018, and ISO 27701); and
- (ii) the System and Organization Controls (SOC) 1 Report, the System and Organization Controls (SOC) 2 Report and the System and Organization Controls (SOC) 3 Report (or the reports or other documentation describing the controls

implemented by AWS that replace or are substantially equivalent to the SOC 1, SOC 2 and SOC 3).

- 10.2 **AWS Audits.** AWS uses external auditors to verify the adequacy of its security measures, including the security of the physical data centers from which AWS provides the Services. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third-party security professionals at AWS's selection and expense; and (d) will result in the generation of an audit report ("**Report**"), which will be AWS's Confidential Information.
  - 10.3 **Audit Reports.** At Customer's written request, and provided that the parties have an applicable NDA in place, AWS will provide Customer with a copy of the Report so that Customer can reasonably verify AWS's compliance with its obligations under this DPA.
  - 10.4 **Privacy Impact Assessment and Prior Consultation.** Taking into account the nature of the processing and the information available to AWS, AWS will assist Customer in complying with Customer's obligations in respect of data protection impact assessments and prior consultation, by providing the information AWS makes available under this Section 10.
11. **Customer Audits.** Customer chooses to conduct any audit, including any inspection, it has the right to request or mandate on its own behalf, and on behalf of its controllers when Customer is acting as a processor, under Applicable Data Protection Law or the Standard Contractual Clauses, by instructing AWS to carry out the audit described in Section 10. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending AWS written notice as provided for in the Agreement. If AWS declines to follow any instruction requested by Customer regarding audits, including inspections, Customer is entitled to terminate the Agreement in accordance with its terms.
12. **Transfers of Personal Data.**
- 12.1 **Regions.** Customer can specify the location(s) where Customer Data will be processed within the AWS Network (each a "**Region**"), including Regions in the EEA. Once Customer has made its choice, AWS will not transfer Customer Data from Customer's selected Region(s) except as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or valid and binding order of a governmental body.
  - 12.2 **Application of Standard Contractual Clauses.** Subject to Section 12.3, the Standard Contractual Clauses will only apply to Customer Data subject to the GDPR that is transferred, either directly or via onward transfer, to any Third Country, (each a "**Data Transfer**").
    - 12.2.1 When Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.
    - 12.2.2 When Customer is acting as a processor, the Processor-to-Processor Clauses will apply to a Data Transfer. Taking into account the nature of the processing, Customer agrees that it is unlikely that AWS will know the identity of Customer's controllers because AWS has no direct relationship with Customer's controllers and therefore, Customer will fulfil AWS's obligations to Customer's controllers under the Processor-to-Processor Clauses.
  - 12.3 **Alternative Transfer Mechanism.** The Standard Contractual Clauses will not apply to a Data Transfer if AWS has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for lawful Data Transfers.

- 13. Termination of the DPA.** This DPA will continue in force until the termination of the Agreement (the “**Termination Date**”).
- 14. Return or Deletion of Customer Data.** At any time up to the Termination Date, and for 90 days following the Termination Date, subject to the terms and conditions of the Agreement, AWS will return or delete Customer Data when Customer uses the Service Controls to request such return or deletion. No later than the end of this 90-day period, Customer will close all AWS accounts containing Customer Data.
- 15. Duties to Inform.** Where Customer Data becomes subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by AWS, AWS will inform Customer without undue delay. AWS will, without undue delay, notify all relevant parties in such action (for example, creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer’s property and area of responsibility and that Customer Data is at Customer’s sole disposition.
- 16. Entire Agreement; Conflict.** This DPA incorporates the Standard Contractual Clauses by reference. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control, except that the Service Terms will control over this DPA. Nothing in this document varies or modifies the Standard Contractual Clauses.
- 17. Definitions.** Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:

“**API**” means an application program interface.

“**Applicable Data Protection Law**” means all laws and regulations applicable to and binding on the processing of Customer Data by a party, including, as applicable, the GDPR and the UK Data Protection Act 2018.

“**AWS Network**” means the servers, networking equipment, and host software systems (for example, virtual firewalls) that are within AWS’s control and are used to provide the Services.

“**Binding Corporate Rules**” has the meaning given to it in the GDPR.

“**controller**” has the meaning given to it in the GDPR.

“**Controller-to-Processor Clauses**” means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at [https://d1.awsstatic.com/Controller to Processor SCCs.pdf](https://d1.awsstatic.com/Controller_to_Processor_SCCs.pdf).

“**Customer Data**” means the “personal data” (as defined in Applicable Data Protection Law) that is uploaded to the Services under Customer’s AWS accounts.

“**Documentation**” means the then-current documentation for the Services located at <http://aws.amazon.com/documentation> (and any successor locations designated by AWS).

“**EEA**” means the European Economic Area.

“**GDPR**” means Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

“**processing**” has the meaning given to it in the GDPR and “process”, “processes” and “processed” will be interpreted accordingly.

“**processor**” has the meaning given to it in the GDPR.

**“Processor-to-Processor Clauses”** means the standard contractual clauses between processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, and currently located at [https://d1.awsstatic.com/Processor\\_to\\_Processor\\_SCCs.pdf](https://d1.awsstatic.com/Processor_to_Processor_SCCs.pdf).

**“Region”** has the meaning given to it in Section 12.1 of this DPA.

**“Security Incident”** means a breach of AWS’s security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

**“Security Standards”** means the security standards attached to this DPA as Annex 1.

**“Service Controls”** means the controls, including security features and functionalities, that the Services provide, as described in the Documentation.

**“Standard Contractual Clauses”** means (i) the Controller-to-Processor Clauses, or (ii) the Processor-to-Processor Clauses, as applicable in accordance with Sections 12.2.1 and 12.2.2.

**“Third Country”** means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

## Annex 1

### Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

**1 Information Security Program.** AWS will maintain an information security program designed to (a) enable Customer to secure Customer Data against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable risks to the security and availability of the AWS Network, and (c) minimize physical and logical security risks to the AWS Network, including through regular risk assessment and testing. AWS will designate one or more employees to coordinate and be accountable for the information security program.

AWS's information security program will include the following measures:

#### 1.1 Logical Security.

**A. Access Controls.** AWS will make the AWS Network accessible only to authorized personnel, and only as necessary to maintain and provide the Services. AWS will maintain access controls and policies to manage authorizations for access to the AWS Network from each network connection and user, including through the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain access controls designed to (i) restrict unauthorized access to data, and (ii) segregate each customer's data from other customers' data.

**B. Restricted User Access.** AWS will (i) provision and restrict user access to the AWS Network in accordance with least privilege principles based on personnel job functions, (ii) require review and approval prior to provisioning access to the AWS Network above least privileged principles, including administrator accounts; (iii) require at least quarterly review of AWS Network access privileges and, where necessary, revoke AWS Network access privileges in a timely manner, and (iv) require two-factor authentication for access to the AWS Network from remote locations.

**C. Vulnerability Assessments.** AWS will perform regular external vulnerability assessments and penetration testing of the AWS Network, and will investigate identified issues and track them to resolution in a timely manner.

**D. Application Security.** Before publicly launching new Services or significant new features of Services, AWS will perform application security reviews designed to identify, mitigate and remediate security risks.

**E. Change Management.** AWS will maintain controls designed to log, authorize, test, approve and document changes to existing AWS Network resources, and will document change details within its change management or deployment tools. AWS will test changes according to its change management standards prior to migration to production. AWS will maintain processes designed to detect unauthorized changes to the AWS Network and track identified issues to a resolution.

**F. Data Integrity.** AWS will maintain controls designed to provide data integrity during transmission, storage and processing within the AWS Network. AWS will provide Customer the ability to delete Customer Data from the AWS Network.

**G. Business Continuity and Disaster Recovery.** AWS will maintain a formal risk management program designed to support the continuity of its critical business functions ("**Business Continuity Program**"). The Business Continuity Program includes processes and procedures for identification of, response to, and recovery from, events that could prevent or materially impair AWS's provision of the Services (a

“BCP Event”). The Business Continuity Program includes a three-phased approach that AWS will follow to manage BCP Events:

- (i) **Activation & Notification Phase.** As AWS identifies issues likely to result in a BCP Event, AWS will escalate, validate and investigate those issues. During this phase, AWS will analyze the root cause of the BCP Event.
- (ii) **Recovery Phase.** AWS assigns responsibility to the appropriate teams to take steps to restore normal system functionality or stabilize the affected Services.
- (iii) **Reconstitution Phase.** AWS leadership reviews actions taken and confirms that the recovery effort is complete and the affected portions of the Services and AWS Network have been restored. Following such confirmation, AWS conducts a post-mortem analysis of the BCP Event.

**H. Incident Management.** AWS will maintain corrective action plans and incident response plans to respond to potential security threats to the AWS Network. AWS incident response plans will have defined processes to detect, mitigate, investigate, and report security incidents. The AWS incident response plans include incident verification, attack analysis, containment, data collection, and problem remediation. AWS will maintain an AWS Security Bulletin (as of the Effective Date, <http://aws.amazon.com/security/security-bulletins/>) which publishes and communicates security related information that may affect the Services and provides guidance to mitigate the risks identified.

**I. Storage Media Decommissioning.** AWS will maintain a media decommissioning process that is conducted prior to final disposal of storage media used to store Customer Data. Prior to final disposal, storage media that was used to store Customer Data will be degaussed, erased, purged, physically destroyed, or otherwise sanitized in accordance with industry standard practices designed to ensure that the Customer Data cannot be retrieved from the applicable type of storage media.

## 1.2 Physical Security.

**A. Access Controls.** AWS will (i) implement and maintain physical safeguards designed to prevent unauthorized physical access, damage, or interference to the AWS Network, (ii) use appropriate control devices to restrict physical access to the AWS Network to only authorized personnel who have a legitimate business need for such access, (iii) monitor physical access to the AWS Network using intrusion detection systems designed to monitor, detect, and alert appropriate personnel of security incidents, (iv) log and regularly audit physical access to the AWS Network, and (v) perform periodic reviews to validate adherence with these standards.

**B. Availability.** AWS will (i) implement redundant systems for the AWS Network designed to minimize the effect of a malfunction on the AWS Network, (ii) design the AWS Network to anticipate and tolerate hardware failures, and (iii) implement automated processes designed to move customer data traffic away from the affected area in the case of hardware failure.

## 1.3 AWS Employees.

**A. Employee Security Training.** AWS will implement and maintain employee security training programs regarding AWS information security requirements. The security awareness training programs will be reviewed and updated at least annually.

**B. Background Checks.** Where permitted by law, and to the extent available from applicable governmental authorities, AWS will require that each employee undergo a background investigation

that is reasonable and appropriate for that employee's position and level of access to the AWS Network.

**2 Continued Evaluation.** AWS will conduct periodic reviews of the information security program for the AWS Network. AWS will update or alter its information security program as necessary to respond to new security risks and to take advantage of new technologies.





TELEMATICA

# DSGVO

VEREINBARUNG ZUR  
AUFTRAGSVERARBEITUNG



# VEREINBARUNG ZUR AUFTRAGSVERARBEITUNG NACH ART 28 DSGVO

zwischen

**Telematica Internet Service Provider GmbH**  
Münzgrabenstraße 84b/5, 8010 Graz  
Österreich

– im Folgenden „AN“ genannt –  
als „Auftragsverarbeiter“ gemäß DSGVO

und

**Arivo Parking Solutions GmbH**

---

**Am Innovationspark 10, 8020 Graz**

---

**Österreich**

---

– im Folgenden „AG“ genannt –  
als „Verantwortlicher“ gemäß DSGVO

– zusammen „Vertragspartner“ oder „Parteien“ genannt –

## PRÄAMBEL

Diese Vereinbarung dient als Ergänzung und konkretisiert die Verpflichtungen der Vertragspartner zum Datenschutz für alle bestehenden und zukünftigen rechtswirksamen Verträge, Master Level Agreements, Service Level Agreements, Leistungsbeschreibungen etc. (im Folgenden zusammengefasst als „Vertrag“ oder „Verträge“ bezeichnet) zwischen AG und AN. Sie findet Anwendung auf alle Tätigkeiten, die mit den Verträgen zwischen AG und AN in Zusammenhang stehen und bei denen Beschäftigte des AN oder durch den AN Beauftragte personenbezogene Daten (im Folgenden „Daten“ genannt) des AG als Verantwortlichen im Auftrag verarbeiten. Im Übrigen gelten für dieses Dokument alle Bestimmungen und Begriffe der EU-Datenschutzgrundverordnung [Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG] (im Folgenden „DSGVO“ genannt) sowie darüberhinausgehend das für den AG zutreffende respektive für die Verträge anwendbare nationalstaatliche Datenschutzrecht und das österreichische Telekommunikationsgesetz (TKG 2003).

Zum besseren Verständnis und zur leichteren Lesbarkeit gilt in diesem Dokument bei allen personenbezogenen Bezeichnungen die gewählte Form gleichermaßen für alle Geschlechter.

Es wird darauf hingewiesen, dass der AN als verbundenes Unternehmen der Anexia-Unternehmensgruppe mit der ANEXIA Internetdienstleistungs GmbH als Leitgesellschaft (im Folgenden zusammengefasst als „Anexia“ bezeichnet) allen unternehmensgruppenweiten Regelungen („Anexia Corporate Binding Rules“) unterliegt und die Auftragsverarbeitungen, die der AN für den AG als Verantwortlichen durchführt, vor allem durch Mitarbeiter von Anexia sowie im Bedarfsfall durch Nutzung von Infrastrukturen und Systemen von Anexia durchgeführt werden. Die aktiven Zertifizierungen von Anexia in den Bereichen ISO 9001 (Qualitätsmanagement), ISO 27001 (Informationssicherheit) und weitere sind jeweils aktuell auf der Unternehmenshomepage von Anexia publiziert.

# 1. GEGENSTAND, ORT UND DAUER DER AUFTRAGSVERARBEITUNG

- 1.1. Gegenstand und Dauer des Auftrags, Art und Zweck, Ort der Verarbeitung und die verarbeiteten Datenkategorien sowie die Kategorien der betroffenen Personen ergeben sich aus den Verträgen zwischen den Parteien oder werden im optionalen **ANHANG 3** gesondert vom AG angegeben. Unter Anwendung der DSGVO obliegt es dem AG als Verantwortlichen, ein Verzeichnis von Verarbeitungstätigkeiten nach Art 30 Abs 1 DSGVO zu führen. Diese Verpflichtung entfällt, wenn für den AG die Ausnahmeregelung nach Art 30 Abs 5 DSGVO zutrifft. Davon unberührt obliegt es dem AN als Auftragsverarbeiter nach Art 30 Abs 2 DSGVO, ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung zu führen, welche sich auch aus **ANHANG 3** sowie aus dem Kontext der Verträge ergeben.
- 1.2. Über den Ort der Verarbeitung unter Berücksichtigung des Kapitels V DSGVO entscheidet ausschließlich der AG als Verantwortlicher. Er weist den AN vertraglich, mittels Weisung oder mittels **ANHANG 3** an, die Verarbeitung entweder ausschließlich innerhalb der EU bzw. des EWR durchzuführen oder diese teilweise oder zur Gänze unter Berücksichtigung der dafür anwendbaren Rechtsgrundlagen auch in vom AG zu benennenden Drittländern oder an bestimmten vom AG zu benennenden spezifischen Standorten durchzuführen.
- 1.3. Die Laufzeit der Auftragsverarbeitung richtet sich nach der Laufzeit der Verträge und den darin vereinbarten Bestimmungen zwischen AG und AN, sofern sich aus den Bestimmungen dieser Vereinbarung oder aufgrund gesetzlicher Bestimmungen nicht darüber hinausgehende Verpflichtungen ergeben.

## 2. ANWENDUNGSBEREICH UND VERANTWORTLICHKEIT

- 2.1. Der AN („Auftragsverarbeiter“ gemäß Art 4 DSGVO) verarbeitet Daten im Auftrag des AG. Dies umfasst jene Tätigkeiten, die in den Verträgen konkretisiert sind. Der AG („Verantwortlicher“ gemäß Art 4 DSGVO) ist im Rahmen dieser Verträge für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz, insbesondere für die Rechtmäßigkeit der Verarbeitung an sich sowie der Datenweitergabe an den AN als Auftragsverarbeiter allein verantwortlich.
- 2.2. Die Weisungen des AG werden durch die Verträge festgelegt und können vom AG in schriftlicher Form (auch elektronische Textform) an den AN durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Etwaige mündliche Weisungen sind unverzüglich schriftlich in Textform zu bestätigen.

## 3. PFLICHTEN DES AN ALS AUFTRAGSVERARBEITER

- 3.1. Der AN verpflichtet sich, Daten und Verarbeitungsergebnisse nur im Rahmen des Auftrages gemäß Vertrag und der Weisungen des AG zu verarbeiten, außer es liegt ein Ausnahmefall im Sinne des Art 28 Abs 3 lit a DSGVO vor. Der AN informiert den AG unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der AN darf die Umsetzung dieser Weisung dann solange aussetzen, bis dies vom AG widerlegt oder die Weisung entsprechend gesetzeskonform abgeändert wurde.
- 3.2. Der AN verpflichtet sich zur Sicherheit der Verarbeitung nach Art 32 Abs 1 lit a bis c DSGVO als Auftragsverarbeiter unter Berücksichtigung der Machbarkeit im Rahmen der gültigen Verträge mit dem AG und gewährleistet nach Art 32 Abs 1 lit d DSGVO ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen einzusetzen. Dieses Verfahren ist unter anderem durch die erfolgreichen, wiederkehrenden Zertifizierungen von Anexia nach ISO 9001 und ISO 27001 gewährleistet und wird dem AG gemäß Kapitel 7 nachgewiesen. Einzelheiten zu den vom AN nach Art 32 DSGVO getroffenen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung sind in **ANHANG 1** angeführt.
- 3.3. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem AN ohne gesonderte Ankündigung dann vorbehalten, wenn das vertraglich vereinbarte Schutzniveau dadurch nicht unterschritten wird und sie nicht der DSGVO widersprechen. Im Standardfall handelt es sich dabei um Verbesserungen der Datensicherheit durch Maßnahmen im Sinne von Informationssicherheit, Datenschutz und Qualitätsmanagement.
- 3.4. Der AN hat in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der AN und Anexia treffen technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des AG, die den Anforderungen des Art 32 DSGVO genügen. Der AN und Anexia treffen hierbei insbesondere Maßnahmen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Für die Einhaltung der vereinbarten Schutzmaßnahmen und deren geprüfte Wirksamkeit wird auf die



aktiven Zertifizierungen des Qualitätsmanagementsystems nach ISO 9001 und des Informationssicherheitsmanagementsystems nach ISO 27001 wesentlicher Teile der der Anexia-Unternehmensgruppe durch anerkannte, DAkkS-akkreditierte Prüf- und Zertifizierungsstellen verwiesen, deren Zertifikate dem AG als Nachweis geeigneter Garantien bezüglich dieser Normen ausreichen. Diese Zertifikate werden dem AG auf Anfrage vorgelegt und sind auch auf der Unternehmenshomepage von Anexia veröffentlicht.

- 3.5. Der AN gewährleistet, dass es den mit der Verarbeitung der Daten des AN befassten Mitarbeitern und anderen für den AN tätigen Personen per Verpflichtung untersagt ist, die Daten unbefugt zu verarbeiten (Datengeheimnis entsprechend § 6 DSGVO) und er unterliegt dem Kommunikationsgeheimnis gemäß § 93 TKG 2003. Diese Verpflichtung besteht auch nach Beendigung der Mitarbeit beim AN sowie nach Beendigung des Vertragsverhältnisses fort.
- 3.6. Der AN unterstützt den AG im Rahmen seiner Möglichkeiten bei der Erfüllung der Rechte betroffener Personen nach Kapitel III DSGVO. Darüberhinausgehend unterstützt der AN den AG bei der Einhaltung der in Art 32 bis 36 DSGVO genannten Pflichten des AG im Rahmen der technischen und organisatorischen Machbarkeit, soweit dies nicht in den Verträgen mit dem AG anders geregelt ist.
- 3.7. Der AN unterrichtet den AG unverzüglich, wenn ihm Verletzungen des Schutzes der Daten des AG bekannt werden. Der AN trifft in solchen Fällen die erforderlichen Maßnahmen zur Sicherung der Daten (entsprechend der Weisung des AG) zur Minderung möglicher nachteiliger Folgen für die betroffenen Personen und spricht sich hierzu unverzüglich mit dem AG ab.
- 3.8. Der AN berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der AG dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der AN die datenschutzkonforme Vernichtung von jeglichen betroffenen Datenträgern und sonstigen Materialien aufgrund einer Einzelweisung durch den AG oder gibt diese Datenträger an den AG zurück, sofern nicht anders im Vertrag vereinbart. In besonderen, vom AG zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe an vom AG zu bestimmende Dritte, wobei Vergütung und Schutzmaßnahmen hierzu gesondert zu vereinbaren sind, sofern nicht bereits in den Verträgen geregelt.
- 3.9. Daten, Datenträger sowie sämtliche sonstigen Materialien werden vom AN nach Vertragsende auf Verlangen des AG analog Punkt 3.8 entweder herausgegeben oder gelöscht. Im Falle von Test- und Ausschussmaterialien ist eine Einzelweisung für die Löschung nicht erforderlich. Entstehen zusätzliche Kosten durch vom AG davon abweichende, marktunübliche und nicht aus geltendem Datenschutzrecht oder aus den Verträgen resultierende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der AG.
- 3.10. Im Falle einer Inanspruchnahme des AG durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art 82 DSGVO, verpflichtet sich der AN, den AG bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten bestens zu unterstützen.

## 4. PFLICHTEN DES AG ALS VERANTWORTLICHER

- 4.1. Der AG als Verantwortlicher stellt sicher, dass die Verarbeitung gemäß den Grundsätzen nach Kapitel II DSGVO erfolgt und die vom AN als Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen (**ANHANG 1**) und jene in den Verträgen gegebenenfalls darüberhinausgehend festgelegten Maßnahmen unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen ein angemessenes Schutzniveau bieten.
- 4.2. Der AG hat den AN unverzüglich und vollständig zu informieren, wenn er in den Auftragsverarbeitungsergebnissen Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.
- 4.3. Im Falle einer Inanspruchnahme des AG durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art 82 DSGVO gilt Punkt 3.10 sinngemäß.

## 5. DATENSCHUTZBEAUFTRAGTER UND KONTAKT

- 5.1. Allgemeine Datenschutzfragen des AG können jederzeit an die explizit hierfür eingerichtete Stelle bei Anexia per E-Mail an [data-protection@anexia-it.com](mailto:data-protection@anexia-it.com) gestellt werden. Unabhängig von gesetzlichen Erfordernissen des AN hat die Anexia-Unternehmensgruppe einen gemeinsamen Datenschutzbeauftragten (Group Data Protection Officer, DPO) benannt, der die Einhaltung der datenschutzrechtlichen Vorschriften bei Anexia und beim AN überwacht und für den AG als Hauptansprechpartner zu Datenschutzfragen im Zuge der Vertragserfüllung fungiert. Name und

Kontaktdaten des Group DPO werden jeweils aktuell auf der Homepage des AN sowie auf der Anexia-Unternehmenshomepage veröffentlicht.

- 5.2. Der AG nennt dem AN einen oder mehrere Ansprechpartner für alle im Rahmen der Verträge inklusive der gegenständlichen Vereinbarung anfallenden Datenschutzfragen:

| Vorname | Nachname | E-Mail            | Telefon |
|---------|----------|-------------------|---------|
| Ines    | Schnur   | i.schnur@arivo.co |         |
| Dominik | Wieser   | d.wieser@arivo.co |         |

## 6. ANFRAGEN BETROFFENER PERSONEN

- 6.1. Wendet sich eine betroffene Person mit Forderungen nach Kapitel III DSGVO (z. B. Berichtigung, Löschung oder Auskunft) an den AN, wird dieser die betroffene Person an den AG verweisen, sofern eine Zuordnung zum AG nach Angaben der betroffenen Person möglich ist. Der AN leitet den Antrag der betroffenen Person unverzüglich an den AG weiter. Der AN unterstützt den AG bei der Erfüllung von Betroffenenanfragen im Rahmen seiner Möglichkeiten und auf Weisung des AG, soweit in den Verträgen nicht anders vereinbart.
- 6.2. Der AN haftet nicht, wenn das Ersuchen der betroffenen Person vom AG nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

## 7. NACHWEISMÖGLICHKEITEN UND INSPEKTIONSRECHTE

- 7.1. Der AN weist bei Bedarf seitens AG die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten mit geeigneten Mitteln nach. Dieser Nachweis erfolgt nach Maßgabe von Anexia und des AN in Abstimmung mit dem AG und kann unter anderem umfassen:
- Zertifikat zum Informationssicherheitsmanagementsystem nach ISO 27001
  - Zertifikat zum Qualitätsmanagementsystem nach ISO 9001
  - Datenschutz Zertifizierungen bzw. Datenschutzgütesiegel soweit vorhanden
  - Aktualisiertes Verzeichnis der technischen und organisatorischen Maßnahmen (**ANHANG 1**)
  - Datenschutzrelevante interne Auditberichte bei erweitertem Bedarf soweit vorhanden
- 7.2. Der AG erklärt hiermit, dass ihm im Sinne seiner Kontroll- und Inspektionsrechte die aufrechte ISO 27001 Zertifizierung von Anexia durch unabhängige DAkkS-akkreditierte Prüf- und Zertifizierungsstellen sowie gegebenenfalls vorhandene Datenschutz Zertifizierungen grundsätzlich Genüge tun. Darüberhinausgehend steht für den Bedarf nicht anlassbezogener Inspektionen durch den AG oder einen von diesem beauftragten Prüfer die Möglichkeit, nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit von mindestens vier Wochen an periodisch stattfindenden Führungen an ausgewählten Betriebs- und Rechenzentrumsstandorten des AN teilzunehmen, um sich von der Umsetzung der technischen und organisatorischen Sicherheitsmaßnahmen vor Ort selbst zu überzeugen.
- 7.3. Der AN darf sowohl anlassbezogene als auch nicht anlassbezogene Inspektionen von der vorherigen Anmeldung entsprechend Punkt 7.2 und von der Unterzeichnung einer Vertraulichkeits- und Geheimhaltungsvereinbarung (Non Disclosure Agreement, NDA) hinsichtlich firmeninterner Informationen des AN, der Daten anderer Kunden des AN und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den AG beauftragte Prüfer in einem Wettbewerbsverhältnis zu Anexia stehen, hat der AN gegen diesen ein Einspruchsrecht. Der AG stimmt dann der Benennung eines unabhängigen externen Prüfers durch den AN zu, dessen Auditbericht und Ergebnisse dem AG zur Verfügung gestellt werden.
- 7.4. Der Aufwand einer nicht anlassbezogenen Routineinspektion gemäß Punkt 7.2 durch den AG ist grundsätzlich auf einen Termin pro Kalenderjahr begrenzt, sofern in den Verträgen nicht gesondert geregelt. Für die Unterstützung bei der Durchführung von darüberhinausgehenden, nicht anlassbezogenen Inspektionen ist eine entsprechende Vergütung zwischen den Parteien zu vereinbaren. In diesem Zusammenhang allenfalls weitergehende in der DSGVO



zwingend vorgesehene Rechte gelten als vereinbart und gehen im Falle von Widersprüchen mit den Bestimmungen unter Punkt 7 vor.

- 7.5. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des AG eine anlassbezogene Inspektion vornehmen, so ist eine Unterzeichnung einer Vertraulichkeits- und Geheimhaltungsvereinbarung gemäß Punkt 7.3 dann nicht erforderlich, wenn diese Aufsichtsbehörde bereits einer berufsrechtlichen oder gesetzlichen Verschwiegenheitspflicht unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

## 8. WEITERE AUFTRAGSVERARBEITER

- 8.1. Der AG erteilt hiermit seine Zustimmung zur Verarbeitung der Daten durch die in **ANHANG 2** (Auflistung verbundener Unternehmen der Anexia-Unternehmensgruppe) konkret festgelegten Unternehmen als weitere Auftragsverarbeiter, soweit dies für die Leistungserbringung gemäß Verträgen erforderlich ist. Der AN verpflichtet sich hierbei zur vollinhaltlichen Überbindung der gesetzlichen und aller vertraglichen Datenschutzverpflichtungen an diese unternehmensgruppeninternen weiteren Auftragsverarbeiter. Anexia hat hierfür „Corporate Binding Rules“ in Form einer Rahmenvereinbarung zu Datenschutz und Auftragsverarbeitung als verbindliches schriftliches Rechtsinstrument, eine unternehmensgruppenweite und für alle Mitarbeiter und beauftragten Personen verbindliche Datenschutzrichtlinie sowie ein Datenschutzmanagementsystem (DSMS) etabliert.
- 8.2. Der Einsatz von Subunternehmern bzw. Subdienstleistern als weitere Auftragsverarbeiter ist nur zulässig, wenn der AG vorher schriftlich zugestimmt hat. Die Regelung zu Subunternehmern in Angeboten oder Verträgen zwischen AG und AN gilt vorrangig zu dieser Regelung und entspricht einer solchen schriftlichen Zustimmung des AG.
- 8.3. Neben der konkreten Festlegung von verbundenen Unternehmen der Anexia-Unternehmensgruppe gemäß Punkt 8.1 werden ebenfalls in **ANHANG 2** alle zustimmungspflichtigen Subunternehmen, die als weitere Auftragsverarbeiter für den AG fungieren, angeführt und gelten durch Abschluss der gegenständlichen Vereinbarung als schriftlich genehmigt.
- 8.4. Ein zustimmungspflichtiges Subunternehmerverhältnis als weiterer Auftragsverarbeiter nach Punkt 8.2 liegt vor, wenn der AN weitere Unternehmen mit der ganzen oder einer Teilleistung der in den Verträgen zwischen AG und AN vereinbarten Leistung beauftragt und dabei die Kerntätigkeit in der Verarbeitung personenbezogener Daten des AG als Verantwortlichen besteht. Um ein nicht zustimmungspflichtiges Subunternehmerverhältnis handelt es sich bei der bloßen Erbringung von untergeordneten Nebenleistungen, bei denen die Kerntätigkeit nicht in der Auftragsverarbeitung personenbezogener Daten liegt (z. B. reine Infrastrukturbereitstellung, Telekommunikations-, Post- oder Reinigungsdienstleistungen, Wachschatz).
- 8.5. Erteilt der AN nach erfolgter schriftlicher Zustimmung des AG Aufträge an weitere Auftragsverarbeiter, so ist der AN verpflichtet, alle gesetzlichen und vertraglichen Datenschutzverpflichtungen, denen er gegenüber dem AG unterliegt, an diese weiteren Auftragsverarbeiter vollinhaltlich zu überbinden.

## 9. INFORMATIONSPFLICHTEN, SCHRIFTFORM, SALVATORISCHE KLAUSEL UND RECHTSWAHL

- 9.1. Sollten die Daten des AG beim AN durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der AN den AG unverzüglich darüber zu informieren. Der AN wird alle in diesem Zusammenhang Agierenden unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim AG als Verantwortlichem im Sinne der DSGVO liegen.
- 9.2. Änderungen und Ergänzungen dieser Vereinbarung und all ihrer Bestandteile bedürfen Ergänzungsvereinbarungen in Schriftform und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung zu dieser Vereinbarung handelt. Dies gilt auch für den Verzicht auf dieses Schriftformerfordernis.
- 9.3. Bei etwaigen datenschutzrechtlichen Widersprüchen oder Unschärfen gehen Regelungen dieser Vereinbarung zum Datenschutz den Regelungen der Verträge vor. Sollten einzelne Teile dieses Dokuments unwirksam sein oder werden, so berührt dies die Wirksamkeit des Dokuments im Übrigen nicht.
- 9.4. Es gilt österreichisches Recht.

## 10. HAFTUNG UND SCHADENERSATZ

Der AG und der AN haften gegenüber betroffenen Personen datenschutzrechtlich entsprechend der in Art 82 DSGVO getroffenen Regelung. Jegliche nicht datenschutzrechtlichen bzw. darüberhinausgehenden oder individuellen Haftungs- und Schadenersatzregelungen sind ausschließlich in den Angeboten und Verträgen zwischen dem AG und dem AN zu vereinbaren.

## 11. VERTRAULICHKEIT UND VERSCHWIEGENHEIT

Beide Parteien verpflichten sich zur grundsätzlichen Vertraulichkeit und zur Verschwiegenheit bezüglich der Inhalte dieser Vereinbarung. Davon ausgenommen sind gesetzliche Offenlegungspflichten gegenüber Behörden, in Gerichts- oder Strafverfahren sowie vertragliche Verpflichtungen gegenüber Personen und Auditoren sowohl des AG als auch des AN, die sich zur Vertraulichkeit gegenüber dem AG bzw. dem AN verpflichten oder einer Verschwiegenheitsverpflichtung gemäß Punkt 7.5 unterliegen und letztlich auch weitere Auftragsverarbeiter und verbundene Unternehmen, für die die gegenständlichen Festlegungen einen integralen Bestandteil im Rahmen ihrer Tätigkeitserfüllung darstellen.

Graz, 13.03.2023

Ort, Datum

  
Arivo Parking Solutions GmbH  
Am Innovationspark 10, 8020 Graz, Austria  
ATU 68330419 FN467497x  
Info@arivo.co | +43 316 375 018 www.arivo.co

AG

Graz, 14.03.2023

Ort, Datum

  
TELEMATICA  
Internet Service Provider GmbH  
Münzgrabenstraße 84b/5, 8010 Graz  
FN: 40 74 53 x | UID: ATU 68330415  
www.telematica.at | +43 (0)5 056 400-0

*Vo.T. Kömmer*

AN

### Anlagen

- ☒ ANHANG 1 – Technische und organisatorische Maßnahmen
- ☐ ANHANG 2 – Weitere Auftragsverarbeiter
- ☐ ANHANG 3 – Auftragsverarbeitungsspezifikationen



# AVV ANHANG 1

## TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN

Das gegenständliche Dokument ergänzt die zwischen AG und AN abgeschlossene Auftragsverarbeitungsvereinbarung (AVV) gemäß Art 28 DSGVO (EU-Datenschutzgrundverordnung).

Die technischen und organisatorischen Maßnahmen werden vom AN und Anexia entsprechend Art 32 DSGVO umgesetzt. Sie werden laufend nach Machbarkeit und Stand der Technik – nicht zuletzt auch im Sinne der aktiven ISO 27001 Zertifizierung – verbessert und auf ein höheres Sicherheits- und Schutzniveau gebracht.

### 1. VERTRAULICHKEIT

#### 1.1. Zutrittskontrolle

*Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.*

| Technische Maßnahmen                           | Organisatorische Maßnahmen                 |
|------------------------------------------------|--------------------------------------------|
| ✓ Alarmanlage                                  | ✓ Schlüsselregelung / Liste                |
| ✓ Automatisches Zugangskontrollsystem          | ✓ Empfang / Rezeption / Pförtner           |
| ✓ Biometrische Zugangssperren                  | ✓ Besucherbuch / Protokoll der Besucher    |
| ✓ Chipkarten / Transpondersysteme              | ✓ Mitarbeiter- / Besucherausweise          |
| ✓ Manuelles Schließsystem                      | ✓ Besucher in Begleitung durch Mitarbeiter |
| ✓ Türen mit Knauf Außenseite                   | ✓ Sorgfalt bei Auswahl des Wachpersonals   |
| ✓ Klingelanlage mit Kamera                     | ✓ Sorgfalt bei Auswahl Reinigungsdienste   |
| ✓ Videoüberwachung der Eingänge                | ✓ Richtlinie Informationssicherheit        |
| ✓ Biometrische Zutrittskontrolle Rechenzentrum | ✓ Arbeitsanweisung Betriebssicherheit      |
|                                                | ✓ Arbeitsanweisung Zutrittssteuerung       |

#### 1.2. Zugangskontrolle

*Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*

| Technische Maßnahmen                                                      | Organisatorische Maßnahmen             |
|---------------------------------------------------------------------------|----------------------------------------|
| ✓ Login mit Benutzername + Starkes Passwort                               | ✓ Verwalten von Benutzerberechtigungen |
| ✓ Anti-Viren-Software Server                                              | ✓ Erstellen von Benutzerprofilen       |
| ✓ Anti-Virus-Software Clients                                             | ✓ Zentrale Passwortvergabe             |
| ✓ Anti-Virus-Software mobile Geräte                                       | ✓ Richtlinie Informationssicherheit    |
| ✓ Firewall                                                                | ✓ Arbeitsanweisung IT-Benutzerordnung  |
| ✓ Intrusion Detection Systeme                                             | ✓ Arbeitsanweisung Betriebssicherheit  |
| ✓ Einsatz VPN bei Remote-Zugriffen                                        | ✓ Arbeitsanweisung Zugangssteuerung    |
| ✓ Verschlüsselung von Datenträgern                                        | ✓ Mobile Device Policy                 |
| ✓ Verschlüsselung Smartphones                                             |                                        |
| ✓ Automatische Desktopsperre                                              |                                        |
| ✓ Verschlüsselung von Notebooks / Tablet                                  |                                        |
| ✓ Zwei-Faktor-Authentifizierung im RZ-Betrieb und bei kritischen Systemen |                                        |

### 1.3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

| Technische Maßnahmen                                                                                                                                                                                                                                                                                                                                                                                                                          | Organisatorische Maßnahmen                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>✓ Aktenshredder mind. empfohlene Sicherheitsstufe P-4 (DIN 66399)</li><li>✓ Externer Aktenvernichtung mind. Sicherheitsstufe P-6 (DIN 66399)</li><li>✓ Physische Löschung von Datenträgern</li><li>✓ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten</li><li>✓ Zugriffe SSH Verschlüsselt</li><li>✓ zertifizierte SSL Verschlüsselung</li></ul> | <ul style="list-style-type: none"><li>✓ Einsatz Berechtigungskonzepte</li><li>✓ Minimale Anzahl an Administratoren</li><li>✓ Verwaltung Benutzerrechte durch Administratoren</li><li>✓ Richtlinie Informationssicherheit</li><li>✓ Arbeitsanweisung Kommunikationssicherheit</li><li>✓ Arbeitsanweisung Umgang mit Informationen und Werten</li></ul> |

### 1.4. Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

| Technische Maßnahmen                                                                                                                                                                                                                                                                                                                                        | Organisatorische Maßnahmen                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>✓ Trennung von Produktiv- und Testumgebung</li><li>✓ Physikalische Trennung (Systeme / Datenbanken / Datenträger)</li><li>✓ Mandantenfähigkeit relevanter Anwendungen</li><li>✓ VLAN-Segmentierung</li><li>✓ Kundensysteme logisch getrennt</li><li>✓ Staging von Entwicklungs-, Test und Produktivumgebung</li></ul> | <ul style="list-style-type: none"><li>✓ Steuerung über Berechtigungskonzept</li><li>✓ Festlegung von Datenbankrechten</li><li>✓ Richtlinie Informationssicherheit</li><li>✓ Richtlinie Datenschutz</li><li>✓ Arbeitsanweisung Betriebssicherheit</li><li>✓ Arbeitsanweisung Sicherheit in der Softwareentwicklung</li></ul> |

### 1.5. Pseudonymisierung

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

| Technische Maßnahmen                                                                                                                                                                                                                 | Organisatorische Maßnahmen                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>✓ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem System (verschlüsselt)</li><li>✓ auf Wunsch des Kunden werden Logfiles pseudonymisiert</li></ul> | <ul style="list-style-type: none"><li>✓ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren</li><li>✓ Richtlinie Informationssicherheit</li><li>✓ Richtlinie Datenschutz</li><li>✓ Separate, explizite Arbeitsanweisung Kryptographie (dzt. in Ausarbeitung)</li></ul> |



## 2. INTEGRITÄT

### 2.1. Weitergabekontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*

| Technische Maßnahmen                                                                                                                                                                                                                                                      | Organisatorische Maßnahmen                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>✓ Einsatz von VPN</li><li>✓ Protokollierung der Zugriffe und Abrufe</li><li>✓ Bereitstellung über verschlüsselte Verbindungen wie sftp, https – Secure Cloudstores</li><li>✓ Nutzung von Signaturverfahren (fallabhängig)</li></ul> | <ul style="list-style-type: none"><li>✓ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen</li><li>✓ Weitergabe in anonymisierter oder pseudonymisierter Form</li><li>✓ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen</li><li>✓ Persönliche Übergabe mit Protokoll</li><li>✓ Richtlinie Informationssicherheit</li><li>✓ Richtlinie Datenschutz</li></ul> |

### 2.2. Eingabekontrolle

*Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können.*

| Technische Maßnahmen                                                                                                                                                                                                        | Organisatorische Maßnahmen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>✓ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten</li><li>✓ Manuelle oder automatisierte Kontrolle der Protokolle (nach strikten internen Vorgaben)</li></ul> | <ul style="list-style-type: none"><li>✓ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können</li><li>✓ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen)</li><li>✓ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts</li><li>✓ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden</li><li>✓ Klare Zuständigkeiten für Löschungen</li><li>✓ Richtlinie Informationssicherheit</li><li>✓ Arbeitsanweisung IT-Benutzerordnung</li></ul> |

### 3. VERFÜGBARKEIT UND BELASTBARKEIT

#### 3.1. Verfügbarkeitskontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (USV, Klimaanlage, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidssysteme, Plattenspiegelungen etc.).*

| Technische Maßnahmen                                                                                                                                                                                                                                                                                                                                                                                                                                               | Organisatorische Maßnahmen                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>✓ Feuer- und Rauchmeldeanlagen</li><li>✓ Feuerlöscher Serverraum</li><li>✓ Serverraumüberwachung Temperatur und Feuchtigkeit</li><li>✓ Serverraum klimatisiert</li><li>✓ USV-Anlage und Notrom-Dieselaggregate RZ</li><li>✓ Schutzsteckdosenleisten Serverraum</li><li>✓ RAID System / Festplattenspiegelung</li><li>✓ Videoüberwachung Serverraum</li><li>✓ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum</li></ul> | <ul style="list-style-type: none"><li>✓ Backup-Konzept</li><li>✓ Keine sanitären Anschlüsse im Serverraum</li><li>✓ Existenz eines Notfallplans</li><li>✓ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums</li><li>✓ Getrennte Partitionen für Betriebssysteme und Daten, wo notwendig</li><li>✓ Richtlinie Informationssicherheit</li><li>✓ Arbeitsanweisung Betriebssicherheit</li><li>✓ Regelmäßige Tests der Dieselaggregate RZ</li></ul> |

#### 3.2. Wiederherstellbarkeit

*Maßnahmen die dazu befähigen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.*

| Technische Maßnahmen                                                                                                                                                                                        | Organisatorische Maßnahmen                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>✓ Backup-Monitoring und -Reporting</li><li>✓ Wiederherstellbarkeit aus Automatisierungs-Tools</li><li>✓ Backup-Konzept nach Kritikalität und Kundenvorgaben</li></ul> | <ul style="list-style-type: none"><li>✓ Recovery-Konzept</li><li>✓ Kontrolle des Sicherungsvorgangs</li><li>✓ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse</li><li>✓ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums</li><li>✓ Existenz eines Notfallplans</li><li>✓ Richtlinie Informationssicherheit</li><li>✓ Arbeitsanweisung Betriebssicherheit</li></ul> |

## 4. VERFAHREN ZUR ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

### 4.1. Datenschutzmanagement

| Technische Maßnahmen                                                                                                                                                                                                                                                                                                                                                                                        | Organisatorische Maßnahmen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>✓ Zentrale Dokumentation aller Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter</li><li>✓ Sicherheitszertifizierung nach ISO 27001</li><li>✓ Eine Überprüfung der Wirksamkeit der TOM wird mind. jährlich durchgeführt und TOMs aktualisiert</li><li>✓ Datenschutzprüfpunkte durchgängig in Tool-gestütztem Risk Assessment implementiert</li></ul> | <ul style="list-style-type: none"><li>✓ Interner Datenschutzbeauftragter bestellt: Group Data Protection Officer, DPO</li><li>✓ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet</li><li>✓ Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich</li><li>✓ Interner Informationssicherheits-Beauftragter bestellt: Group Information Security Officer, ISO</li><li>✓ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt</li><li>✓ Prozess betr. Informationspflichten nach Art. 13 und 14 DSGVO etabliert</li><li>✓ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden</li><li>✓ Datenschutzbetrachtung im Rahmen des Corporate Risk Managements etabliert</li><li>✓ ISO 27001 Zertifizierung wesentlicher Unternehmensteile inkl. RZ-Betrieb und jährliche Überwachungsaudits</li></ul> |

### 4.2. Incident-Response-Management

*Unterstützung bei der Reaktion auf Sicherheitsverletzungen sowie Data Breach Prozess.*

| Technische Maßnahmen                                                                                                                                                                                                                                                                                                                                                                               | Organisatorische Maßnahmen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>✓ Einsatz von Firewall und regelmäßige Aktualisierung</li><li>✓ Einsatz von Spamfilter und regelmäßige Aktualisierung</li><li>✓ Einsatz von Virens Scanner und regelmäßige Aktualisierung</li><li>✓ Intrusion Detection System (IDS) für Kundensysteme auf Bestellung</li><li>✓ Intrusion Prevention System (IPS) für Kundensysteme auf Bestellung</li></ul> | <ul style="list-style-type: none"><li>✓ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)</li><li>✓ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen</li><li>✓ Einbindung von DPO und ISO in Sicherheitsvorfälle und Datenpannen</li><li>✓ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen</li><li>✓ Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem</li><li>✓ Formaler Prozess zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen</li><li>✓ Richtlinie Informationssicherheit</li><li>✓ Richtlinie Datenschutz</li><li>✓ Arbeitsanweisung Betriebssicherheit</li><li>✓ Arbeitsanweisung IT-Benutzerordnung</li></ul> |



#### 4.3. Datenschutzfreundliche Voreinstellungen

„Privacy by design“ / „Privacy by default“ gem. Art 25 Abs 2 DSGVO.

| Technische Maßnahmen                                                                                                                                                                                                                                   | Organisatorische Maßnahmen                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>✓ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind</li><li>✓ Anwendung datenschutzfreundlicher Voreinstellung in Standard- sowie Individualsoftware</li></ul> | <ul style="list-style-type: none"><li>✓ Richtlinie Datenschutz (inkludiert Prinzipien „Privacy by design / default“)</li><li>✓ OWASP Secure Mobile Development Security Checks werden durchgeführt</li><li>✓ Perimeteranalyse bei Webapplikationen</li></ul> |

#### 4.4. Auftragskontrolle (Outsourcing, Subauftragnehmer und Auftragsverarbeitung)

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

| Technische Maßnahmen                                                                                                                                                                                                                                    | Organisatorische Maßnahmen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>✓ Überwachung von Remote-Zugriffen Externer z. B. im Rahmen von Remote-Support</li><li>✓ Überwachung von Subunternehmern nach den Prinzipien und mit den Technologien gem. vorausgehenden Kapiteln 1, 2</li></ul> | <ul style="list-style-type: none"><li>✓ Arbeitsanweisung Lieferantenmanagement und Lieferantenbewertung</li><li>✓ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation</li><li>✓ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)</li><li>✓ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln</li><li>✓ Rahmenvereinbarung zur Auftragsverarbeitung innerhalb der Unternehmensgruppe</li><li>✓ Schriftliche Weisungen an den Auftragnehmer</li><li>✓ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis</li><li>✓ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer</li><li>✓ Regelung zum Einsatz weiterer Subunternehmer</li><li>✓ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags</li><li>✓ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus</li></ul> |

## 5. ORGANISATION UND DATENSCHUTZ BEI ANEXIA

- 5.1. Die Anexia Unternehmensgruppe hat sich in ihrer **strategischen Leitlinie Qualitäts-, Risiko- und Compliance-Politik** unter anderem zum Ziel gesetzt, ihren Kunden die zu liefernden Produkte und Services auf **höchstmöglichem Informationssicherheitsniveau rechtskonform** zur Verfügung zu stellen. Diese Leitlinie bildet den Rahmen für eine **transparente, nachhaltige, prozessbasierte und risikoorientierte Steuerung** der Unternehmensgruppe im Rahmen eines **Integrierten Management Systems (IMS)**.
- 5.2. Anexia hat in diesem Zusammenhang eine ausgeprägte **Sicherheits-Querschnittsorganisation** etabliert, um einen umfassenden Schutz ihrer eigenen Unternehmensinformationen- und Daten sowie den Schutz der Daten ihrer Kunden und Auftraggeber zu gewährleisten. Dabei sind die Funktionen **Information Security Officer (ISO)**, **Data Protection Officer (DPO)**, **Quality Officer (QO)**, **Risk Officer (RO)** sowie **Legal Compliance Officer (LCO)** mit gruppenweiter Verantwortung und direktem Weisungsrecht in diesen Wirkungsbereichen innerhalb der **direkt dem CEO zugeordneten Stabsabteilung „Quality, Risk & Compliance“** eingerichtet und ein umfassendes Regelwerk aus **internen Richtlinien und Regelungen („Anexia Corporate Binding Rules“** u. a. zu Informationssicherheit und Datenschutz) etabliert, das für alle Mitarbeiter verbindlich einzuhalten ist und einen sicheren und datenschutzkonformen Umgang mit Informationen und Daten festlegt.
- 5.3. Die **Mitarbeiter** werden laufend **auf dem Gebiet des Datenschutzes informiert und geschult**. Darüberhinausgehend sind alle Mitarbeiter dienstvertraglich zum **Datengeheimnis und zur Geheimhaltung verpflichtet**. **Externe**, die im Rahmen ihrer Tätigkeit für Anexia in Berührung mit personenbezogenen Daten kommen könnten, werden vor Beginn ihrer Tätigkeit zur Verschwiegenheit und Geheimhaltung sowie zur Einhaltung von Datenschutz und Datengeheimnis mittels einem sogenannten **NDA (Non-Disclosure-Agreement)** verpflichtet.
- 5.4. Alle verbundenen Unternehmen der Anexia Unternehmensgruppe innerhalb der EU bzw. des EWR haben eine gemeinsame **Rahmenvereinbarung zu Datenschutz und Auftragsverarbeitung** als verbindliches schriftliches Rechtsinstrument gemäß Art 28 DSGVO abgeschlossen, um einen einheitlich hohen Datenschutz- und Datensicherheitsstandard über die gesamte Gruppe hinweg zu gewährleisten und die Rechte und Pflichten bei jeglichen Auftragsverarbeitungen klar zu regeln. Jegliche mit weiterer Auftragsverarbeitung betraute Subunternehmen werden erst nach Genehmigung des Verantwortlichen und nach Abschluss einer Auftragsverarbeitungsvereinbarung (AVV) nach Art 28 DSGVO eingesetzt, mit welcher ihnen alle datenschutzrechtlichen Pflichten, denen Anexia selbst unterliegt, vollinhaltlich überbunden werden.
- 5.5. All diese organisatorischen Maßnahmen flankieren die jeweils aktuellen, **hohen technischen Sicherheitsstandards** von Anexia und beide Dimensionen werden **periodisch** im Zuge **interner Audits** sowie jährlich im Rahmen der **ISO 9001 und ISO 27001 Überwachungs- bzw. Re-Zertifizierungsaudits** von unabhängigen, externen, **DAKKS-akkreditierten Zertifizierungsstellen** auf ihre Angemessenheit und Wirksamkeit überprüft und bestätigt.

## 6. ZERTIFIZIERUNGEN

Sowohl das **Qualitätsmanagementsystem nach ISO 9001** als auch das **Informationssicherheitsmanagementsystem nach ISO 27001** wesentlicher Teile von **Anexia inkl. DATASIX Rechenzentrumsbetrieb** sind durch die unabhängige TÜV NORD CERT GmbH **zertifiziert**.

| Maßnahme                       | DSGVO-konform umgesetzt | Kommentare                        |
|--------------------------------|-------------------------|-----------------------------------|
| Zutrittskontrolle              | ✓                       | ISO 27001 & ISO 9001 zertifiziert |
| Zugangskontrolle               | ✓                       | ISO 27001 & ISO 9001 zertifiziert |
| Zugriffskontrolle              | ✓                       | ISO 27001 & ISO 9001 zertifiziert |
| Weitergabekontrolle            | ✓                       | ISO 27001 & ISO 9001 zertifiziert |
| Eingabekontrolle               | ✓                       | ISO 27001 & ISO 9001 zertifiziert |
| Auftragskontrolle              | ✓                       | ISO 27001 & ISO 9001 zertifiziert |
| Verfügbarkeitskontrolle        | ✓                       | ISO 27001 & ISO 9001 zertifiziert |
| Trennungskontrolle             | ✓                       | ISO 27001 & ISO 9001 zertifiziert |
| Innerbetriebliche Organisation | ✓                       | ISO 27001 & ISO 9001 zertifiziert |





## AVV ANHANG 2

### WEITERE AUFTRAGSVERARBEITER (VERBUNDENE UNTERNEHMEN)

Die folgenden verbundene Unternehmen (siehe Auswahl) im Geltungsbereich der „Anexia Corporate Rules zum Datenschutz“ in Form einer Rahmenvereinbarung zu Datenschutz und Auftragsverarbeitung als verbindliches schriftliches Rechtsinstrument gem. Art 28 DSGVO und einer unternehmensgruppenweit gültigen Datenschutzrichtlinie sowie im Vollarwendungsbereich des Anexia Datenschutzmanagementsystems (DSMS) liegend innerhalb der Anexia-Unternehmensgruppe können – je nach Art und Umfang der Auftragsverarbeitung – als weitere Auftragsverarbeiter im Rahmen der Vertrags- und Auftragserfüllung zum Einsatz kommen. Für sie gelten jegliche Bestimmungen und Verpflichtungen der gegenständlichen Auftragsverarbeitungsvereinbarung (AVV) sinngemäß und vollinhaltlich.

Konkrete Festlegung der tatsächlich für im Rahmen der gegenständlichen Auftragsverarbeitungsvereinbarung (AVV) als weiter Auftragsverarbeiter eingesetzten Unternehmen mittels Kontrollkästchenauswahl:

- ☐ ANX Holding GmbH, Klagenfurt, Österreich
- ☐ ANEXIA Internetdienstleistungs GmbH, Klagenfurt, Österreich
- ☐ ANEXIA Deutschland GmbH, München, Deutschland
- ☐ DATASIX Rechenzentrumsbetriebs GmbH, Wien, Österreich

### SONSTIGE WEITERE AUFTRAGSVERARBEITER (SUBUNTERNEHMEN)

Die folgenden Subunternehmen werden im Rahmen der Vertrags- bzw. Auftragserfüllung als sonstige weitere Auftragsverarbeiter eingesetzt. Sie unterliegen ausnahmslos denselben, sich aus der DSGVO und aus der gegenständlichen Vereinbarung ergebenden datenschutzrechtlichen Pflichten gegenüber dem Verantwortlichen und dem Auftragsverarbeiter, die ihnen mittels separater Verträge zur Auftragsverarbeitung als verbindliches schriftliches Rechtsinstrument gem. Art 28 DSGVO überbunden wurden:

Firma

Adresse



## AVV ANHANG 3

Dieser Bereich ist optional und kann auf Wunsch des AG zusätzlich ausgefüllt und vereinbart werden.

### AUFTRAGSVERARBEITUNGSSPEZIFIKATIONEN

#### 1. GEGENSTAND (ART UND ZWECK) DER VERARBEITUNG

- ☐ Der Gegenstand der Auftragsverarbeitung durch den AN für den AG als Verantwortlichen ergibt sich konkret aus den **bestehenden Verträgen** zwischen den Parteien.
- ☐ Die Auftragsverarbeitung hat den **folgenden konkreten Gegenstand:**

[Kurzbeschreibung des Verarbeitungsgegenstands durch den AG]

#### 2. DAUER DER VERARBEITUNG

- ☐ Die Dauer der Auftragsverarbeitung durch den AN für den AG als Verantwortlichen richtet sich nach der Auftragsdauer, die sich **aus den Verträgen** zwischen den Parteien ergibt.
- ☐ Die Auftragsverarbeitung durch den AN erfolgt in **folgendem Zeitraum** (vorbehaltlich darüberhinausgehender gesetzlicher Verpflichtungen):

[Zeitraum der Verarbeitung durch den AG anzuführen]

#### 3. ORT DER VERARBEITUNG

- ☐ Der Ort der Auftragsverarbeitung durch den AN für den AG als Verantwortlichen ergibt sich konkret aus den **bestehenden Verträgen** zwischen den Parteien.
- ☐ Die Verarbeitung hat durch den AN **ausschließlich innerhalb der EU bzw. des EWR** zu erfolgen.
- ☐ Die Verarbeitung kann durch den AN teilweise oder zur Gänze unter Berücksichtigung der dafür anwendbaren Rechtsgrundlagen auch in **folgenden Drittländern** erfolgen:

[Auflistung genehmigter Drittländer durch den AG]

- ☐ Die Verarbeitung soll vom AN **ausschließlich an folgendem/n spezifischen Standort/en** erfolgen:

[Auflistung Standort(e) durch den AG]

## 4. KATEGORIEN BETROFFENER PERSONEN

entweder

- ☐ Die Kategorien der betroffenen Personen, deren Daten verarbeitet werden **ergeben sich aus den Verträgen** zwischen den Parteien **oder sind nur dem AG als Verantwortlichen bekannt** und dieser stellt dabei sicher, dass die Verarbeitung gemäß den Grundsätzen nach Kapitel II DSGVO erfolgt und die vom AN als Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen angemessen sind.

oder

- ☐ Es werden Daten der **folgenden Personenkategorien** verarbeitet:

|                                               |                                                |
|-----------------------------------------------|------------------------------------------------|
| <input type="checkbox"/> Kunden               | <input type="checkbox"/> Mitarbeiter des AG    |
| <input type="checkbox"/> Interessenten        | <input type="checkbox"/> Externe Mitarbeiter   |
| <input type="checkbox"/> Lieferanten          | <input type="checkbox"/> Auftragsverarbeiter   |
| <input type="checkbox"/> Besucher der Website | <input type="checkbox"/> Newsletter-Abonnenten |
| <input type="checkbox"/>                      | <input type="checkbox"/>                       |
| <input type="checkbox"/>                      | <input type="checkbox"/>                       |

[Auswahl und ggf. Auflistung weiterer Betroffenenkategorien durch den AG]

## 5. KATEGORIEN PERSONENBEZOGENER DATEN

entweder

- ☐ Die verarbeiteten Datenkategorien ergeben sich **im Detail aus den Verträgen** zwischen den Parteien **oder sind nur dem AG als Verantwortlichen bekannt** und dieser stellt dabei sicher, dass die Verarbeitung gemäß den Grundsätzen nach Kapitel II DSGVO erfolgt und die vom AN als Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen angemessen sind.

oder

- ☐ Es werden Daten der **folgenden Kategorien** verarbeitet:

|                                                            |                                                                  |
|------------------------------------------------------------|------------------------------------------------------------------|
| <input type="checkbox"/> Namensdaten                       | <input type="checkbox"/> Kontakt- und Adressdaten                |
| <input type="checkbox"/> Geburtsdatum                      | <input type="checkbox"/> Kundenvertragsdaten                     |
| <input type="checkbox"/> Bank- und Zahlungsdaten           | <input type="checkbox"/> Logindaten                              |
| <input type="checkbox"/> Standort und Geoinformationsdaten | <input type="checkbox"/> Daten zu Vorlieben und Verhaltensweisen |
| <input type="checkbox"/> Bildungsdaten                     | <input type="checkbox"/> Bewegungsprofilen                       |
| <input type="checkbox"/> Verkehrsdaten                     | <input type="checkbox"/> Foto- und Videodaten                    |
| <input type="checkbox"/> Strafrechtsrelevante Daten        | <input type="checkbox"/>                                         |
| <input type="checkbox"/>                                   | <input type="checkbox"/>                                         |
| <input type="checkbox"/>                                   | <input type="checkbox"/>                                         |

[Auswahl und ggf. Auflistung weiterer Datenkategorien durch den AG]

und/oder

- ☐ Es werden **keine besonderen Kategorien personenbezogener Daten** („sensible Daten“) verarbeitet.

oder

- ☐ Es werden die **folgenden besonderen Kategorien personenbezogener Daten** („sensible Daten“) verarbeitet:

|                                                                        |                                                                 |
|------------------------------------------------------------------------|-----------------------------------------------------------------|
| <input type="checkbox"/> Rassistische und ethnische Herkunft           | <input type="checkbox"/> Politische Meinungen                   |
| <input type="checkbox"/> Religiöse oder weltanschauliche Überzeugungen | <input type="checkbox"/> Gewerkschaftszugehörigkeit             |
| <input type="checkbox"/> Genetischen Daten                             | <input type="checkbox"/> Gesundheitsdaten                       |
| <input type="checkbox"/> Biometrischen Daten                           | <input type="checkbox"/> Sexualleben oder sexuelle Orientierung |

[Auswahl besonderer Kategorien personenbezogener Daten durch den AG]



# Data Protection Addendum

Last Updated: February 14, 2023

This Data Protection Addendum ("*Addendum*") forms part of the agreement between Customer and Twilio covering Customer's use of the Services (as defined below) ("*Agreement*").

## I. Introduction

### 1. Definitions

- "*Applicable Data Protection Law*" means all laws and regulations applicable to Twilio's processing of personal data under the Agreement.
- "*controller*" means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "*Customer Account Data*" means personal data that relates to Customer's relationship with Twilio, including the names or contact information of individuals authorized by Customer to access Customer's account, and billing information of individuals that Customer has associated with its account. Customer Account Data also includes any personal data Twilio may need to collect for the purpose of identity verification (including providing the Multi-Factor Authentication Services, as defined below), or as part of its legal obligation to retain Subscriber Records (as defined below).
- "*Customer Content*" means (a) personal data exchanged as a result of using the Services (as defined below), such as text message bodies, voice and video media, images, email bodies, email recipients, sound, and, where applicable, details Customer submits to the Services from its designated software applications and services and (b) data stored on Customer's behalf such as communication logs within the Services or marketing campaign data that Customer has uploaded to the Services (as defined below).
- "*Customer Data*" has the meaning given in the Agreement. Customer Data includes Customer Account Data, Customer Usage Data, Customer Content, and Sensitive Data, each as defined in this Addendum.
- "*Customer Usage Data*" means data processed by Twilio for the purposes of transmitting or exchanging Customer Content utilizing phone numbers either through the public switched telephone network or by way of other communication networks. Customer Usage Data includes data used to identify the source and destination of a communication, such as (a) individual data subjects' telephone numbers, data on the location of the device generated in the

providing the Services, and the date, time, duration and the type of communication and (b) activity logs used to identify the source of Service requests, optimize and maintain performance of the Services, and investigate and prevent system abuse.

- *"Multi-Factor Authentication Services"* means the provision of a portion of the Services under which Customer adds an additional factor for verification of Customer's end users' identity in connection with such end users' use of Customer's software applications or services.
- *"personal data"* means any information relating to an identified or identifiable natural person (*"data subject"*). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- *"processor"* means the entity which processes personal data on behalf of the controller.
- *"processing"* (and *"process"*) means any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- *"Security Incident"* means a confirmed or reasonably suspected accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Data.
- *"Sensitive Data"* means (a) social security number, passport number, driver's license number, or similar identifier (or any portion thereof); (b) credit or debit card number (other than the truncated (last four digits) of a credit or debit card), financial information, banking account numbers or passwords; (c) employment, financial, genetic, biometric or health information; (d) racial, ethnic, political or religious affiliation, trade union membership, or information about sexual life or sexual orientation; (e) account passwords, mother's maiden name, or date of birth; (f) criminal history; or (g) any other information or combinations of information that falls within the definition of "special categories of data" under GDPR (as defined below) or any other applicable law or regulation relating to privacy and data protection.
- *"Services"* means the products and services provided by Twilio or its Affiliates, as applicable, that are (a) used by Customer, including, without limitation, products and services that are on a trial basis or otherwise free of charge or (b) ordered by Customer under an order form.
- *"Subscriber Records"* means Customer Account Data containing proof of identification and proof of physical address necessary for Twilio to provide Customer or Customer's end users with phone numbers in certain countries (*"telephone number assignments"*). When required by law or regulation, Subscriber Records are shared with local telecommunications providers, which provide local connectivity services, or local government authorities (additional information about these regulatory requirements is available at <https://www.twilio.com/guidelines/regulatory> (<https://www.twilio.com/guidelines/regulatory>)).
- *"sub-processor"* means (a) Twilio, when Twilio is processing Customer Content and where Customer is a processor of such Customer Content or (b) any third-party processor engaged by Twilio to process Customer Content in order to provide the Services to Customer. For the avoidance of doubt, telecommunication providers are not sub-processors.



- “*Third Party Request*” means any request, correspondence, inquiry, or complaint from a data subject, regulatory authority, or third party.
- “*Twilio Privacy Notice*” means the privacy notice for the Services, the current version of which is available at <https://www.twilio.com/legal/privacy> (<https://www.twilio.com/legal/privacy>).

Any capitalized term not defined in this Section 1 will have the meaning provided in this Addendum or the Agreement.

## II. Controller and Processor

### 2. Relationship

2.1 Twilio as a Processor. Customer and Twilio agree that with regard to the processing of Customer Content, Customer may act either as a controller or processor and Twilio is a processor. Twilio will process Customer Content in accordance with Customer’s instructions as set forth in Section 5 (Customer Instructions).

2.2 Twilio as a Controller of Customer Account Data. Customer and Twilio acknowledge that, with regard to the processing of Customer Account Data, Customer is a controller and Twilio is an independent controller, not a joint controller with Customer. Twilio will process Customer Account Data as a controller in order to (a) manage the relationship with Customer; (b) carry out Twilio’s core business operations, such as accounting and filing taxes; (c) detect, prevent, or investigate security incidents, fraud, and other abuse or misuse of the Services; (d) perform identity verification; (e) comply with Twilio’s legal or regulatory obligation to retain Subscriber Records; and (f) as otherwise permitted under Applicable Data Protection Law and in accordance with this Addendum, the Agreement, and the Twilio Privacy Notice.

2.3 Twilio as a Controller of Customer Usage Data. The parties acknowledge that, with regard to the processing of Customer Usage Data, Customer may act either as a controller or processor and Twilio is an independent controller, not a joint controller with Customer. Twilio will process Customer Usage Data as a controller in order to carry out the necessary functions as a communications service provider, such as: (a) Twilio’s accounting, tax, billing, audit, and compliance purposes; (b) to provide, optimize, and maintain the Services, platform and security; (c) to investigate fraud, spam, wrongful or unlawful use of the Services; (d) as required by applicable law or regulation; or (e) as otherwise permitted under Applicable Data Protection Law and in accordance with this Addendum, the Agreement, and the Twilio Privacy Notice.

**3. Purpose Limitation.** Twilio will process personal data in order to provide the Services in accordance with the Agreement. Schedule 1 (Details of Processing) of this Addendum further specifies the nature and purpose of the processing, the processing activities, the duration of the processing, the types of personal data and categories of data subjects.

**4. Compliance.** Customer is responsible for ensuring that (a) it has complied, and will continue to comply, with Applicable Data Protection Law in its use of the Services and its own processing of personal data and (b) it has, and will continue to have, the right to transfer, or provide access to, personal data to Twilio for processing in accordance with the terms of the Agreement and this Addendum.

### III. Twilio as a Processor – Processing Customer Content

**5. Customer Instructions.** Customer appoints Twilio as a processor to process Customer Content on behalf of, and in accordance with, Customer's instructions (a) as set forth in the Agreement, this Addendum, and as otherwise necessary to provide the Services to Customer, and which includes investigating security incidents and preventing spam, fraudulent activity, and violations of the Twilio Acceptable Use Policy, the current version of which is available at <https://www.twilio.com/legal/aup> (<https://www.twilio.com/legal/aup>), and detecting and preventing network exploits or abuse; (b) as necessary to comply with applicable law or regulation, including Applicable Data Protection Law; and (c) as otherwise agreed in writing between Customer and Twilio ("**Permitted Purposes**").

**5.1 Lawfulness of Instructions.** Customer will ensure that its instructions comply with Applicable Data Protection Law. Customer acknowledges that Twilio is neither responsible for determining which laws or regulations are applicable to Customer's business nor whether Twilio's provision of the Services meets or will meet the requirements of such laws or regulations. Customer will ensure that Twilio's processing of Customer Content, when done in accordance with Customer's instructions, will not cause Twilio to violate any applicable law or regulation, including Applicable Data Protection Law. Twilio will inform Customer if it becomes aware, or reasonably believes, that Customer's instructions violate any applicable law or regulation, including Applicable Data Protection Law.

**5.2 Additional Instructions.** Additional instructions outside the scope of the Agreement or this Addendum will be agreed to in writing between Customer and Twilio, including any additional fees that may be payable by Customer to Twilio for carrying out such additional instructions.

### 6. Confidentiality

**6.1 Responding to Third Party Requests.** In the event any Third Party Request is made directly to Twilio in connection with Twilio's processing of Customer Content, Twilio will promptly inform Customer and provide details of the same, to the extent legally permitted. Twilio will not respond to any Third Party Request without Customer's prior consent, except as legally required to do so or to confirm that such Third Party Request relates to Customer.

**6.2 Confidentiality Obligations of Twilio Personnel.** Twilio will ensure that any person it authorizes to process Customer Content has agreed to protect personal data in accordance with Twilio's confidentiality obligations in the Agreement.

## 7. Sub-processors

7.1 Authorization for Onward Sub-processing. Customer provides a general authorization for Twilio to engage onward sub-processors that is conditioned on the following requirements:

(a) Twilio will restrict the onward sub-processor's access to Customer Content only to what is strictly necessary to provide the Services, and Twilio will prohibit the sub-processor from processing the personal data for any other purpose;

(b) Twilio agrees to impose contractual data protection obligations, including appropriate technical and organizational measures to protect personal data, on any sub-processor it appoints that require such sub-processor to protect Customer Content to the standard required by Applicable Data Protection Law, including the requirements set forth in Schedule 4 (Jurisdiction Specific Terms) of this Addendum; and

(c) Twilio will remain liable for any breach of this Addendum that is caused by an act, error, or omission of its sub-processors.

7.2 Current Sub-processors and Notification of Sub-processor Changes. Customer consents to Twilio engaging third party sub-processors to process Customer Content within the Services for the Permitted Purposes provided that Twilio maintains an up-to-date list of its sub-processors at <https://www.twilio.com/legal/sub-processors> (<https://www.twilio.com/legal/sub-processors>), which contains a mechanism for Customer to subscribe to notifications of new sub-processors. If Customer subscribes to such notifications, Twilio will provide details of any change in sub-processors as soon as reasonably practicable. With respect to changes in infrastructure providers, Twilio will endeavor to give written notice sixty (60) days prior to any change, but in any event will give written notice no less than thirty (30) days prior to any such change. With respect to Twilio's other sub-processors, Twilio will endeavor to give written notice thirty (30) days prior to any change, but will give written notice no less than ten (10) days prior to any such change.

7.3 Objection Right for new Sub-processors. Customer may object to Twilio's appointment or replacement of a sub-processor prior to its appointment or replacement, provided such objection is in writing and based on reasonable grounds relating to data protection. In such an event, Customer and Twilio agree to discuss commercially reasonable alternative solutions in good faith. If Customer and Twilio cannot reach a resolution within ninety (90) days from the date of Twilio's receipt of Customer's written objection, Customer may discontinue the use of the affected Services by providing written notice to Twilio. Such discontinuation will be without prejudice to any fees incurred by Customer prior to the discontinuation of the affected Services. If no objection has been raised prior to Twilio replacing or appointing a new sub-processor, Twilio will deem Customer to have authorized the new sub-processor.



**8. Data Subject Rights.** Twilio provides Customer with a number of self-service features via the Services, including the ability to delete, obtain a copy of, or restrict use of Customer Content. Customer may use such self-service features to assist in complying with its obligations under Applicable Data Protection Law with respect to responding to Third Party Requests from data subjects via the Services at no additional cost. Upon Customer's request, Twilio will provide reasonable additional and timely assistance to Customer in complying with Customer's data protection obligations with respect to data subject rights under Applicable Data Protection Law to the extent Customer does not have the ability to resolve a Third Party Request from a data subject through self-service features made available via the Services.

**9. Impact Assessments and Consultations.** Twilio will provide reasonable cooperation to Customer in connection with any data protection impact assessment (at Customer's expense only if such reasonable cooperation will require Twilio to assign significant resources to that effort) or consultations with regulatory authorities that may be required in accordance with Applicable Data Protection Law.

**10. Return or Deletion of Customer Content.** Twilio will, in accordance with Section 3 (Duration of the Processing) of Schedule 1 (Details of Processing) of this Addendum, delete or return to Customer any Customer Content stored within the Services.

10.1 Extension of Addendum. Upon termination of the Agreement, Twilio may retain Customer Content in storage for the time periods set forth in Schedule 1 (Details of Processing) of this Addendum, provided that Twilio will ensure that Customer Content (a) is processed only as necessary for the Permitted Purposes and (b) remains protected in accordance with the terms of the Agreement, this Addendum, and Applicable Data Protection Law.

10.2 Retention Required by Law. Notwithstanding anything to the contrary in this Section 10, Twilio may retain Customer Content, or any portion of it, if required by applicable law or regulation, including Applicable Data Protection Law, provided such Customer Content remains protected in accordance with the terms of the Agreement, this Addendum, and Applicable Data Protection Law.

## **IV. Security and Audits**

### **11. Security**

11.1 Security Measures. Twilio has implemented and will maintain the technical and organizational security measures as set forth in the Agreement. Additional information about Twilio's technical and organizational security measures to protect Customer Data is set forth in Schedule 2 (Technical and Organizational Security Measures) of this Addendum.

11.2 Determination of Security Requirements. Customer acknowledges the Services include certain features and functionalities that Customer may elect to use which impact the security of Customer Data processed by Customer's use of the Services, such as, but not limited to, encryption of voice recordings, availability of multi-factor authentication on Customer's account, or optional Transport Layer Security (TLS) encryption. Customer is responsible for reviewing the information Twilio makes available regarding its data security, including its audit reports, and making an independent determination as to whether the Services meet the Customer's requirements and legal obligations, including its obligations under Applicable Data Protection Law. Customer is further responsible for properly configuring the Services and using features and functionalities made available by Twilio to maintain appropriate security in light of the nature of Customer Data processed as a result of Customer's use of the Services.

11.3 Security Incident Notification. Twilio will provide notification of a Security Incident in the following manner:

(a) Twilio will, to the extent permitted by applicable law or regulation, notify Customer without undue delay, but in no event later than seventy-two (72) hours after Twilio's discovery of a Security Incident impacting Customer Data of which Twilio is a processor;

(b) Twilio will, to the extent permitted and required by applicable law or regulation, notify Customer without undue delay of any Security Incident involving Customer Data of which Twilio is a controller; and

(c) Twilio will notify Customer of any Security Incident via email to the email address(es) designated by Customer in Customer's account.

Twilio will make reasonable efforts to identify a Security Incident, and to the extent a Security Incident is caused by Twilio's violation of this Addendum, remediate the cause of such Security Incident. Twilio will provide reasonable assistance to Customer in the event that Customer is required under Applicable Data Protection Law to notify a regulatory authority or any data subjects impacted by a Security Incident.

**12. Audits.** Customer and Twilio acknowledge that Customer must be able to assess Twilio's compliance with its obligations under Applicable Data Protection Law and this Addendum, insofar as Twilio is acting as a processor on behalf of Customer.

12.1 Twilio's Audit Program. Twilio uses external auditors to verify the adequacy of its security measures with respect to its processing of Customer Content. Such audits are performed at least once annually at Twilio's expense by independent third-party security professionals at Twilio's selection and result in the generation of a confidential audit report ("*Audit Report*").

12.2 Customer Audit. Upon Customer's written request at reasonable intervals, and subject to reasonable confidentiality controls, Twilio will make available to Customer a copy of Twilio's most recent Audit Report. Customer agrees that any audit rights granted by Applicable Data Protection Law will be satisfied by these Audit Reports. To the extent that Twilio's provision of an Audit Report does not provide sufficient information or Customer is required to respond to a regulatory authority audit, Customer agrees to a mutually agreed-upon audit plan with Twilio that: (a) ensures the use of an independent third party; (b) provides written notice to Twilio in a timely fashion; (c) requests access only during business hours; (d) accepts billing to Customer at Twilio's then-current rates; (e) occurs no more than once annually; (f) restricts its findings to only data relevant to Customer; and (g) obligates Customer, to the extent permitted by law or regulation, to keep confidential any information gathered that, by its nature, should be confidential.

## V. International Provisions

**13. Jurisdiction Specific Terms.** To the extent Twilio processes personal data originating from and protected by Applicable Data Protection Law in one of the jurisdictions listed in Schedule 4 (Jurisdiction Specific Terms) of this Addendum, the terms specified in Schedule 4 with respect to the applicable jurisdiction(s) apply in addition to the terms of this Addendum.

**14. Cross Border Data Transfer Mechanisms.** To the extent Customer's use of the Services requires an onward transfer mechanism to lawfully transfer personal data from a jurisdiction (i.e., the European Economic Area, the United Kingdom, Switzerland, Guernsey, Jersey, or any other jurisdiction listed in Schedule 4 (Jurisdiction Specific Terms) of this Addendum) to Twilio located outside of that jurisdiction ("*Transfer Mechanism*"), the terms set forth in Schedule 3 (Cross Border Transfer Mechanisms) of this Addendum will apply.

## VI. Miscellaneous

**15. Cooperation and Data Subject Rights.** In the event that either party receives (a) any request from a data subject to exercise any of its rights under Applicable Data Protection Law (including its rights of access, correction, objection, erasure, and data portability, as applicable) or (b) any Third Party Request relating to the processing of Customer Account Data or Customer Usage Data conducted by the other party, such party will promptly inform such other party in writing. Customer and Twilio agree to cooperate, in good faith, as necessary to respond to any Third Party Request and fulfill their respective obligations under Applicable Data Protection Law.

**16. Conflict.** In the event of any conflict or inconsistency among the following documents, the order of precedence will be: (1) the applicable terms set forth in Schedule 4 (Jurisdiction Specific Terms) of this Addendum; (2) the terms of this Addendum outside of Schedule 4 (Jurisdiction Specific Terms); (3) the Agreement; and (4) the Twilio Privacy Notice. Any claims brought in connection with this Addendum will be subject to the terms and conditions, including, without limitation, the exclusions and limitations set forth in the Agreement.

**17. Updates.** Twilio may update the terms of this Addendum from time to time; provided, however, Twilio will provide at least thirty (30) days prior written notice to Customer when an update is required as a result of (a) changes in Applicable Data Protection Law; (b) a merger, acquisition, or other similar transaction; or (c) the release of new products or services or material changes to any of the existing Services. The then-current terms of this Addendum are available at <https://www.twilio.com/legal/data-protection-addendum> (<https://www.twilio.com/legal/data-protection-addendum>).

---

## Schedule 1

### Details of Processing

**1. Nature and Purpose of the Processing.** Twilio will process personal data as necessary to provide the Services under the Agreement. Twilio does not sell Customer's personal data or Customer end users' personal data and does not share such end users' information with third parties for compensation or for those third parties' own business interests.

1.1 Customer Content. Twilio will process Customer Content as a processor in accordance with Customer's instructions as set forth in Section 5 (Customer Instructions) of this Addendum.

1.2 Customer Account Data. Twilio will process Customer Account Data as a controller for the purposes set forth in Section 2.2 (Twilio as a Controller of Customer Account Data) of this Addendum.

1.3 Customer Usage Data. Twilio will process Customer Usage Data as a controller for the purposes set forth in Section 2.3 (Twilio as a Controller of Customer Usage Data) of this Addendum.

### 2. Processing Activities

2.1 Customer Content. Personal data contained in Customer Content will be subject to the following basic processing activities:

(a) the provision of programmable communication products and services, primarily offered in the form of application programming interfaces, to Customer, including transmittal to or from Customer's software applications or; services and designated third parties as directed by Customer, from or to the publicly-switched telephone network or by way of other communications networks. Storage of personal data on Twilio's network;

(b) the provision of products and services which allow the transmission and delivery of email communications on behalf of Customer to its recipients. Twilio will also provide Customer with analytic reports regarding the email communications it sends on Customer's behalf. Storage of personal data on Twilio's network; and

(c) the provision of products and services which allows Customer to integrate, manage and control its data relating to end users. Storage of personal data on Twilio's network.

2.2 Customer Account Data. Personal data contained in Customer Account Data will be subject to the processing activities of providing the Services.

2.3 Customer Usage Data. Personal data contained in Customer Usage Data will be subject to the processing activities of providing the Services.

**3. Duration of the Processing.** The period for which personal data will be retained and the criteria used to determine that period is as follows:

#### 3.1 Customer Content.

(a) Services. Prior to the termination of the Agreement, (x) Twilio will process stored Customer Content for the Permitted Purposes until Customer elects to delete such Customer Content via the Services and (y) Customer agrees that it is solely responsible for deleting Customer Content via the Services. Except as set forth in Section 3.1(b) (SendGrid Services) of this Schedule 1, upon termination of the Agreement, Twilio will (i) provide Customer thirty (30) days after the termination effective date to obtain a copy of any stored Customer Content via the Services; (ii) automatically delete any stored Customer Content thirty (30) days after the termination effective date; and (iii) automatically delete any stored Customer Content on Twilio's back-up systems sixty (60) days after the termination effective date. Any Customer Content archived on Twilio's back-up systems will be securely isolated and protected from any further processing, except as otherwise required by applicable law or regulation.

(b) SendGrid Services. Upon termination of the Agreement, Twilio will (i) at Customer's election, delete or return to Customer the Customer Content (including copies) stored within any services and application programming interfaces branded as "SendGrid" or "Twilio SendGrid" (collectively, "*SendGrid Services*") and (ii) automatically delete any stored Customer Content in the SendGrid Services on Twilio's back-up systems one (1) year after the termination effective date.

3.2 Customer Account Data. Twilio will process Customer Account Data as long as required (a) to provide the Services to Customer; (b) for Twilio's legitimate business needs; or (c) by applicable law or regulation. Customer Account Data will be stored in accordance with the Twilio Privacy Notice.

3.3 Customer Usage Data. Upon termination of the Agreement, Twilio may retain, use, and disclose Customer Usage Data for the purposes set forth in Section 1.3 (Customer Usage Data) of this Schedule 1, subject to the confidentiality obligations set forth in the Agreement. Twilio will anonymize or delete Customer Usage Data when Twilio no longer requires it for the purposes set forth in Section 1.3 (Customer Usage Data) of this Schedule 1.

#### 4. Categories of Data Subjects

4.1 Customer Content. Customer's end users.

4.2 Customer Account Data. Customer's employees and individuals authorized by Customer to access Customer's Twilio account or make use of the Multi-Factor Authentication Services or telephone number assignments received from Twilio.

4.3 Customer Usage Data. Customer's end users.

**5. Categories of Personal Data.** Twilio processes personal data contained in Customer Account Data, Customer Content, and Customer Usage Data.

#### 6. Sensitive Data or Special Categories of Data

6.1 Customer Content. Sensitive Data may, from time to time, be processed via the Services where Customer or its end users choose to include Sensitive Data within the communications that are transmitted using the Services. Customer is responsible for ensuring that suitable safeguards are in place prior to transmitting or processing, or prior to permitting Customer's end users to transmit or process, any Sensitive Data via the Services.

6.2 Customer Account Data and Customer Usage Data.

(a) Sensitive Data may be found in Customer Account Data in the form of Subscriber Records containing passport or similar identifier data necessarily processed in order to receive telephone number assignments.

(b) Customer Usage Data does not contain Sensitive Data.

---

## Schedule 2

### Technical and Organizational Security Measures

The full text of Twilio's technical and organizational security measures to protect Customer Data is available at <https://www.twilio.com/legal/security-overview> (<https://www.twilio.com/legal/security-overview>) ("*Security Overview*").

Where applicable, this Schedule 2 will serve as Annex II to the EU Standard Contractual Clauses. The following table provides more information regarding the technical and organizational security measures set forth below.

| Technical and Organizational Security Measure                                                                                                                 | Evidence of Technical and Organizational Security Measure                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Measures of pseudonymisation and encryption of personal data                                                                                                  | See Section 13 (Encryption) of the <a href="https://www.twilio.com/legal/security-overview">Security Overview</a> ( <a href="https://www.twilio.com/legal/security-overview">https://www.twilio.com/legal/security-overview</a> )                                                                                                                   |
| Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services                                      | See Section 18 ( Resilience and Service Continuity) and Section 19 (Customer Data Backups) of the <a href="https://www.twilio.com/legal/security-overview">Security Overview</a> ( <a href="https://www.twilio.com/legal/security-overview">https://www.twilio.com/legal/security-overview</a> )                                                    |
| Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident | See Section 18 ( Resilience and Service Continuity) and Section 19 (Customer Data Backups) of the <a href="https://www.twilio.com/legal/security-overview">Security Overview</a> ( <a href="https://www.twilio.com/legal/security-overview">https://www.twilio.com/legal/security-overview</a> )                                                    |
| Processes for regularly testing, assessing and evaluating the effectiveness of technical and                                                                  | See Section 3 (Security Organization and Program), Section 7 (Security Certifications and Attestations), and Section 15 (Penetration Testing) of the <a href="https://www.twilio.com/legal/security-overview">Security Overview</a> ( <a href="https://www.twilio.com/legal/security-overview">https://www.twilio.com/legal/security-overview</a> ) |



| Technical and Organizational Security Measure                                             | Evidence of Technical and Organizational Security Measure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| organizational measures in order to ensure the security of the processing                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Measures for user identification and authorisation                                        | See Section 11 (Access Controls) of the <a href="https://www.twilio.com/legal/security-overview">Security Overview (https://www.twilio.com/legal/security-overview)</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Measures for the protection of data during transmission                                   | See Section 13 (Encryption) and Section 19 (Customer Data Backups) of the <a href="https://www.twilio.com/legal/security-overview">Security Overview (https://www.twilio.com/legal/security-overview)</a>                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Measures for the protection of data during storage                                        | See Section 8 (Hosting Architecture and Data Segregation) and Section 13 (Encryption) of the <a href="https://www.twilio.com/legal/security-overview">Security Overview (https://www.twilio.com/legal/security-overview)</a>                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Measures for ensuring physical security of locations at which personal data are processed | See Section 9 (Physical Security) of the <a href="https://www.twilio.com/legal/security-overview">Security Overview (https://www.twilio.com/legal/security-overview)</a>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Measures for ensuring events logging                                                      | See: <a href="https://www.twilio.com/docs/runtime/serverless-api/api/logs">https://www.twilio.com/docs/runtime/serverless-api/api/logs</a><br>( <a href="https://www.twilio.com/docs/runtime/serverless-api/api/logs">https://www.twilio.com/docs/runtime/serverless-api/api/logs</a> )<br><br>and:<br><br><a href="https://docs.sendgrid.com/ui/analytics-and-reporting/email-activity-feed">https://docs.sendgrid.com/ui/analytics-and-reporting/email-activity-feed</a><br>( <a href="https://docs.sendgrid.com/ui/analytics-and-reporting/email-activity-feed">https://docs.sendgrid.com/ui/analytics-and-reporting/email-activity-feed</a> ) |

Technical and  
Organizational Security  
Measure

Evidence of Technical and Organizational Security Measure

Measures for ensuring  
system configuration,  
including default  
configuration

See: <https://www.twilio.com/docs/runtime/serverless-api/api/logs>  
(<https://www.twilio.com/docs/runtime/serverless-api/api/logs>)

and:

<https://docs.sendgrid.com/ui/analytics-and-reporting/email-activity-feed>  
(<https://docs.sendgrid.com/ui/analytics-and-reporting/email-activity-feed>)

Measures for internal IT and  
IT security governance and  
management

See Section 3 (Security Organization and Program) of the [Security Overview](https://www.twilio.com/legal/security-overview)  
(<https://www.twilio.com/legal/security-overview>)

Measures for  
certification/assurance of  
processes and products

See Section 3 (Security Organization and Program) and Section 7 (Security  
Certifications and Attestations) of the [Security Overview](https://www.twilio.com/legal/security-overview)  
(<https://www.twilio.com/legal/security-overview>)

Measures for ensuring data  
minimisation

As an organization, Twilio has adopted [Binding Corporate Rules](https://www.twilio.com/legal/bcr)  
(<https://www.twilio.com/legal/bcr>) (BCRs) as the “code of conduct” for  
Twilio’s processing of personal data worldwide. BCRs are based on the data  
protection principles of the GDPR. Twilio’s BCRs were approved in May 2018 by  
European Union data protection authorities, and Twilio audits against and re-  
certifies its commitments established in its BCRs on an annual basis. More  
information about how Twilio processes personal data is set forth in the Privacy  
Policy available at <https://www.twilio.com/legal/privacy>  
(<https://www.twilio.com/legal/privacy#twilio-privacy-statement>), and further  
detailed in Twilio BCRs available at <https://www.twilio.com/legal/bcr>  
(<https://www.twilio.com/legal/bcr>).

Technical and  
Organizational Security  
Measure

Evidence of Technical and Organizational Security Measure

Measures for ensuring data  
quality

As an organization, Twilio has adopted [Binding Corporate Rules](https://www.twilio.com/legal/bcr) (<https://www.twilio.com/legal/bcr>) (BCRs) as the “code of conduct” for Twilio’s processing of personal data worldwide. BCRs are based on the data protection principles of the GDPR. Twilio’s BCRs were approved in May 2018 by European Union data protection authorities, and Twilio audits against and re-certifies its commitments established in its BCRs on an annual basis. More information about how Twilio processes personal data is set forth in the Privacy Policy available at <https://www.twilio.com/legal/privacy> (<https://www.twilio.com/legal/privacy#twilio-privacy-statement>), and further detailed in Twilio’s BCRs available at <https://www.twilio.com/legal/bcr> (<https://www.twilio.com/legal/bcr>).

Measures for ensuring  
limited data retention

As an organization, Twilio has adopted [Binding Corporate Rules](https://www.twilio.com/legal/bcr) (<https://www.twilio.com/legal/bcr>) (BCRs) as the “code of conduct” for Twilio’s processing of personal data worldwide. BCRs are based on the data protection principles of the GDPR. Twilio’s BCRs were approved in May 2018 by European Union data protection authorities, and Twilio audits against and re-certifies its commitments established in its BCRs on an annual basis. More information about how Twilio processes personal data is set forth in the Privacy Policy available at <https://www.twilio.com/legal/privacy> (<https://www.twilio.com/legal/privacy#twilio-privacy-statement>), and further detailed in Twilio’s BCRs available at <https://www.twilio.com/legal/bcr> (<https://www.twilio.com/legal/bcr>).

Measures for ensuring  
accountability

As an organization, Twilio has adopted [Binding Corporate Rules](https://www.twilio.com/legal/bcr) (<https://www.twilio.com/legal/bcr>) (BCRs) as the “code of conduct” for Twilio’s processing of personal data worldwide. BCRs are based on the data protection principles of the GDPR. Twilio’s BCRs were approved in May 2018 by European Union data protection authorities, and Twilio audits against and re-certifies its commitments established in its BCRs on an annual basis. More information about how Twilio processes personal data is set forth in the Privacy Policy available at <https://www.twilio.com/legal/privacy>

Technical and  
Organizational Security  
Measure

Evidence of Technical and Organizational Security Measure

---

<https://www.twilio.com/legal/privacy#twilio-privacy-statement>), and further detailed in Twilio's BCRs available at <https://www.twilio.com/legal/bcr> (<https://www.twilio.com/legal/bcr>).

---

Customer is able to export or delete Customer Content using the self-service features of the Services as set forth in the applicable documentation for the Services available at <https://www.twilio.com/docs> (<https://www.twilio.com/docs>).

For an example of data portability self-service features, see:  
<https://support.twilio.com/hc/en-us/articles/223183588-Exporting-SMS-and-Call-Logs> (<https://support.twilio.com/hc/en-us/articles/223183588-Exporting-SMS-and-Call-Logs>)

Measures for allowing data  
portability and ensuring  
erasure

For an example of data portability self-service features, see:

<https://docs.sendgrid.com/ui/managing-contacts/create-and-manage-contacts#export-contacts> (<https://docs.sendgrid.com/ui/managing-contacts/create-and-manage-contacts#export-contacts>)

For an example of data erasure self-service features, see:  
<https://support.twilio.com/hc/en-us/articles/223181008-Twilio-SMS-message-and-traffic-storage> (<https://support.twilio.com/hc/en-us/articles/223181008-Twilio-SMS-message-and-traffic-storage>)

For an example of data erasure self-service features, see:  
<https://docs.sendgrid.com/api-reference/contacts/delete-contacts> (<https://docs.sendgrid.com/api-reference/contacts/delete-contacts>)

---

## Technical and

### Organizational Security Measure

### Evidence of Technical and Organizational Security Measure

Technical and organizational measures to be taken by the [sub]-processor to provide assistance to the controller and, for transfers from a processor to a [sub]-processor, to the Customer.

When Twilio engages a sub-processor under Section 7.1 (Authorization for Onward Sub-processing) of this Addendum, Twilio and the sub-processor enter into an agreement with data protection obligations substantially similar to those contained in this Addendum. Each sub-processor agreement must ensure that Twilio is able to meet its obligations to Customer. In addition to implementing technical and organizational measures to protect personal data, sub-processors must (a) notify Twilio in the event of a Security Incident so Twilio may notify Customer; (b) delete personal data when instructed by Twilio in accordance with Customer's instructions to Twilio; (c) not engage additional sub-processors without Twilio's authorization; d) not change the location where personal data is processed; or (e) process personal data in a manner which conflicts with Customer's instructions to Twilio.

## Schedule 3

### Cross Border Data Transfer Mechanisms

#### 1. Definitions

- "*BCR Services*" means all Services, except the SendGrid Services.
- "*EEA*" means the European Economic Area
- "*EU Standard Contractual Clauses*" means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.
- "*Twilio BCRs*" means Twilio's Binding Corporate Rules as set forth at <https://www.twilio.com/legal/binding-corporate-rules> (<https://www.twilio.com/legal/binding-corporate-rules>).
- "*Twilio CBPR Certification*" means Twilio's certification under Asia-Pacific Economic Cooperation ("*CBPRs*") and Privacy Recognition for Processors Systems, as recorded in the directory available at <http://www.cbprs.org/compliance-directory/cbpr-system> (<http://www.cbprs.org/compliance-directory/cbpr-system>).
- "*UK International Data Transfer Agreement*" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

## 2. Cross Border Data Transfer Mechanisms

2.1 Order of Precedence. In the event the Services are covered by more than one Transfer Mechanism, the transfer of personal data will be subject to a single Transfer Mechanism in accordance with the following order of precedence: (a) Twilio's binding corporate rules as set forth in Section 2.2 (Twilio BCRs) of this Schedule 3; (b) the EU Standard Contractual Clauses as set forth in Section 2.4 (EU Standard Contractual Clauses) of this Schedule 3; (c) the UK International Data Transfer Agreement as set forth in Section 2.5 (UK International Data Transfer Agreement) of this Schedule 3; and, if neither (a) nor (b) nor (c) is applicable, then (d) other applicable data Transfer Mechanisms permitted under Applicable Data Protection Law.

2.2 Twilio BCRs. Twilio will process personal data within the BCR Services in accordance with the Twilio BCRs. Customer and Twilio agree that, with respect to the BCR Services, the Twilio BCRs will be the lawful Transfer Mechanism of Customer Account Data, Customer Content, and Customer Usage Data from the EEA, Switzerland, or the United Kingdom to (a) Twilio in the United States of America or (b) any other non-EEA Twilio entity. For avoidance of doubt, the Twilio BCRs do not serve as a Transfer Mechanism for the SendGrid Services.

2.3 Twilio CBPR Certification. Twilio's privacy program has been certified under the APEC CBPRs, a government-backed data privacy certification to demonstrate compliance with internationally-recognized data privacy protections. Twilio will process personal data in accordance with the Twilio CBPR Certification to the extent applicable.

2.4 EU Standard Contractual Clauses. The EU Standard Contractual Clauses will apply to personal data that is transferred via the Services from the EEA, Switzerland, Guernsey, or Jersey, either directly or via onward transfer, to any country or recipient outside the EEA, Switzerland, Guernsey, or Jersey that is not (a) recognized by the relevant competent authority as providing an adequate level of protection for personal data and (b) covered by the Twilio BCRs. For data transfers that are subject to the EU Standard Contractual Clauses, the EU Standard Contractual Clauses will be deemed entered into, and incorporated into this Addendum by this reference, and completed as follows:

(a) Module One (Controller to Controller) of the EU Standard Contractual Clauses will apply where (i) Twilio is processing Customer Account Data and (ii) Customer is a controller of Customer Usage Data and Twilio is processing Customer Usage Data;

(b) Module Two (Controller to Processor) of the EU Standard Contractual Clauses will apply where Customer is a controller of Customer Content and Twilio is processing Customer Content;

(c) Module Three (Processor to Processor) of the EU Standard Contractual Clauses will apply where Customer is a processor of Customer Content and Twilio is processing Customer Content;

(d) Module Four (Processor to Controller) of the EU Standard Contractual Clauses will apply where Customer is a processor of Customer Usage Data and Twilio processes Customer Usage Data; and

(e) For each Module, where applicable:

(i) in Clause 7 of the EU Standard Contractual Clauses, the optional docking clause will not apply;

(ii) in Clause 9 of the EU Standard Contractual Clauses, Option 2 will apply and the time period for prior written notice of sub-processor changes will be as set forth in Section 7.2 (Current Sub-processors and Notification of Sub-processor Changes) of this Addendum;

(iii) in Clause 11 of the EU Standard Contractual Clauses, the optional language will not apply;

(iv) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by Irish law;

(v) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Ireland;

(vi) in Annex I, Part A of the EU Standard Contractual Clauses:

Data Exporter: Customer

Contact details: The email address(es) designated by Customer in Customer's account via its notification preferences.

Data Exporter Role: The Data Exporter's role is set forth in Section 2 (Relationship) of this Addendum.

Signature and Date: By entering into the Agreement, Data Exporter is deemed to have signed these EU Standard Contractual Clauses incorporated herein, including their Annexes, as of the effective date of the Agreement.

Data Importer: Twilio Inc.

Contact details: Twilio Privacy Team - [privacy@twilio.com](mailto:privacy@twilio.com)

Data Importer Role: The Data Importer's role is set forth in Section 2 (Relationship) of this Addendum.

Signature and Date: By entering into the Agreement, Data Importer is deemed to have signed these EU Standard Contractual Clauses, incorporated herein, including their Annexes, as of the effective date of the Agreement;



(vii) in Annex I, Part B of the EU Standard Contractual Clauses:

The categories of data subjects are set forth in Section 4 of Schedule 1 (Details of Processing) of this Addendum.

The Sensitive Data transferred is set forth in Section 6 of Schedule 1 (Details of Processing) of this Addendum.

The frequency of the transfer is a continuous basis for the duration of the Agreement.

The nature of the processing is set forth in Section 1 of Schedule 1 (Details of Processing) of this Addendum.

The purpose of the processing is set forth in Section 1 of Schedule 1 (Details of Processing) of this Addendum.

The period for which the personal data will be retained is set forth in Section 3 of Schedule 1 (Details of Processing) of this Addendum.

For transfers to sub-processors, the subject matter, nature, and duration of the processing is set forth at <https://www.twilio.com/legal/sub-processors> (<https://www.twilio.com/legal/sub-processors>);

(viii) in Annex I, Part C of the EU Standard Contractual Clauses: The Irish Data Protection Commission will be the competent supervisory authority; and

(ix) Schedule 2 (Technical and Organizational Security Measures) of this Addendum serves as Annex II of the EU Standard Contractual Clauses.

2.5 UK International Data Transfer Agreement. Customer and Twilio agree that the UK International Data Transfer Agreement will apply to personal data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not (a) recognized by the competent United Kingdom regulatory authority or governmental body for the United Kingdom as providing an adequate level of protection for personal data and (b) covered by the Twilio BCRs. For data transfers from the United Kingdom that are subject to the UK International Data Transfer Agreement, the UK International Data Transfer Agreement will be deemed entered into, and incorporated into this Addendum by this reference, and completed as follows:

(a) In Table 1 of the UK International Data Transfer Agreement, Customer's and Twilio's details and key contact information are set forth in Section 2.3 (e)(vi) of this Schedule 3;

(b) In Table 2 of the UK International Data Transfer Agreement, information about the version of the Approved EU SCCs, modules, and selected clauses, which the UK International Data Transfer Agreement is appended to, are set forth in Section 2.4 (EU Standard Contractual Clauses) of this Schedule 3;

(c) In Table 3 of the UK International Data Transfer Agreement:

(i) The list of Parties is set forth in Section 2.4(e)(vi) of this Schedule 3.

(ii) The description of the transfer is set forth in Section 1 (Nature and Purpose of the Processing) of Schedule 1 (Details of the Processing).

(iii) Annex II is located in Schedule 2 (Technical and Organizational Security Measures) of this Addendum.

(iv) The list of sub-processors is available at <https://www.twilio.com/legal/sub-processors> (<https://www.twilio.com/legal/sub-processors>); and

(d) In Table 4 of the UK International Data Transfer Agreement, both the Importer and the exporter may end the UK International Data Transfer Agreement in accordance with the terms of the UK International Data Transfer Agreement.

2.6 Conflict. To the extent there is any conflict or inconsistency between the EU Standard Contractual Clauses or UK International Data Transfer Agreement and any other terms in this Addendum, including Schedule 4 (Jurisdiction Specific Terms), the Agreement, or the Twilio Privacy Notice, the provisions of the EU Standard Contractual Clauses or UK International Data Transfer Agreement, as applicable, will prevail.

---

## Schedule 4

### Jurisdiction Specific Terms

#### 1. Australia:

1.1 The definition of “Applicable Data Protection Law” includes the Australian Privacy Principles and the Australian Privacy Act (1988).

1.2 The definition of “personal data” includes “Personal Information” as defined under Applicable Data Protection Law.

1.3 The definition of “Sensitive Data” includes “Sensitive Information” as defined under Applicable Data Protection Law.

## **2. Brazil:**

2.1 The definition of “Applicable Data Protection Law” includes the Lei Geral de Proteção de Dados (General Personal Data Protection Act).

2.2 The definition of “Security Incident” includes a security incident that may result in any relevant risk or damage to data subjects.

2.3 The definition of “processor” includes “operator” as defined under Applicable Data Protection Law.

## **3. Canada:**

3.1 The definition of “Applicable Data Protection Law” includes the Federal Personal Information Protection and Electronic Documents Act.

3.2 Twilio’s sub-processors, as set forth in Section 7 (Sub-processors) of this Addendum, are third parties under Applicable Data Protection Law, with whom Twilio has entered into a written contract that includes terms substantially similar to this Addendum. Twilio has conducted appropriate due diligence on its sub-processors.

3.3 Twilio will implement technical and organizational measures as set forth in Section 11 (Security) of this Addendum.

## **4. European Economic Area (EEA):**

4.1 The definition of “Applicable Data Protection Law” includes the General Data Protection Regulation (EU 2016/679) (“*GDPR*”).

4.2 When Twilio engages a sub-processor under Section 7.1 (Authorization for Onward Sub-processing) of this Addendum, it will:

(a) require any appointed sub-processor to protect the Customer Content to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and

(b) require any appointed sub-processor to (i) agree in writing to only process personal data in a country that the European Union has declared to have an “adequate” level of protection or (ii) only process personal data on terms equivalent to the EU Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

4.3 Notwithstanding anything to the contrary in this Addendum or in the Agreement (including, without limitation, either party’s indemnification obligations), neither party will be responsible for any GDPR fines issued or levied under Article 83 of the GDPR against the other party by a regulatory authority or governmental body in connection with such other party’s violation of the GDPR.

4.4 Customer acknowledges that Twilio, as a controller, may be required under Applicable Data Protection Law to notify a regulatory authority of Security Incidents involving Customer Usage Data. If a regulatory authority requires Twilio to notify impacted data subjects with whom Twilio does not have a direct relationship (e.g., Customer’s end users), Twilio will notify Customer of this requirement. Customer will provide reasonable assistance to Twilio to notify the impacted data subjects.

## **5. Israel:**

5.1 The definition of “Applicable Data Protection Law” includes the Protection of Privacy Law.

5.2 The definition of “controller” includes “Database Owner” as defined under Applicable Data Protection Law.

5.3 The definition of “processor” includes “Holder” as defined under Applicable Data Protection Law.

5.4 Twilio will require that any personnel authorized to process Customer Content comply with the principle of data secrecy and have been duly instructed about Applicable Data Protection Law. Such personnel sign confidentiality agreements with Twilio in accordance with Section 6 (Confidentiality) of this Addendum.

5.5 Twilio must take sufficient steps to ensure the privacy of data subjects by implementing and maintaining the security measures as specified in Section 11 (Security) of this Addendum and complying with the terms of the Agreement.

5.6 Twilio must ensure that the personal data will not be transferred to a sub-processor unless such sub-processor has executed an agreement with Twilio pursuant to Section 7.1 (Authorization for Onward Sub-processing) of this Addendum.

## **6. Japan:**

6.1 The definition of “Applicable Data Protection Law” includes the Act on the Protection of Personal Information (“*APPI*”).

6.2 The definition of “personal data” includes information about a specific individual applicable under Section 2(1) of the APPI, which Customer entrusts to Twilio during Twilio’s provision of the Services to Customer.

6.3 Twilio agrees it has and will maintain a privacy program conforming to the standards prescribed by rules of the Personal Information Protection Commission concerning the handling of personal data pursuant to the provisions of Chapter 4 of the APPI. Accordingly:

(a) Twilio will (i) process personal data as necessary to provide the Services to Customer in accordance with the Agreement and as set forth in Schedule 1 (Details of the Processing) of this Addendum (“*Purpose of Use*”) and (ii) not process personal data for any purpose other than the Purpose of Use without Customer’s consent;

(b) Twilio will implement and maintain measures appropriate and necessary to prevent unauthorized disclosure and loss of personal data and for the secure management of personal data in accordance with the APPI as set forth in Section 11 (Security) of this Addendum;

(c) Twilio will notify Customer for (i) a failure to comply with Section 6.3(a) of this Schedule 4 or (ii) Twilio’s discovery of a Security Incident impacting Customer Data, in either case, in accordance with Section 11.3 (Security Incident Notification). Twilio will provide reasonable assistance to Customer in the event that Customer is required to notify a regulatory authority or any data subjects impacted by a Security Incident;

(d) Twilio will ensure that any of its employees who have access to personal data (i) have executed employee agreements requiring them to keep such personal data confidential and (ii) who violate confidentiality will be subject to disciplinary action and possible termination; (iii) carry out appropriate employee supervision and training for the secure management of personal data; and (iv) limit the number of authorized personnel, including Twilio’s employees, who have access to personal data and control such access such that it is only permitted for the time period necessary for the Purpose of Use;

(e) Twilio will not disclose personal data to any third party, except as Customer has authorized Twilio to do so in the Agreement. When engaging sub-processors, Twilio will comply with the obligations in Section 7 (Sub-processors) of this Addendum to ensure that procedures are in place to maintain the confidentiality and security of personal data;

(f) Twilio will keep records of the handling of personal data entrusted to it by, and performed for, Customer;

(g) Twilio will promptly notify Customer of any Third Party Request and not respond to such Third Party Request without Customer's prior consent, except as legally required to do so or to confirm that such Third Party Request relates to Customer. To the extent Customer does not have the ability to resolve a Third Party Request from a data subject through the self-service features made available via the Services, then, upon Customer's request, Twilio will provide reasonable cooperation and support to assist Customer in resolving such Third Party Request from a data subject in accordance with Section 8 (Data Subject Rights) of this Addendum;

(h) Unless prohibited by applicable law or regulation, Twilio will promptly notify Customer of any Third Party Request that requires Twilio to disclose personal data on order or disposition of any governmental authority or court of law. Twilio will (i) comply with its law enforcement guidelines available at <https://www.twilio.com/legal/law-enforcement-guidelines> and (ii) limit any personal data provided to the minimum extent required and strictly for the required purpose;

(i) Customer may assess Twilio's compliance with its obligations under Applicable Data Protection Law and as set forth in Section 12 (Audits) of this Addendum. In addition, Twilio will respond to any Customer inquiries or questionnaires relating to Twilio's processing of personal data under the Agreement in good faith and within a reasonable period of time. Customer may direct APPI-related inquiries to [privacy@twilio.com](mailto:privacy@twilio.com). Twilio will identify its Chief Privacy Officer upon written request;

(j) Twilio will provide reasonable cooperation to Customer upon written request, where Customer is reporting to the Personal Information Protection Commission or other regulatory authorities; and

(k) Twilio's primary processing facilities are located in the United States of America, and, depending on Customer's use of the Services, from the locations set forth at <https://www.twilio.com/legal/sub-processors> (collectively, "*Processing Locations*"). Twilio will notify customer of any Processing Location change and provide Customer the opportunity to object in accordance with, respectively, Section 7.2 (Current Sub-processors and Notification of Sub-process or Changes) and Section 7.3 (Objection Right for new Sub-processors) of this Addendum. Where Twilio processes personal data in a country other than Japan, Twilio will ensure it complies with its privacy program as described in this Addendum. Twilio will promptly notify Customer of any changes in applicable law and regulation that may materially affect Twilio's obligations with respect to the processing of personal data, and in such case, Customer may, at its discretion, suspend the transfer of personal data.

#### 6.4 The following data subject consent terms apply:

(a) Customer entrusts Twilio with personal data for the Purpose of Use. Customer agrees that Twilio is not a "third party" as the term is used in the APPI provisions that restrict the provision of personal data to third parties. As such, the requirement to obtain data subject consent in advance for domestic transfers within Japan do not apply;

(b) Customer agrees that Twilio's APEC CBPRs and privacy program set forth in Section 6.3 of this Schedule 4 meets the equivalent standards prescribed by the Personal Information Protection Commission and the APPI. As such, the APPI restrictions on the provision of personal data to third parties in foreign countries outside of Japan, which require data subject consent in advance of such international transfers do not apply. Customer may take the necessary actions set forth in Section 6.3(h) of this Schedule 4 to ensure continuous implementation of Twilio's APEC CBPRs and privacy program and respond to Third Party Requests from data subjects; and

(c) Customer acknowledges that data subject consent may be required under Article 4 of the Telecommunications Business Act in the event Customer instructs Twilio's support personnel to access the content of communications. Customer will comply with any consent requirements specific to its use of the Services and instructions as required by Section 4 (Compliance) of this Addendum.

## **7. Mexico:**

7.1 The definition of "Applicable Data Protection Law" includes the Federal Law for the Protection of Personal Data Held by Private Parties and its Regulations.

7.2 When acting as a processor, Twilio will:

(a) treat personal data in accordance with Customer's instructions set forth in Section 5 (Customer Instructions) of this Addendum;

(b) process personal data only to the extent necessary to provide the Services;

(c) implement security measures in accordance with Applicable Data Protection Law and Section 11 (Security) of this Addendum;

(d) keep confidentiality regarding the personal data processed in accordance with the Agreement;

(e) delete all personal data upon termination of the Agreement in accordance with Section 10 (Return or Deletion of Customer Content) of this Addendum; and

(f) only transfer personal data to sub-processors in accordance with Section 7 (Sub-processors) of this Addendum.

## **8. Singapore:**

8.1 The definition of "Applicable Data Protection Law" includes the Personal Data Protection Act 2012 ("*PDPA*").



8.2 Twilio will process personal data to a standard of protection in accordance with the PDPA by implementing adequate technical and organizational measures as set forth in Section 11 (Security) of this Addendum and complying with the terms of the Agreement.

## 9. Switzerland:

9.1 The definition of "Applicable Data Protection Law" includes the Swiss Federal Act on Data Protection, as revised ("*FADP*").

9.2 When Twilio engages a sub-processor under Section 7.1 (Authorization for Onward Sub-processing) of this Addendum, it will:

(a) require any appointed sub-processor to protect the Customer Content to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular, providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and

(b) require any appointed sub-processor to (i) agree in writing to only process personal data in a country that Switzerland has declared to have an "adequate" level of protection or (ii) only process personal data on terms equivalent to the EU Standard Contractual Clauses or pursuant to a Binding Corporate Rules approval granted by competent European Union data protection authorities.

9.3 To the extent that personal data transfers from Switzerland are subject to the EU Standard Contractual Clauses in accordance with Section 2.3 of Schedule 3 (Cross Border Data Transfer Mechanisms), the following amendments will apply to the EU Standard Contractual Clauses:

(a) references to "EU Member State" and "Member State" will be interpreted to include Switzerland, and

(b) insofar as the transfer or onward transfers are subject to the FADP:

(i) references to "Regulation (EU) 2016/679" are to be interpreted as references to the FADP;

(ii) the "competent supervisory authority" in Annex I, Part C will be the Swiss Federal Data Protection and Information Commissioner;

(iii) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by the laws of Switzerland; and

(iv) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Switzerland.

## 10. United Kingdom (UK):

10.1 References in this Addendum to “GDPR” will be deemed references to the corresponding laws and regulations of the United Kingdom, including, without limitation, the UK GDPR and Data Protection Act 2018.

10.2 When Twilio engages a sub-processor under Section 7.1 (Authorization for Onward Sub-processing) of this Addendum, it will:

(a) require any appointed sub-processor to protect the Customer Content to the standard required by Applicable Data Protection Law, such as including the same data protection obligations referred to in Article 28(3) of the GDPR, in particular providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the GDPR, and

(b) require any appointed sub-processor to (i) agree in writing to only process personal data in a country that the United Kingdom has declared to have an “adequate” level of protection or (ii) only process personal data on terms equivalent to the UK International Data Transfer Agreement or pursuant to a Binding Corporate Rules approval granted by competent United Kingdom data protection authorities.

10.3 Notwithstanding anything to the contrary in this Addendum or in the Agreement (including, without limitation, either party’s indemnification obligations), neither party will be responsible for any UK GDPR fines issued or levied under Article 83 of the UK GDPR against the other party by a regulatory authority or governmental body in connection with such other party’s violation of the UK GDPR.

10.4 Customer acknowledges that Twilio, as a controller, may be required under Applicable Data Protection Law to notify a regulatory authority of Security Incidents involving Customer Usage Data. If a regulatory authority requires Twilio to notify impacted data subjects with whom Twilio does not have a direct relationship (e.g., Customer’s end users), Twilio will notify Customer of this requirement. Customer will provide reasonable assistance to Twilio to notify the impacted data subjects.

## 11. United States of America:

11.1 “*US State Privacy Laws*” mean all state laws relating to the protection and processing of personal data in effect in the United States of America, which may include, without limitation, the California Consumer Privacy Act, as amended by the California Privacy Rights Act (“*CCPA*”), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act, and the Utah Consumer Privacy Act.

11.2 The definition of “Applicable Data Protection Law” includes US State Privacy Laws.

11.3 The following terms apply where Twilio processes personal data subject to the CCPA:

(a) The term “*personal information*”, as used in this Section 11.3, will have the meaning provided in the CCPA;

(b) Twilio is a service provider when processing Customer Content. Twilio will process any personal information contained in Customer Content only for the business purposes set forth in the Agreement, including the purpose of processing and processing activities set forth in this Addendum (“*Purpose*”). As a service provider, Twilio will not sell or share Customer Content or retain, use, or disclose Customer Content (i) for any purpose other than the Purpose, including retaining, using, or disclosing Customer Content for a commercial purpose other than the Purpose, or as otherwise permitted by the CCPA; or (ii) outside of the direct business relationship between Customer and Twilio;

(c) Twilio will (i) comply with obligations applicable to it as a service provider under the CCPA and (ii) provide personal information with the same level of privacy protection as is required by the CCPA. Customer is responsible for ensuring that it has complied, and will continue to comply, with the requirements of the CCPA in its use of the Services and its own processing of personal information;

(d) Customer will have the right to take reasonable and appropriate steps to help ensure that Twilio uses personal information in a manner consistent with Customer’s obligations under the CCPA;

(e) Twilio will notify Customer if it makes a determination that it can no longer meet its obligations as a service provider under the CCPA;

(f) Upon notice, Customer will have the right to take reasonable and appropriate steps in accordance with the Agreement to stop and remediate unauthorized use of personal information;

(g) Twilio will provide reasonable additional and timely assistance to assist Customer in complying with its obligations with respect to consumer requests as set forth in the Agreement;

(h) For any sub-processor used by Twilio to process personal information subject to the CCPA, Twilio will ensure that Twilio’s agreement with such sub-processor complies with the CCPA, including, without limitation, the contractual requirements for service providers and contractors;

(i) Twilio will not combine Customer Content that it receives from, or on behalf of, Customer, with personal information that it receives from, or on behalf of, another person or persons, or collects from its own interaction with the consumer, unless such combination is required to perform any business

purpose as permitted by the CCPA, including any regulations thereto, or by regulations adopted by the California Privacy Protection Agency; and

(j) Twilio certifies that it understands and will comply with its obligations under the CCPA.

11.4 Twilio acknowledges and confirms that it does not receive Customer Content as consideration for any Services provided to Customer.



**Note to copy:**

*The HubSpot Data Processing Agreement is made available at <https://legal.hubspot.com/dpa> and is incorporated into the HubSpot Customer Terms of Service available at <https://legal.hubspot.com/terms-of-service>, as specified in the HubSpot Customer Terms of Service.*

*For Customers that would like to receive a signed copy of the HubSpot Data Processing Agreement, we have made this copy available to you. This copy includes signatures on the Data Processing Agreement version last modified September 2, 2022, followed by a complete copy of the Standard Contractual Clauses and UK Addendum, which are incorporated by reference within the DPA. No changes made to this copy are agreed to by HubSpot, Inc. or its affiliates.*

*Please note that we update the Data Processing Agreement as we describe in the 'General Provisions' section below. Current Data Processing Agreement terms are available at <https://legal.hubspot.com/dpa> and archived Data Processing Agreement terms are available at <https://legal.hubspot.com/legal-stuff/archive>.*

*If you have any questions, please contact your HubSpot representative.*

## **HubSpot Data Processing Agreement**

Last Modified: November 15, 2022

This HubSpot Data Processing Agreement and its Annexes ("DPA") reflects the parties' agreement with respect to the Processing of Personal Data by us on behalf of you in connection with the HubSpot Subscription Services under the [HubSpot Customer Terms of Service](https://legal.hubspot.com/terms-of-service) available at <https://legal.hubspot.com/terms-of-service> between you and us (also referred to in this DPA as the "Agreement").

This DPA is supplemental to, and forms an integral part of, the Agreement and is effective upon its incorporation into the Agreement, which may be specified in the Agreement, an Order or an executed amendment to the Agreement. In case of any conflict or inconsistency with the terms of the Agreement, this DPA will take precedence over the terms of the Agreement to the extent of such conflict or inconsistency.

We update these terms from time to time. If you have an active HubSpot subscription, we will let you know when we do via email (if you have subscribed to receive email notifications via the link in our General Terms) or via in-app notification. You can find archived versions of the DPA in our archives at <https://legal.hubspot.com/legal-stuff/archive>.

The term of this DPA will follow the term of the Agreement. Terms not otherwise defined in this DPA will have the meaning as set forth in the Agreement.

1. Definitions
2. Customer Responsibilities
3. HubSpot Obligations
4. Data Subject Requests
5. Sub-Processors
6. Data Transfers
7. Additional Provisions for European Data
8. Additional Provisions for California Personal Information
9. General Provisions
10. Parties to this DPA

Annex 1 - Details of Processing

Annex 2 - Security Measures

Annex 3 - Sub-Processors

## **1. Definitions**

“California Personal Information” means Personal Data that is subject to the protection of the CCPA.

"CCPA" means California Civil Code Sec. 1798.100 et seq. (also known as the California Consumer Privacy Act of 2018).

"Consumer", "Business", "Sell" and "Service Provider" will have the meanings given to them in the CCPA.

“Controller” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“Data Protection Laws” means all applicable worldwide legislation relating to data protection and privacy which applies to the respective party in the role of Processing Personal Data in question under the Agreement, including without limitation European Data Protection Laws, the CCPA and the data protection and privacy laws of Australia and Singapore; in each case as amended, repealed, consolidated or replaced from time to time.

“Data Subject” means the individual to whom Personal Data relates.

"Europe" means the European Union, the European Economic Area and/or their member states, Switzerland and the United Kingdom.

“European Data” means Personal Data that is subject to the protection of European Data Protection Laws.

"European Data Protection Laws" means data protection laws applicable in Europe, including: (i) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ("GDPR"); (ii) Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector; and (iii) applicable national implementations of (i) and (ii); or (iii) GDPR as it forms parts of the United Kingdom domestic law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 ("UK GDPR"); and (iv) Swiss Federal Data Protection Act on 19 June 1992 and its Ordinance ("Swiss DPA"); in each case, as may be amended, superseded or replaced.

"Instructions" means the written, documented instructions issued by a Controller to a Processor, and directing the same to perform a specific or general action with regard to Personal Data (including, but not limited to, depersonalizing, blocking, deletion, making available).

"Permitted Affiliates" means any of your Affiliates that (i) are permitted to use the Subscription Services pursuant to the Agreement, but have not signed their own separate agreement with us and are not a "Customer" as defined under the Agreement, (ii) qualify as a Controller of Personal Data Processed by us, and (iii) are subject to European Data Protection Laws.

"Personal Data" means any information relating to an identified or identifiable individual where (i) such information is contained within Customer Data; and (ii) is protected similarly as personal data, personal information or personally identifiable information under applicable Data Protection Laws.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed by us and/or our Sub-Processors in connection with the provision of the Subscription Services. "Personal Data Breach" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

"Privacy Shield" means the EU-U.S. and Swiss-US Privacy Shield self-certification program operated by the U.S. Department of Commerce and approved by the European Commission pursuant to its Decision of July 12, 2016 and by the Swiss Federal Council on January 11, 2017 respectively; as may be amended, superseded or replaced.

"Privacy Shield Principles" means the Privacy Shield Principles (as supplemented by the Supplemental Principles) contained in Annex II to the European Commission Decision of July 12, 2016; as may be amended, superseded or replaced.



“Processing” means any operation or set of operations which is performed on Personal Data, encompassing the collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or erasure of Personal Data. The terms “Process”, “Processes” and “Processed” will be construed accordingly.

“Processor” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller.

“Standard Contractual Clauses” means the standard contractual clauses annexed to the European Commission’s Decision (EU) 2021/914 of 4 June 2021 currently found at [https://ec.europa.eu/info/system/files/1\\_en\\_annexe\\_acte\\_autonome\\_cp\\_part1\\_v5\\_0.pdf%20](https://ec.europa.eu/info/system/files/1_en_annexe_acte_autonome_cp_part1_v5_0.pdf%20), as may be amended, superseded or replaced.

“Sub-Processor” means any Processor engaged by us or our Affiliates to assist in fulfilling our obligations with respect to the provision of the Subscription Services under the Agreement. Sub-Processors may include third parties or our Affiliates but will exclude any HubSpot employee or consultant.

“UK Addendum” means the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018 currently found at <https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf>, as may be amended, superseded, or replaced.

## **2. Customer Responsibilities**

a. Compliance with Laws. Within the scope of the Agreement and in its use of the services, you will be responsible for complying with all requirements that apply to it under applicable Data Protection Laws with respect to its Processing of Personal Data and the Instructions it issues to us.

In particular but without prejudice to the generality of the foregoing, you acknowledge and agree that you will be solely responsible for: (i) the accuracy, quality, and legality of Customer Data and the means by which you acquired Personal Data; (ii) complying with all necessary transparency and lawfulness requirements under applicable Data Protection Laws for the collection and use of the Personal Data, including obtaining any necessary consents and authorizations (particularly for use by Customer for marketing purposes); (iii) ensuring you have the right to transfer, or provide access to, the Personal Data to us for Processing in accordance with the terms of the Agreement (including this DPA); (iv) ensuring that your Instructions to us regarding the Processing of Personal Data comply with applicable laws, including Data Protection Laws; and (v) complying with all laws (including Data Protection Laws) applicable to any emails or other content created, sent or managed through the Subscription Services, including those relating to obtaining consents (where required) to send emails, the content of the

emails and its email deployment practices. You will inform us without undue delay if you are not able to comply with your responsibilities under this 'Compliance with Laws' section or applicable Data Protection Laws.

b. Controller Instructions. The parties agree that the Agreement (including this DPA), together with your use of the Subscription Service in accordance with the Agreement, constitute your complete Instructions to us in relation to the Processing of Personal Data, so long as you may provide additional instructions during the subscription term that are consistent with the Agreement, the nature and lawful use of the Subscription Service.

c. Security. You are responsible for independently determining whether the data security provided for in the Subscription Service adequately meets your obligations under applicable Data Protection Laws. You are also responsible for your secure use of the Subscription Service, including protecting the security of Personal Data in transit to and from the Subscription Service (including to securely backup or encrypt any such Personal Data).

### **3. HubSpot Obligations**

a. Compliance with Instructions. We will only Process Personal Data for the purposes described in this DPA or as otherwise agreed within the scope of your lawful Instructions, except where and to the extent otherwise required by applicable law. We are not responsible for compliance with any Data Protection Laws applicable to you or your industry that are not generally applicable to us.

b. Conflict of Laws. If we become aware that we cannot Process Personal Data in accordance with your Instructions due to a legal requirement under any applicable law, we will (i) promptly notify you of that legal requirement to the extent permitted by the applicable law; and (ii) where necessary, cease all Processing (other than merely storing and maintaining the security of the affected Personal Data) until such time as you issue new Instructions with which we are able to comply. If this provision is invoked, we will not be liable to you under the Agreement for any failure to perform the applicable Subscription Services until such time as you issue new lawful Instructions with regard to the Processing.

c. Security. We will implement and maintain appropriate technical and organizational measures to protect Personal Data from Personal Data Breaches, as described under Annex 2 to this DPA ("Security Measures"). Notwithstanding any provision to the contrary, we may modify or update the Security Measures at our discretion provided that such modification or update does not result in a material degradation in the protection offered by the Security Measures.

d. Confidentiality. We will ensure that any personnel whom we authorize to Process Personal Data on our behalf is subject to appropriate confidentiality obligations (whether a contractual or statutory duty) with respect to that Personal Data.

e. Personal Data Breaches. We will notify you without undue delay after we become aware of any Personal Data Breach and will provide timely information relating to the Personal Data Breach as it becomes known or reasonably requested by you. At your request, we will promptly provide you with such reasonable assistance as necessary to enable you to notify relevant Personal Data Breaches to competent authorities and/or affected Data Subjects, if you are required to do so under Data Protection Laws.

f. Deletion or Return of Personal Data. We will delete or return all Customer Data, including Personal Data (including copies thereof) Processed pursuant to this DPA, on termination or expiration of your Subscription Service in accordance with the procedures set out in our Product Specific Terms. This term will apply except where we are required by applicable law to retain some or all of the Customer Data, or where we have archived Customer Data on back-up systems, which data we will securely isolate and protect from any further Processing and delete in accordance with our deletion practices. You may request the deletion of your HubSpot account after expiration or termination of your subscription by sending a request using our privacy request form at <https://preferences.hubspot.com/privacy>. You may also cancel your account in accordance with the 'Early Cancellation' section of the Customer Terms of Service and request permanent deletion by following the instructions found <https://knowledge.hubspot.com/account/how-do-i-cancel-my-hubspot-account>. You may retrieve your Customer Data from your account in accordance with our 'Retrieval of Customer Data' sections throughout our Product Specific Terms.

#### **4. Data Subject Requests**

The Subscription Service provides you with a number of controls that you can use to retrieve, correct, delete or restrict Personal Data, which you can use to assist it in connection with its obligations under Data Protection Laws, including your obligations relating to responding to requests from Data Subjects to exercise their rights under applicable Data Protection Laws ("Data Subject Requests").

To the extent that you are unable to independently address a Data Subject Request through the Subscription Service, then upon your written request we will provide reasonable assistance to you to respond to any Data Subject Requests or requests from data protection authorities relating to the Processing of Personal Data under the Agreement. You will reimburse us for the commercially reasonable costs arising from this assistance.

If a Data Subject Request or other communication regarding the Processing of Personal Data under the Agreement is made directly to us, we will promptly inform you and will advise the Data Subject to submit their request to you. You will be solely responsible for responding substantively to any such Data Subject Requests or communications involving Personal Data.

#### **5. Sub-Processors**

You agree we may engage Sub-Processors to Process Personal Data on your behalf, and we do so in three ways. First, we may engage Sub-Processors to assist us with hosting and infrastructure. Second, we may engage with Sub-Processors to support product features and integrations. Third, we may engage with HubSpot Affiliates as Sub-Processors for service and support. Some Sub-Processors will apply to you as default, and some Sub-Processors will apply only if you opt-in.

We have currently appointed, as Sub-Processors, the third parties and HubSpot Affiliates listed in Annex 3 to this DPA. You may subscribe to receive notifications by email if we add or replace any Sub-Processors by completing the form available at <https://legal.hubspot.com/subscribe-subprocessor-updates>. If you opt-in to receive such email, we will notify you at least 30 days prior to any such change.

Where we engage Sub-Processors, we will impose data protection terms on the Sub-Processors that provide at least the same level of protection for Personal Data as those in this DPA (including, where appropriate, the Standard Contractual Clauses), to the extent applicable to the nature of the services provided by such Sub-Processors. We will remain responsible for each Sub-Processor's compliance with the obligations of this DPA and for any acts or omissions of such Sub-Processor that cause us to breach any of its obligations under this DPA.

## 6. Data Transfers

You acknowledge and agree that we may access and Process Personal Data on a global basis as necessary to provide the Subscription Service in accordance with the Agreement, and in particular that Personal Data may be transferred to and Processed by HubSpot, Inc. in the United States and to other jurisdictions where HubSpot Affiliates and Sub-Processors have operations. Wherever Personal Data is transferred outside its country of origin, each party will ensure such transfers are made in compliance with the requirements of Data Protection Laws.

## 7. Additional Provisions for European Data

a. Scope. This 'Additional Provisions for European Data' section will apply only with respect to European Data.

b. Roles of the Parties. When Processing European Data in accordance with your Instructions, the parties acknowledge and agree that you are the Controller of European Data and we are the Processor.

c. Instructions. If we believe that your Instruction infringes European Data Protection Laws (where applicable), we will inform you without delay.

d. Objection to New Sub-Processors. We will give you the opportunity to object to the engagement of new Sub-Processors on reasonable grounds relating to the protection of Personal Data within 30 days of notifying you in accordance with the 'Sub-Processors'

section. If you do notify us of such an objection, the parties will discuss your concerns in good faith with a view to achieving a commercially reasonable resolution. If no such resolution can be reached, we will, at our sole discretion, either not appoint the new Sub-Processor, or permit you to suspend or terminate the affected Subscription Service in accordance with the termination provisions of the Agreement without liability to either party (but without prejudice to any fees incurred by you prior to suspension or termination). The parties agree that by complying with this sub-section (d), HubSpot fulfills its obligations under Sections 9 of the Standard Contractual Clauses.

e. Sub-Processor Agreements. For the purposes of Clause 9(c) of the Standard Contractual Clauses, you acknowledge that we may be restricted from disclosing Sub-Processor agreements but we will use reasonable efforts to require any Sub-Processor we appoint to permit it to disclose the Sub-Processor agreement to you and will provide (on a confidential basis) all information we reasonably can.

f. Data Protection Impact Assessments and Consultation with Supervisory Authorities. To the extent that the required information is reasonably available to us, and you do not otherwise have access to the required information, we will provide reasonable assistance to you with any data protection impact assessments, and prior consultations with supervisory authorities (for example, the French Data Protection Agency (CNIL), the Berlin Data Protection Authority (BlnBDI) and the UK Information Commissioner's Office (ICO)) or other competent data privacy authorities to the extent required by European Data Protection Laws.

g. Transfer Mechanisms for Data Transfers.

(A) HubSpot will not transfer European Data to any country or recipient not recognized as providing an adequate level of protection for Personal Data (within the meaning of applicable European Data Protection Laws), unless it first takes all such measures as are necessary to ensure the transfer is in compliance with applicable European Data Protection Laws. Such measures may include (without limitation) transferring such data to a recipient that is covered by a suitable framework or other legally adequate transfer mechanism recognized by the relevant authorities or courts as providing an adequate level of protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with European Data Protection Laws, or to a recipient that has executed appropriate standard contractual clauses in each case as adopted or approved in accordance with applicable European Data Protection Laws.

(B) You acknowledge that in connection with the performance of the Subscription Services, HubSpot, Inc. is a recipient of European Data in the United States. Subject to sub-sections (C) and (D), the parties agree that the Standard Contractual Clauses will be incorporated by reference and form part of the Agreement as follows:

- (a) EEA Transfers. In relation to European Data that is subject to the GDPR (i) Customer is the "data exporter" and HubSpot, Inc. is the "data importer"; (ii) the Module Two terms apply to the extent the Customer is a Controller of European



Data and the Module Three terms apply to the extent the Customer is a Processor of European Data; (iii) in Clause 7, the optional docking clause applies; (iv) in Clause 9, Option 2 applies and changes to Sub-Processors will be notified in accordance with the 'Sub-Processors' section of this DPA; (v) in Clause 11, the optional language is deleted; (vi) in Clauses 17 and 18, the parties agree that the governing law and forum for disputes for the Standard Contractual Clauses will be determined in accordance with the 'Contracting Entity; Applicable Law; Notice' section of the Jurisdiction Specific Terms or, if such section does not specify an EU Member State, the Republic of Ireland (without reference to conflicts of law principles); (vii) the Annexes of the Standard Contractual Clauses will be deemed completed with the information set out in the Annexes of this DPA; and (viii) if and to the extent the Standard Contractual Clauses conflict with any provision of this DPA the Standard Contractual Clauses will prevail to the extent of such conflict.

- (b) UK Transfers. In relation to European Data that is subject to the UK GDPR, the Standard Contractual Clauses will apply in accordance with sub-section (a) and the following modifications (i) the Standard Contractual Clauses will be modified and interpreted in accordance with the UK Addendum, which will be incorporated by reference and form an integral part of the Agreement; (ii) Tables 1, 2 and 3 of the UK Addendum will be deemed completed with the information set out in the Annexes of this DPA and Table 4 will be deemed completed by selecting "neither party"; and (iii) any conflict between the terms of the Standard Contractual Clauses and the UK Addendum will be resolved in accordance with Section 10 and Section 11 of the UK Addendum.
- (c) Swiss Transfers. In relation to European Data that is subject to the Swiss DPA, the Standard Contractual Clauses will apply in accordance with sub-section (a) and the following modifications (i) references to "Regulation (EU) 2016/679" will be interpreted as references to the Swiss DPA; (ii) references to "EU", "Union" and "Member State law" will be interpreted as references to Swiss law; and (iii) references to the "competent supervisory authority" and "competent courts" will be replaced with the "the Swiss Federal Data Protection and Information Commissioner " and the "relevant courts in Switzerland".

(C) Where the HubSpot contracting entity under the Agreement is not HubSpot, Inc., such contracting entity (not HubSpot, Inc.) will remain fully and solely responsible and liable to you for the performance of the Standard Contractual Clauses by HubSpot, Inc., and you will direct any instructions, claims or enquiries in relation to the Standard Contractual Clauses to such contracting entity. If HubSpot cannot comply with its obligations under the Standard Contractual Clauses or is breach of any warranties under the Standard Contractual Clauses or UK Addendum (as applicable) for any reason, and you intend to suspend the transfer of European Data to HubSpot or terminate the Standard Contractual Clauses ,or UK Addendum, you agree to provide us with reasonable notice to enable us to cure such non-compliance and reasonably cooperate with us to identify what additional safeguards, if any, may be implemented to remedy such non-compliance. If we have not or cannot cure the non-compliance, you may suspend or terminate the affected part of the Subscription Service in accordance

with the Agreement without liability to either party (but without prejudice to any fees you have incurred prior to such suspension or termination).

(D) Although HubSpot, Inc. does not currently rely on the EU-US Privacy Shield as a legal basis for transfers of European Data in light of the judgment of the Court of Justice of the EU in Case C-311/18, for as long as HubSpot, Inc. is self-certified to the Privacy Shield HubSpot Inc will process European Data in compliance with the Privacy Shield Principles and let you know if it is unable to comply with this requirement. In the event that HubSpot adopts an alternative transfer mechanism (including any new or successor version of the EU-US Privacy Shield) for transfers of European Data to HubSpot, Inc., such alternative transfer mechanism will apply automatically instead of the Standard Contractual Clauses described in this DPA (but only to the extent such alternative transfer mechanism complies with European Data Protection Laws), and you agree to execute such other documents or take such action as may be reasonably necessary to give legal effect such alternative transfer mechanism.

h. Demonstration of Compliance. We will make all information reasonably necessary to demonstrate compliance with this DPA available to you and allow for and contribute to audits, including inspections conducted by or your auditor in order to assess compliance with this DPA. You acknowledge and agree that you will exercise your audit rights under this DPA and Clause 8.9 of the Standard Contractual Clauses by instructing us to comply with the audit measures described in this 'Demonstration of Compliance' section. You acknowledge that the Subscription Service is hosted by our hosting Sub-Processors who maintain independently validated security programs (including SOC 2 and ISO 27001) and that our systems are audited annually as part of SOC 2 compliance and regularly tested by independent third party penetration testing firms. Upon request, we will supply (on a confidential basis) our SOC 2 report and summary copies of our penetration testing report(s) to you so that you can verify our compliance with this DPA. You may download copies of these documents from HubSpot's Security website at <https://legal.hubspot.com/security#downloadable-reports>. Further, at your written request, we will provide written responses (on a confidential basis) to all reasonable requests for information made by you necessary to confirm our compliance with this DPA, provided that you will not exercise this right more than once per calendar year unless you have reasonable grounds to suspect non-compliance with the DPA.

## **8. Additional Provisions for California Personal Information**

a. Scope. The 'Additional Provisions for California Personal Information' section of the DPA will apply only with respect to California Personal Information.

b. Roles of the Parties. When processing California Personal Information in accordance with your Instructions, the parties acknowledge and agree that you are a Business and we are a Service Provider for the purposes of the CCPA.

c. Responsibilities. The parties agree that we will Process California Personal Information as a Service Provider strictly for the purpose of performing the Subscription



Services and Consulting Services under the Agreement (the "Business Purpose") or as otherwise permitted by the CCPA, including as described in the 'Usage Data' section of our Privacy Policy.

## 9. General Provisions

a. Amendments. Notwithstanding anything else to the contrary in the Agreement and without prejudice to the 'Compliance with Instructions' or 'Security' sections of this DPA, we reserve the right to make any updates and changes to this DPA and the terms that apply in the 'Amendment; No Waiver' section of the General Terms will apply.

b. Severability. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

c. Limitation of Liability. Each party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA (and any other DPAs between the parties) and the Standard Contractual Clauses (where applicable), whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the 'Limitation of Liability' section of the General Terms and any reference in such section to the liability of a party means aggregate liability of that party and all of its Affiliates under the Agreement (including this DPA). For the avoidance of doubt, if HubSpot, Inc. is not a party to the Agreement, the 'Limitation of Liability' section of the General Terms will apply as between you and HubSpot, Inc., and in such respect any references to 'HubSpot', 'we', 'us' or 'our' will include both HubSpot, Inc. and the HubSpot entity that is a party to the Agreement. In no event will either party's liability be limited with respect to any individual's data protection rights under this DPA (including the Standard Contractual Clauses) or otherwise.

d. Governing Law. This DPA will be governed by and construed in accordance with the 'Contracting Entity; Applicable Law; Notice' sections of the Jurisdiction Specific Terms, unless required otherwise by Data Protection Laws.

## 10. Parties to this DPA

a. Permitted Affiliates. By signing the Agreement, you enter into this DPA (including, where applicable, the Standard Contractual Clauses) on behalf of yourself and in the name and on behalf of your Permitted Affiliates. For the purposes of this DPA only, and except where indicated otherwise, the terms "Customer", "you" and "your" will include you and such Permitted Affiliates.

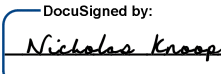
b. Authorization. The legal entity agreeing to this DPA as Customer represents that it is authorized to agree to and enter into this DPA for and on behalf of itself and, as applicable, each of its Permitted Affiliates.

c. Remedies. The parties agree that (i) solely the Customer entity that is the contracting party to the Agreement will exercise any right or seek any remedy any Permitted Affiliate may have under this DPA on behalf of its Affiliates, and (ii) the Customer entity that is the contracting party to the Agreement will exercise any such rights under this DPA not separately for each Permitted Affiliate individually but in a combined manner for itself and all of its Permitted Affiliates together. The Customer entity that is the contracting entity is responsible for coordinating all Instructions, authorizations and communications with us under the DPA and will be entitled to make and receive any communications related to this DPA on behalf of its Permitted Affiliates.

d. Other rights. The parties agree that you will, when reviewing our compliance with this DPA pursuant to the 'Demonstration of Compliance' section, take all reasonable measures to limit any impact on us and our Affiliates by combining several audit requests carried out on behalf of the Customer entity that is the contracting party to the Agreement and all of its Permitted Affiliates in one single audit.

***EXECUTED BY THE PARTIES AUTHORIZED REPRESENTATIVES:***

**HubSpot, Inc., by and on behalf of its affiliates, as applicable.**

Signature:  \_\_\_\_\_  
DocuSigned by:  
2D95909F17D54E7...

Name: Nicholas Knoop

Title: Data Protection Officer

Controller: \_\_\_\_\_

Signature: \_\_\_\_\_

Name: \_\_\_\_\_

Title: \_\_\_\_\_

Date: \_\_\_\_\_

## **Annex 1 - Details of Processing**

### **A. List of Parties**

#### **Data exporter:**

Name: The Customer, as defined in the HubSpot Customer Terms of Service (on behalf of itself and Permitted Affiliates)

Address: The Customer's address, as set out in the Order Form

Contact person's name, position and contact details: The Customer's contact details, as set out in the Order Form and/or as set out in the Customer's HubSpot Account

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the HubSpot Subscription Services under the HubSpot Customer Terms of Service

Role (controller/processor): Controller

#### **Data importer:**

Name: HubSpot, Inc.

Address: 25 First Street, 2nd Floor, Cambridge, MA 02141, USA

Contact person's name, position and contact details: Nicholas Knoop, Data Protection Officer, HubSpot, Inc., 25 First Street, 2nd Floor, Cambridge, MA 02141 USA

Activities relevant to the data transferred under these Clauses: Processing of Personal Data in connection with Customer's use of the HubSpot Subscription Services under the HubSpot Customer Terms of Service

Role (controller/processor): Processor

### **B. Description of Transfer**

#### **Categories of Data Subjects whose Personal Data is Transferred**

You may submit Personal Data in the course of using the Subscription Service, the extent of which is determined and controlled by you in your sole discretion, and which may include, but is not limited to Personal Data relating to the following categories of Data Subjects:

Your Contacts and other end users including your employees, contractors, collaborators, customers, prospects, suppliers and subcontractors. Data Subjects may

also include individuals attempting to communicate with or transfer Personal Data to your end users.

### **Categories of Personal Data Transferred**

You may submit Personal Data to the Subscription Services, the extent of which is determined and controlled by you in your sole discretion, and which may include but is not limited to the following categories of Personal Data:

- a. Contact Information (as defined in the General Terms).
- b. Any other Personal Data submitted by, sent to, or received by you, or your end users, via the Subscription Service.

### **Sensitive Data transferred and applied restrictions or safeguards**

The parties do not anticipate the transfer of sensitive data.

### **Frequency of the transfer**

Continuous

### **Nature of the Processing**

Personal Data will be Processed in accordance with the Agreement (including this DPA) and may be subject to the following Processing activities:

1. Storage and other Processing necessary to provide, maintain and improve the Subscription Services provided to you; and/or
2. Disclosure in accordance with the Agreement (including this DPA) and/or as compelled by applicable laws.

### **Purpose of the transfer and further processing**

We will Process Personal Data as necessary to provide the Subscription Services pursuant to the Agreement, as further specified in the Order Form, and as further instructed by you in your use of the Subscription Services.

### **Period for which Personal Data will be retained**

Subject to the 'Deletion or Return of Personal Data' section of this DPA, we will Process Personal Data for the duration of the Agreement, unless otherwise agreed in writing.

## **C. Competent Supervisory Authority**

For the purposes of the Standard Contractual Clauses, the supervisory authority that will act as competent supervisory authority will be determined in accordance with GDPR.

## Annex 2 - Security Measures

We currently observe the Security Measures described in this Annex 2. All capitalized terms not otherwise defined herein will have the meanings as set forth in the General Terms. For more information on these security measures, please refer to HubSpot's SOC 2 Type II Report, SOC 3 Report, Security Overview and Penetration Test Summaries, available at <https://legal.hubspot.com/security#downloadable-reports>.

### a) Access Control

#### i) Preventing Unauthorized Product Access

**Outsourced processing:** We host our Service with outsourced cloud infrastructure providers. Additionally, we maintain contractual relationships with vendors in order to provide the Service in accordance with our DPA. We rely on contractual agreements, privacy policies, and vendor compliance programs in order to protect data processed or stored by these vendors.

**Physical and environmental security:** We host our product infrastructure with multi-tenant, outsourced infrastructure providers. We do not own or maintain hardware located at the outsourced infrastructure providers' data centers. Production servers and client-facing applications are logically and physically secured from our internal corporate information systems. The physical and environmental security controls are audited for SOC 2 Type II and ISO 27001 compliance, among other certifications.

**Authentication:** We implement a uniform password policy for our customer products. Customers who interact with the products via the user interface must authenticate before accessing non-public customer data.

**Authorization:** Customer Data is stored in multi-tenant storage systems accessible to Customers via only application user interfaces and application programming interfaces. Customers are not allowed direct access to the underlying application infrastructure. The authorization model in each of our products is designed to ensure that only the appropriately assigned individuals can access relevant features, views, and customization options. Authorization to data sets is performed through validating the user's permissions against the attributes associated with each data set.

**Application Programming Interface (API) access:** Public product APIs may be accessed using an API key or through OAuth authorization.

#### ii) Preventing Unauthorized Product Use

We implement industry standard access controls and detection capabilities for the internal networks that support its products.

**Access controls:** Network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the product infrastructure. The technical measures implemented differ between infrastructure providers and include Virtual Private Cloud (VPC) implementations, security group assignment, and traditional firewall rules.

**Intrusion detection and prevention:** We implement a Web Application Firewall (WAF) solution to protect hosted customer websites and other internet-accessible applications. The WAF is designed to identify and prevent attacks against publicly available network services.

**Static code analysis:** Code stored in our source code repositories is checked for best practices and identifiable software flaws using automated tooling.

**Penetration testing:** We maintain relationships with industry recognized penetration testing service providers for four annual penetration tests. The intent of the penetration tests is to identify and resolve foreseeable attack vectors and potential abuse scenarios. Penetration tests are performed against the application layers and infrastructure layers of the HubSpot technology stack.

**Bug bounty:** A bug bounty program invites and incentivizes independent security researchers to ethically discover and disclose security flaws. We implement a bug bounty program in an effort to widen the available opportunities to engage with the security community and improve the product defenses against sophisticated attacks.

### iii) Limitations of Privilege & Authorization Requirements

**Product access:** A subset of our employees have access to the products and to customer data via controlled interfaces. The intent of providing access to a subset of employees is to provide effective customer support, product development and research, to troubleshoot potential problems, to detect and respond to security incidents and implement data security. Access is enabled through “just in time” (JITA) requests for access; all such requests are logged. Employees are granted access by role, and reviews of high risk privilege grants are initiated daily. Administrative or high risk access permissions are reviewed at least once every six months.

**Background checks:** Where permitted by applicable law, HubSpot employees undergo a third-party background or reference checks. In the United States, employment offers are contingent upon the results of a third-party background check. All HubSpot employees are required to conduct themselves in a manner consistent with company guidelines, non-disclosure requirements, and ethical standards.

## **b) Transmission Control**



**In-transit:** We require HTTPS encryption (also referred to as SSL or TLS) on all login interfaces and for free on every customer site hosted on the HubSpot products. Our HTTPS implementation uses industry standard algorithms and certificates.

**At-rest:** We store user passwords following policies that follow industry standard practices for security. We have implemented technologies to ensure that stored data is encrypted at rest.

### **c) Input Control**

**Detection:** We designed our infrastructure to log extensive information about the system behavior, traffic received, system authentication, and other application requests. Internal systems aggregate log data and alert appropriate employees of malicious, unintended, or anomalous activities. Our personnel, including security, operations, and support personnel, are responsive to known incidents.

**Response and tracking:** We maintain a record of known security incidents that includes description, dates and times of relevant activities, and incident disposition. Suspected and confirmed security incidents are investigated by security, operations, or support personnel; and appropriate resolution steps are identified and documented. For any confirmed incidents, we will take appropriate steps to minimize product and Customer damage or unauthorized disclosure. Notification to you will be in accordance with the terms of the Agreement.

### **d) Availability Control**

**Infrastructure availability:** The infrastructure providers use commercially reasonable efforts to ensure a minimum of 99.95% uptime. The providers maintain a minimum of N+1 redundancy to power, network, and heating, ventilation and air conditioning (HVAC) services.

**Fault tolerance:** Backup and replication strategies are designed to ensure redundancy and fail-over protections during a significant processing failure. Customer data is backed up to multiple durable data stores and replicated across multiple availability zones.

**Online replicas and backups:** Where feasible, production databases are designed to replicate data between no less than 1 primary and 1 secondary database. All databases are backed up and maintained using at least industry standard methods.

**Disaster Recovery Plans:** We maintain and regularly test disaster recovery plans to help ensure availability of information following interruption to, or failure of, critical business processes.

Our products are designed to ensure redundancy and seamless failover. The server instances that support the products are also architected with a goal to prevent single

points of failure. This design assists our operations in maintaining and updating the product applications and backend while limiting downtime.

### Annex 3 - Sub-Processors

This Annex 3 is incorporated into the [DPA](#) and [Agreement](#). This annex explains how HubSpot engages with Sub-Processors.

1. Infrastructure Sub-Processors
2. Feature Specific Sub-Processors
3. HubSpot Affiliate Sub-Processors
4. Updates to Sub-Processors

Please review each section for additional details.

#### 1. Infrastructure Sub-Processors

To help HubSpot deliver the Subscription Service, we engage Sub-Processors to support our infrastructure. By agreeing to the [DPA](#), you agree all of these Sub-Processors may have access to Customer Data.

| Third Party Sub-Processor | Purpose                                   | Applicable Service                                                                                                                                                              | US Data Center Sub-Processor Location: United States | EU Data Center Sub-Processor Location: EU or Other                                                                         |
|---------------------------|-------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| Amazon Web Services, Inc  | Hosting & Infrastructure                  | Used as a on-demand cloud computing platforms and APIs                                                                                                                          | United States                                        | Germany                                                                                                                    |
| Cloudflare                | Content Delivery Network                  | Used as a web infrastructure and website security, providing content delivery network services, DDoS mitigation, internet security, and distributed domain name server services | United States                                        | Local<br><br>**Data Centers located all around the world. Traffic will be automatically routed to the nearest data center. |
| Google, Inc.              | Infrastructure - Regional Data Processing | Data hosting provider                                                                                                                                                           | United States                                        | Germany                                                                                                                    |

|                 |                |                                                                 |               |         |
|-----------------|----------------|-----------------------------------------------------------------|---------------|---------|
| Snowflake, Inc. | Infrastructure | Data warehouse solution which serves as the repository of data. | United States | Germany |
|-----------------|----------------|-----------------------------------------------------------------|---------------|---------|

\*\*For further information regarding Cloudflare services, visit <https://blog.cloudflare.com/introducing-regional-services/#eu>.

## 2. Feature Specific Sub-Processors

Some of our features and integrations require the use of additional Sub-Processors. Some Sub-Processors will apply to you as a default, and some Sub-Processors will apply to you only if and when you opt-in. We will notify you before you turn on a feature or install an integration that requires support from an opt-in Sub-Processor where indicated in the table below.

| Third Party Sub-Processor | Purpose                           | Applicable Service                                                                | US Data Center Sub-Processor Location: United States | EU Data Center Sub-Processor Location: EU or Other |
|---------------------------|-----------------------------------|-----------------------------------------------------------------------------------|------------------------------------------------------|----------------------------------------------------|
| Ably.io                   | Conversation & Chat Functionality | Used to support conversations/chat features in the HubSpot product                | United States                                        | Ireland and Germany                                |
| ConvertAPI                | File Functionality                | Used for files and documents conversion for websites and web/desktop applications | United States                                        | Germany                                            |
| Google reCAPTCHA          | Form submission spam prevention   | Used for HubSpot form submission spam prevention                                  | United States                                        | *United States                                     |

|                                         |                            |                                                                                                                                                                                                                                |               |                           |
|-----------------------------------------|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|---------------------------|
| HelloSign                               | E-Signature Functionality  | Used for HubSpot product E-signature solution for deals                                                                                                                                                                        | United States | Germany                   |
| Litmus                                  | Email Functionality        | Used for email previews                                                                                                                                                                                                        | United States | N/A in the EU data center |
| Meta Platforms, Inc.<br><br>OPT-IN ONLY | Conversation Functionality | Used to support the connection of your WhatsApp Business account to the conversations inbox.<br><br>Use of WhatsApp is an opt-in integration. If you do not install the WhatsApp integration, no Customer Data will be shared. | United States | *United States            |
| Mux                                     | Video Functionality        | Used for HubSpot video service provider                                                                                                                                                                                        | United States | *United States            |
| Twilio, Inc.                            | Calling Functionality      | Used as a service which allows HubSpot calling                                                                                                                                                                                 | United States | *United States            |

\*You may choose not to use the functionality provided by our Sub-Processors marked with an asterisk above. Please see the HubSpot Regional Data Hosting Policy available at <https://legal.hubspot.com/hubspot-regional-data-hosting-policy> for further information.

### 3. HubSpot Affiliate Sub-Processors

To help HubSpot deliver the Subscription Service, we engage HubSpot Affiliates as Sub-Processors to assist with our data processing activities. By agreeing to the [DPA](#), you agree all of these Sub-Processors may have access to Customer Data.

| HubSpot Affiliate Sub-Processor | Purpose            | Location      |
|---------------------------------|--------------------|---------------|
| HubSpot Inc.                    | Services & Support | United States |
| HubSpot Ireland Ltd             | Services & Support | Ireland       |

|                               |                    |                 |
|-------------------------------|--------------------|-----------------|
| HubSpot Germany GmbH          | Services & Support | Germany         |
| HubSpot Australia Pty. Ltd.   | Services & Support | Australia       |
| HubSpot Asia Pte. Ltd.        | Services & Support | Singapore       |
| HubSpot Japan KK              | Services & Support | Japan           |
| HubSpot Latin America, S.A.S. | Services & Support | Colombia        |
| HubSpot Sweden                | Services & Support | Sweden          |
| HubSpot France S.A.S.         | Services & Support | France          |
| HubSpot UK Holdings Ltd.      | Services & Support | United Kingdom  |
| HubSpot Belgium NV            | Services & Support | Belgium         |
| HubSpot Canada Inc.           | Services & Support | Canada          |
| HubSpot Spain, S.L.           | Services & Support | Spain           |
| HubSpot Netherlands B.V.      | Services & Support | The Netherlands |

#### 4. Updates to Sub-Processors

Due to the nature of our global business and our ongoing efforts to delight our customers, our business needs and services providers may change from time to time. For example, we may deprecate a service provider to consolidate and minimize our use of service providers. Similarly, we may add a service provider if we believe that doing so will enhance our ability to deliver our Subscription Service.

You may subscribe to notifications by email if we add or replace any Sub-Processors by completing the form available at <https://legal.hubspot.com/subscribe-subprocessor-updates>. If you opt-in to receive such email, we will notify you at least 30 days prior to any such change.

For more information on HubSpot's privacy practices, please visit our [Privacy Policy](#). If you have any questions regarding this page, please contact us at [privacy@hubspot.com](mailto:privacy@hubspot.com).



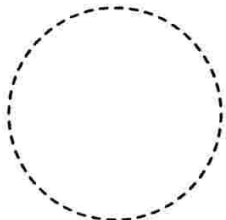
**On behalf of the data exporter:**

Name (written out in full): ...

Position: ...

Address: ...

Other information necessary in order for the contract to be binding (if any):

|                                                                                   |               |
|-----------------------------------------------------------------------------------|---------------|
|  | Signature ... |
|-----------------------------------------------------------------------------------|---------------|

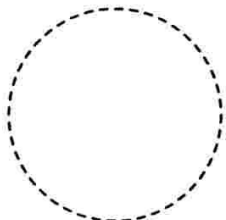
**On behalf of the data importer:**

Name (written out in full): Nicholas Knoop

Position: Data Protection Officer

Address: 25 First Street, Cambridge, MA 02492 U.S.A.

Other information necessary in order for the contract to be binding (if any):

|                                                                                    |                                                                                                                                   |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
|  | <div>Signature ...</div> <div><small>DocuSigned by:</small><br/><i>Nicholas Knoop</i><br/><small>2D95909F17D54E7...</small></div> |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|

## Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

This Appendix forms part of the Standard Contractual Clauses. A description of the Details of Processing, including (i) List of Parties, (ii) Description of the Transfer and (iii) Competent Supervisory Authority are set out in Annex 1 of the DPA.

### DATA EXPORTER

Name: ...

Authorised Signature ...

### DATA IMPORTER

Name: Nicholas Knoop, Data Protection Officer

Authorised Signature

DocuSigned by:

*Nicholas Knoop*

2D95909F17D54E7...

## Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

A description of the technical and organisational security measures implemented by the data importer in accordance with Standard Contractual Clauses are set out in Annex 2 of the DPA.

DATA EXPORTER

Name: ...

Authorised Signature ...

DATA IMPORTER

Name: Nicholas Knoop, Data Protection Officer

Authorised Signature

DocuSigned by:  
*Nicholas Knoop*  
2D95909F17D54E7...

### Appendix 3 to the Standard Contractual Clauses

This Appendix forms part of the Standard Contractual Clauses (the 'Clauses').

The List of Sub-Processors used by the data importer are listed in accordance with Clause 9(a) of the Standard Contractual Clauses are set out in Annex 2 of the DPA:

Name: ...

Authorised Signature ...

DATA IMPORTER

Name: Nicholas Knoop, Data Protection Officer

Authorised Signature

DocuSigned by:

*Nicholas Knoop*

2D95909F17D54E7...



EUROPEAN  
COMMISSION

Brussels, 4.6.2021  
C(2021) 3972 final

ANNEX

**ANNEX**

*to the*

**COMMISSION IMPLEMENTING DECISION**

**on standard contractual clauses for the transfer of personal data to third countries  
pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council**

## **ANNEX**

### **STANDARD CONTRACTUAL CLAUSES**

#### **SECTION I**

##### *Clause 1*

##### ***Purpose and scope***

- (a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)<sup>1</sup> for the transfer of personal data to a third country.
- (b) The Parties:
  - (i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter “entity/ies”) transferring the personal data, as listed in Annex I.A. (hereinafter each “data exporter”), and
  - (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)have agreed to these standard contractual clauses (hereinafter: “Clauses”).
- (c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
- (d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

##### *Clause 2*

##### ***Effect and invariability of the Clauses***

- (a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to

---

<sup>1</sup> Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision [...].

select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

- (b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### *Clause 3*

#### ***Third-party beneficiaries***

- (a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
  - (ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
  - (iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
  - (iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
  - (v) Clause 13;
  - (vi) Clause 15.1(c), (d) and (e);
  - (vii) Clause 16(e);
  - (viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.
- (b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

### *Clause 4*

#### ***Interpretation***

- (a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
- (c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.



*Clause 5****Hierarchy***

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

*Clause 6****Description of the transfer(s)***

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

*Clause 7 - Optional****Docking clause***

- (a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.
- (b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.
- (c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

**SECTION II – OBLIGATIONS OF THE PARTIES***Clause 8****Data protection safeguards***

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**MODULE ONE: Transfer controller to controller****8.1 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

- (i) where it has obtained the data subject's prior consent;
- (ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

## **8.2 Transparency**

- (a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
  - (i) of its identity and contact details;
  - (ii) of the categories of personal data processed;
  - (iii) of the right to obtain a copy of these Clauses;
  - (iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
- (b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
- (c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
- (d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

## **8.3 Accuracy and data minimisation**

- (a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
- (b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
- (c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

## **8.4 Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures

to ensure compliance with this obligation, including erasure or anonymisation<sup>2</sup> of the data and all back-ups at the end of the retention period.

## **8.5 Security of processing**

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- (b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
- (e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
- (f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

---

<sup>2</sup> This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

- (g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

## **8.6 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

## **8.7 Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union<sup>3</sup> (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

- (i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
- (iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
- (iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
- (v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or
- (vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

---

<sup>3</sup> The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

#### **8.8 Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

#### **8.9 Documentation and compliance**

- (a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
- (b) The data importer shall make such documentation available to the competent supervisory authority on request.

### **MODULE TWO: Transfer controller to processor**

#### **8.1 Instructions**

- (a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
- (b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

#### **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

#### **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

#### **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

## **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

## **8.6 Security of processing**

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
- (b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all

information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

## **8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

## **8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union<sup>4</sup> (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

---

<sup>4</sup> The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.



## **8.9 Documentation and compliance**

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
- (c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
- (d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

## **MODULE THREE: Transfer processor to processor**

### **8.1 Instructions**

- (a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.
- (b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.
- (c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.
- (d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter<sup>5</sup>.

<sup>5</sup> See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

## **8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

## **8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

## **8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

## **8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

## **8.6 Security of processing**

- (a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing

can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

- (b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
- (c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
- (d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

## 8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

## 8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union<sup>6</sup>

---

<sup>6</sup> The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union

(in the same country as the data importer or in another third country, hereinafter “onward transfer”) if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

- (i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
- (ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;
- (iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
- (iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

## **8.9 Documentation and compliance**

- (a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.
- (b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.
- (c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.
- (d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.
- (e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.
- (f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
- (g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

---

data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

**MODULE FOUR: Transfer processor to controller****8.1 Instructions**

- (a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.
- (b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.
- (c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.
- (d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

**8.2 Security of processing**

- (a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data<sup>7</sup>, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
- (b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.
- (c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

**8.3 Documentation and compliance**

- (a) The Parties shall be able to demonstrate compliance with these Clauses.

---

<sup>7</sup> This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences.

- (b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

### Clause 9

#### *Use of sub-processors*

#### **MODULE TWO: Transfer controller to processor**

- (a) **OPTION 1: SPECIFIC PRIOR AUTHORISATION** The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

**OPTION 2: GENERAL WRITTEN AUTHORISATION** The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.<sup>8</sup> The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in

<sup>8</sup> This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

### **MODULE THREE: Transfer processor to processor**

- (a) **OPTION 1: SPECIFIC PRIOR AUTHORISATION** The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

**OPTION 2: GENERAL WRITTEN AUTHORISATION** The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

- (b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.<sup>9</sup> The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
- (c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
- (d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.
- (e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the

---

<sup>9</sup> This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.



sub-processor contract and to instruct the sub-processor to erase or return the personal data.

### *Clause 10*

### ***Data subject rights***

#### **MODULE ONE: Transfer controller to controller**

- (a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.<sup>10</sup> The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
- (b) In particular, upon request by the data subject the data importer shall, free of charge :
  - (i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
  - (ii) rectify inaccurate or incomplete data concerning the data subject;
  - (iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
- (c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
- (d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

---

<sup>10</sup> That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

- (i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
  - (ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
- (e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
- (f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
- (g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

#### **MODULE TWO: Transfer controller to processor**

- (a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
- (b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

#### **MODULE THREE: Transfer processor to processor**

- (a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
- (b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

- (c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

#### **MODULE FOUR: Transfer processor to controller**

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

#### *Clause 11*

##### **Redress**

- (a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body<sup>11</sup> at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

#### **MODULE ONE: Transfer controller to controller**

#### **MODULE TWO: Transfer controller to processor**

#### **MODULE THREE: Transfer processor to processor**

- (b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
- (c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
- (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
  - (ii) refer the dispute to the competent courts within the meaning of Clause 18.
- (d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

---

<sup>11</sup> The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

- (e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
- (f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

## *Clause 12*

### ***Liability***

#### **MODULE ONE: Transfer controller to controller**

#### **MODULE FOUR: Transfer processor to controller**

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
- (c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

#### **MODULE TWO: Transfer controller to processor**

#### **MODULE THREE: Transfer processor to processor**

- (a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
- (b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
- (c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the

data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

- (d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
- (e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
- (f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
- (g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

### *Clause 13*

### ***Supervision***

#### **MODULE ONE: Transfer controller to controller**

#### **MODULE TWO: Transfer controller to processor**

#### **MODULE THREE: Transfer processor to processor**

- (a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

- (b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries,

submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

### **SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES**

#### *Clause 14*

#### ***Local laws and practices affecting compliance with the Clauses***

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

**MODULE FOUR: Transfer processor to controller** *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

- (a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
- (b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
  - (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
  - (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards<sup>12</sup>;

<sup>12</sup> As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or

- (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.
- (c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
- (d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
- (e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]
- (f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three: , if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

### *Clause 15*

#### ***Obligations of the data importer in case of access by public authorities***

#### **MODULE ONE: Transfer controller to controller**

#### **MODULE TWO: Transfer controller to processor**

---

other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.



**MODULE THREE: Transfer processor to processor**

**MODULE FOUR: Transfer processor to controller** *(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)*

**15.1 Notification**

- (a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
  - (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

- (b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
- (c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]
- (d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.
- (e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

- (a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and

principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

- (b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]
- (c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## **SECTION IV – FINAL PROVISIONS**

### *Clause 16*

#### ***Non-compliance with the Clauses and termination***

- (a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
- (b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
- (c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
  - (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
  - (ii) the data importer is in substantial or persistent breach of these Clauses; or
  - (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

- (d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data

collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

- (e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

### *Clause 17*

#### ***Governing law***

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of \_\_\_\_\_ (*specify Member State*).]

[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of \_\_\_\_\_ (*specify Member State*).]

**MODULE FOUR: Transfer processor to controller**

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of \_\_\_\_\_ (*specify country*).

### *Clause 18*

#### ***Choice of forum and jurisdiction***

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

- (a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
- (b) The Parties agree that those shall be the courts of \_\_\_\_\_ (*specify Member State*).

- (c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
- (d) The Parties agree to submit themselves to the jurisdiction of such courts.

#### **MODULE FOUR: Transfer processor to controller**

Any dispute arising from these Clauses shall be resolved by the courts of \_\_\_\_\_ (*specify country*).

## **APPENDIX**

### EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

### **ANNEX I**

#### **A. LIST OF PARTIES**

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

**MODULE FOUR: Transfer processor to controller**

**Data exporter(s):** *[Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

2. ...

**Data importer(s):** *[Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Activities relevant to the data transferred under these Clauses: ...

Signature and date: ...

Role (controller/processor): ...

2. ...

**B. DESCRIPTION OF TRANSFER**

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

**MODULE FOUR: Transfer processor to controller**

*Categories of data subjects whose personal data is transferred*

.....

*Categories of personal data transferred*

.....

*Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.*

.....

*The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).*

.....

*Nature of the processing*

.....

*Purpose(s) of the data transfer and further processing*

.....

*The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period*

.....

*For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing*

.....

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13

.....

## **ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

**MODULE ONE: Transfer controller to controller**

**MODULE TWO: Transfer controller to processor**

**MODULE THREE: Transfer processor to processor**

### EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

*Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.*

*[Examples of possible measures:*

*Measures of pseudonymisation and encryption of personal data*

*Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services*

*Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident*

*Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing*

*Measures for user identification and authorisation*

*Measures for the protection of data during transmission*

*Measures for the protection of data during storage*

*Measures for ensuring physical security of locations at which personal data are processed*

*Measures for ensuring events logging*

*Measures for ensuring system configuration, including default configuration*

*Measures for internal IT and IT security governance and management*

*Measures for certification/assurance of processes and products*



*Measures for ensuring data minimisation*

*Measures for ensuring data quality*

*Measures for ensuring limited data retention*

*Measures for ensuring accountability*

*Measures for allowing data portability and ensuring erasure]*

*For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter*

## **ANNEX III – LIST OF SUB-PROCESSORS**

### **MODULE TWO: Transfer controller to processor**

### **MODULE THREE: Transfer processor to processor**

#### EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

1. Name: ...

Address: ...

Contact person's name, position and contact details: ...

Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): ...

2. ...



## Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018

### International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

**VERSION B1.0, in force 21 March 2022**

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

#### Part 1: Tables

**Table 1: Parties**

| Start date              |                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                          |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The Parties             | Exporter (who sends the Restricted Transfer)                                                                                                                                                                                                                             | Importer (who receives the Restricted Transfer)                                                                                                                                                                                                                          |
| <b>Parties' details</b> | Full legal name: <input type="text"/><br>Trading name (if different): <input type="text"/><br>Main address (if a company registered address): <input type="text"/><br>Official registration number (if any) (company number or similar identifier): <input type="text"/> | Full legal name: <input type="text"/><br>Trading name (if different): <input type="text"/><br>Main address (if a company registered address): <input type="text"/><br>Official registration number (if any) (company number or similar identifier): <input type="text"/> |

## International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

|                                                              |                                  |  |                                  |  |
|--------------------------------------------------------------|----------------------------------|--|----------------------------------|--|
| <b>Key Contact</b>                                           | Full Name (optional):            |  | Full Name (optional):            |  |
|                                                              | Job Title:                       |  | Job Title:                       |  |
|                                                              | Contact details including email: |  | Contact details including email: |  |
| <b>Signature (if required for the purposes of Section 2)</b> |                                  |  |                                  |  |

**Table 2: Selected SCCs, Modules and Selected Clauses**

| <b>Addendum EU SCCs</b> |                     | <input type="checkbox"/> The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information:<br>Date: <input type="text"/><br>Reference (if any): <input type="text"/><br>Other identifier (if any): <input type="text"/><br>Or<br><input type="checkbox"/> the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum: |                    |                                                          |                         |                                                                                                    |
|-------------------------|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----------------------------------------------------------|-------------------------|----------------------------------------------------------------------------------------------------|
| Module                  | Module in operation | Clause 7 (Docking Clause)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Clause 11 (Option) | Clause 9a (Prior Authorisation or General Authorisation) | Clause 9a (Time period) | Is personal data received from the Importer combined with personal data collected by the Exporter? |
| 1                       |                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                    |                                                          |                         |                                                                                                    |
| 2                       |                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                    |                                                          |                         |                                                                                                    |
| 3                       |                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                    |                                                          |                         |                                                                                                    |
| 4                       |                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                    |                                                          |                         |                                                                                                    |

**Table 3: Appendix Information**

“**Appendix Information**” means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties:

Annex 1B: Description of Transfer:

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data:

Annex III: List of Sub processors (Modules 2 and 3 only):

**Table 4: Ending this Addendum when the Approved Addendum Changes**
**Ending this Addendum when the Approved Addendum changes**

Which Parties may end this Addendum as set out in Section 19:

- ☐ Importer
- ☐ Exporter
- ☐ neither Party

**Part 2: Mandatory Clauses****Entering into this Addendum**

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.
2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

**Interpretation of this Addendum**

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

## International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

|                         |                                                                                                                                                                                                                                                    |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Addendum                | This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.                                                                                                                                    |
| Addendum EU SCCs        | The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.                                                                                                              |
| Appendix Information    | As set out in Table 3.                                                                                                                                                                                                                             |
| Appropriate Safeguards  | The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR. |
| Approved Addendum       | The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.                                                                 |
| Approved EU SCCs        | The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.                                                                                                                            |
| ICO                     | The Information Commissioner.                                                                                                                                                                                                                      |
| Restricted Transfer     | A transfer which is covered by Chapter V of the UK GDPR.                                                                                                                                                                                           |
| UK                      | The United Kingdom of Great Britain and Northern Ireland.                                                                                                                                                                                          |
| UK Data Protection Laws | All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK,                                                                                              |

## International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

|         |                                                          |
|---------|----------------------------------------------------------|
|         | including the UK GDPR and the Data Protection Act 2018.  |
| UK GDPR | As defined in section 3 of the Data Protection Act 2018. |

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.
5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.
6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.
7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.
8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

## Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.
10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.
11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

**Incorporation of and changes to the EU SCCs**

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:
  - a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;
  - b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and
  - c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.
13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.
14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.
15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:
  - a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;
  - b. In Clause 2, delete the words:

"and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";
  - c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";
  - d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";



## International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

- e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

“the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;”

- f. References to “Regulation (EU) 2016/679”, “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)” and “that Regulation” are all replaced by “UK Data Protection Laws”. References to specific Article(s) of “Regulation (EU) 2016/679” are replaced with the equivalent Article or Section of UK Data Protection Laws;

- g. References to Regulation (EU) 2018/1725 are removed;

- h. References to the “European Union”, “Union”, “EU”, “EU Member State”, “Member State” and “EU or Member State” are all replaced with the “UK”;

- i. The reference to “Clause 12(c)(i)” at Clause 10(b)(i) of Module one, is replaced with “Clause 11(c)(i)”;

- j. Clause 13(a) and Part C of Annex I are not used;

- k. The “competent supervisory authority” and “supervisory authority” are both replaced with the “Information Commissioner”;

- l. In Clause 16(e), subsection (i) is replaced with:

“the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;”;

- m. Clause 17 is replaced with:

“These Clauses are governed by the laws of England and Wales.”;

- n. Clause 18 is replaced with:

“Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts.”; and

- o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

**Amendments to this Addendum**

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.
17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.
18. From time to time, the ICO may issue a revised Approved Addendum which:
  - a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
  - b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:
  - a its direct costs of performing its obligations under the Addendum; and/or
  - b its risk under the Addendum,and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.
20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

|                          |                                                                                                                                                                                                                                                                               |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Mandatory Clauses</b> | Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses. |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

# DATA PROCESSING AGREEMENT

This Data Processing Agreement (“**DPA**”) is subject to and forms part of your [Stripe Services Agreement](#) and governs Stripe’s and its Affiliates’ Processing of Personal Data.

1. **Structure.** If your Stripe Account is located in North America or South America, you enter this DPA with Stripe, Inc. (“**SINC**”). If your Stripe Account is located elsewhere, you enter this DPA with Stripe Payments Europe, Limited (“**SPEL**”). Accordingly, references in this DPA to “**Stripe**” mean SINC or SPEL, as applicable. If your [Stripe Services Agreement](#) is with an SSA Affiliate, Stripe may engage that SSA Affiliate to Process Personal Data according to this DPA.

2. **Definitions.** Capitalized terms not defined in this DPA have the meanings given to them in your [Stripe Services Agreement](#).

“**Approved Data Transfer Mechanism**” means, as applicable, the EEA SCCs, the UK Data Transfer Addendum or any data transfer mechanism a supervisory authority approves under DP Law that is incorporated into this DPA.

“**Authorized Services**” means Services that a Governmental Authority licenses, authorizes or regulates.

“**CCPA**” means the California Consumer Privacy Act of 2018, Cal. Civ. Code Sections 1798.100-1798.199.

“**DP Law**” means all Law that applies to Personal Data Processing under your [Stripe Services Agreement](#) and this DPA, including international, federal, state, provincial and local Law relating to privacy, data protection or data security.

“**Data Controller**” means the entity which, alone or jointly with others, determines the purposes and means of Processing Personal Data, which may include, as applicable, a “Business” as defined under the CCPA.

“**Data Processor**” means the entity that Processes Personal Data on behalf of the Data Controller, which may include, as applicable, a “Service Provider” as defined under the CCPA.

“**Data Security Measures**” means technical and organizational measures that are intended to secure Personal Data to a level of security appropriate for the risk of the Processing.

“**Data Subject**” means an identified or identifiable natural person to which Personal Data relates.

“**EEA**” means the European Economic Area.

“**EEA SCCs**” mean Module 2 (Transfer: Controller to Processor) of the standard contractual clauses set out in the European Commission Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries according to the GDPR.

“**GDPR**” means the General Data Protection Regulation (EU) 2016/679.

“**Instructions**” means this DPA and any further written agreement or documentation under which the Data Controller instructs a Data Processor to perform specific Processing of Personal Data for that Data Controller.

“**Joint Controller**” means a Data Controller that jointly determines the purposes and means of Processing Personal Data with one or more Data Controllers.

“**Personal Data**” means any information relating to an identified or identifiable natural person that is Processed in connection with the Services, and includes “personal data” as defined under the GDPR and “personal information” as defined under the CCPA.

**“Process”** means to perform any operation or set of operations on Personal Data or sets of Personal Data, such as collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing by transmission, disseminating or otherwise making available, aligning or combining, restricting, erasing or destroying, as described under DP Law.

**“Sensitive Data”** means (a) Personal Data that is genetic data, biometric data, data concerning health, a natural person's sex life or sexual orientation; or (b) data about racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, to the extent this data is treated distinctly as a special category of Personal Data under DP Law.

**“SSA Affiliate”** means an Affiliate of Stripe that acts as (a) a Joint Controller with Stripe in relation to Authorized Services; or (b) a Data Processor on behalf of Stripe in relation to Services other than Authorized Services.

**“Sub-processor”** means an entity a Data Processor engages to Process Personal Data on that Data Processor's behalf in connection with the Services.

**“UK Data Transfer Addendum”** means the international data transfer addendum to the EEA SCCs issued by the United Kingdom's Information Commissioner's Office.

**“UK GDPR”** means the GDPR, as transposed into United Kingdom national law by operation of section 3 of the European Union (Withdrawal) Act 2018 and as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.

### 3. **Stripe as Data Processor and Data Controller.**

3.1. Data Processing Roles. To the extent Stripe Processes Personal Data as a:

- (a) Data Processor, it is acting as a Data Processor on behalf of you, the Data Controller; and
- (b) Data Controller, it has the sole and exclusive authority to determine the purposes and means of Processing Personal Data it receives from or through you.

3.2. Categories of Data Subjects and Personal Data.

- (a) *Data Subjects.* Stripe may Process the Personal Data of your Customers, representatives and any natural persons who access or use your Stripe Account.
- (b) *Personal Data.* Where applicable, Stripe may Process Payment Account Details, bank account details, billing/shipping address, name, date/time/amount of transaction, device ID, email address, IP address/location, order ID, payment card details, tax ID/status, unique customer identifier, identity information including government issued documents (e.g., national IDs, driver's licenses and passports).
- (c) *Sensitive Data.* Where applicable, Stripe may Process facial recognition data.

3.3. Data Processing Purposes.

- (a) The purposes of Stripe's Processing of Personal Data are when Stripe is operating in its capacity as a Data Processor for a Service, including:
  - (i) servicing the Stripe platform; and
  - (ii) facilitating payment transactions on behalf of Stripe users.

- (b) The purposes of Stripe's Processing of Personal Data in its capacity as a Data Controller are:
  - (i) determining the Processing of Personal Data when providing Stripe products and services, including when Stripe provides a payment method, and determining the third parties (banks and payment method providers) to be utilized;
  - (ii) monitoring, preventing and detecting fraudulent transactions and other fraudulent activity on the Stripe platform;
  - (iii) complying with Law, including applicable anti-money laundering screening and know-your-customer obligations; and
  - (iv) analyzing and developing Stripe's services.

#### 4. **Stripe Obligations when Acting as a Data Processor.**

4.1. **Obligations.** To the extent that Stripe is acting as a Data Processor for you, Stripe will:

- (a) Process Personal Data on behalf of and according to your Instructions. Stripe will not sell, retain, use or disclose Personal Data for any purpose other than for the specific purposes of performing the Services and to comply with Law, unless otherwise permitted by your [Stripe Services Agreement](#) (including this DPA) or DP Law. Stripe will inform you if, in its opinion, Instructions violate or infringe DP Law;
- (b) ensure that all persons Stripe authorizes to Process Personal Data in the context of the Services are granted access to Personal Data on a need-to-know basis and are committed to respecting the confidentiality of Personal Data;
- (c) to the extent required by DP Law, inform you of requests Stripe receives from Data Subjects (including "verifiable consumer requests" as defined under the CCPA) exercising their applicable rights under DP Law to (i) access (e.g., right to know under the CCPA) their Personal Data; (ii) have their Personal Data corrected or erased; (iii) restrict or object to Stripe's Processing; or (iv) data portability. Other than to request further information, identify the Data Subject, and, if applicable, direct the Data Subject to you as Data Controller, Stripe will not respond to these requests unless you instruct Stripe in writing to do so;
- (d) to the extent required by DP Law, inform you of each law enforcement request Stripe receives from a Governmental Authority requiring Stripe to disclose Personal Data or participate in an investigation involving Personal Data;
- (e) to the extent required by DP Law, provide you with reasonable assistance through appropriate technical and organizational measures, at your expense, to assist you in complying with your obligations under DP Law, which assistance may include conducting data protection impact assessments and consulting with a supervisory authority, taking into account the nature of the Processing and the information available to Stripe;
- (f) implement and maintain a written information security program with the Data Security Measures stated in [Exhibit 1](#) of this DPA. In addition, Stripe will implement a data security incident management program that addresses how Stripe will manage a data security incident involving the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of, or access to, Personal Data ("**Incident**"). If Stripe is required by DP Law to notify you of an Incident, then Stripe will notify you without unreasonable delay, but in no event later than any time period required by DP Law. In

addition, for Incidents affecting Personal Data subject to GDPR or UK GDPR, Stripe will notify you no later than 48 hours after Stripe becomes aware of the Incident. Stripe will partner with you to respond to the Incident. The response may include identifying key partners, investigating the Incident, providing regular updates, and discussing notice obligations. Except as required by DP Law, Stripe will not notify your affected Data Subjects about an Incident without first consulting you;

- (g) engage Sub-processors as necessary to perform the Services on the basis of the general written authorization you give to Stripe under [Section 4.2](#) of this DPA;
- (h) to the extent required by DP Law and upon your written request, contribute to audits or inspections by making audit reports available to you, which reports are Stripe's confidential information. Upon your written request, and no more frequently than once annually, Stripe will promptly provide documentation or complete a written data security questionnaire of reasonable scope and duration regarding Stripe's and its Affiliates' Processing of Personal Data. All documentation provided, including any response to a security questionnaire, is Stripe's confidential information; and
- (i) at your choice, and subject to Stripe's rights and obligations under your [Stripe Services Agreement](#) (including this DPA), delete or return all Personal Data to you after the Term, and delete existing copies held by Stripe, unless Stripe is required or authorized by DP Law to store Personal Data for a longer period.

#### 4.2 Sub-processors.

- (a) You specifically authorize Stripe to engage its Sub-processors and Affiliates from the agreed lists of Sub-processors and Affiliates at [stripe.com/service-providers/legal](https://stripe.com/service-providers/legal) ("**Stripe Service Providers List**"). If you subscribe to email notifications at the Stripe Service Providers List, then Stripe will notify you via email of any changes Stripe intends to make to the Stripe Service Providers List at least 30 days before the changes take effect. You may reasonably object to a change on legitimate grounds within 30 days after you receive notice of the change. You acknowledge that Stripe's Sub-processors are essential to provide the Services and that if you object to Stripe's use of a Sub-processor, then notwithstanding anything to the contrary in your [Stripe Services Agreement](#) (including this DPA), Stripe will not be obligated to provide you the Services for which Stripe uses that Sub-processor.
- (b) Stripe will enter into a written agreement with each Sub-processor that imposes on that Sub-processor obligations comparable to those imposed on Stripe under this DPA, including implementing appropriate Data Security Measures. If a Sub-processor fails to fulfill its data protection obligations under that agreement, Stripe will remain liable to you for the acts and omissions of its Sub-processor to the same extent Stripe would be liable if performing the relevant Services directly under this DPA.

4.3 CCPA Certification. To the extent applicable to the Services, Stripe certifies that it understands and will comply with the requirements in this DPA relating to the CCPA.

4.4 **Disclaimer of Liability. Notwithstanding anything to the contrary in your [Stripe Services Agreement](#) or this DPA, Stripe and its Affiliates will not be liable for any claim made by a Data Subject arising from or related to Stripe's or any of its Affiliates' acts or omissions, to the extent that Stripe was acting in accordance with your Instructions.**

#### 5. **Your obligations when acting as a Data Controller.** You must:

- 5.1 only provide Instructions to Stripe that are lawful;
- 5.2 comply with and perform your obligations under DP Law, including with regard to Data Subject rights, data security and confidentiality, and ensure you have an appropriate legal

basis for the Processing of Personal Data as described in your [Stripe Services Agreement](#), including this DPA; and

- 5.3 provide Data Subjects with all necessary information (including by means of offering a transparent and easily accessible public privacy notice) regarding, respectively, Stripe's and your Processing of Personal Data for the purposes described in your [Stripe Services Agreement](#), including this DPA.

## 6. Data transfers.

- 6.1 General. Stripe and its Affiliates may transfer Personal Data on a global basis as necessary to provide the Services. In particular, Stripe and its Affiliates may transfer Personal Data to SINC in the United States and to Stripe's Affiliates and Sub-processors in other jurisdictions. Where Stripe transfers Personal Data under this DPA to a country or recipient not recognised as having an adequate level of protection for Personal Data according to DP Law, Stripe will comply with its obligations under DP Law.
- 6.2 Transfers from the EEA to SINC. The EEA SCCs apply to a transfer from the EEA of Personal Data Processed under this DPA between you and SINC and are incorporated into this DPA. You agree that the EEA SCCs are completed and supplemented as follows:
- (a) you are the data exporter and SINC is the data importer;
  - (b) the optional docking clause under [Clause 7](#) of the EEA SCCs will not apply;
  - (c) option 2 under [Clause 9](#) of the EEA SCCs applies and you generally authorize SINC to engage Sub-processors according to [Section 4.2](#) of this DPA;
  - (d) the optional redress language under [Clause 11\(a\)](#) of the EEA SCCs will not apply;
  - (e) the governing law under [Clause 17](#) of the EEA SCCs will be Ireland;
  - (f) the choice of forum and jurisdiction under [Clause 18](#) of the EEA SCCs will be the courts of Ireland;
  - (g) [Annexes I, II and III](#) of the EEA SCCs are deemed to be populated with the information set out in [Exhibits 1 and 2](#) of this DPA; and
  - (h) [Annex IV of Exhibit 2](#) of this DPA supplements the EEA SCCs with additional clauses.
- 6.3 2010 SCCs. For the purposes of a transfer of Personal Data from the EEA, Switzerland or the United Kingdom, any reference to the standard contractual clauses adopted under Directive 95/46/EC ("**2010 SCCs**") in an agreement you have entered into with Stripe or its Affiliates will be construed as a reference to the Approved Data Transfer Mechanism. The 2010 SCCs are terminated and replaced by the Approved Data Transfer Mechanism. Any Personal Data transferred under the 2010 SCCs will not be returned or destroyed due to the termination of the 2010 SCCs and instead will become subject to the Approved Data Transfer Mechanism.
- 6.4 Transfers from the United Kingdom to SINC. The UK Data Transfer Addendum applies to a transfer from the United Kingdom of Personal Data Processed under this DPA between you and SINC and is incorporated into this DPA. You agree that the UK Data Transfer Addendum is completed and supplemented as follows:
- (a) you are the data exporter and SINC is the data importer;
  - (b) Table 1 of the UK Data Transfer Addendum is deemed to be populated with the information set out in [Annex IA of Exhibit 2](#) of this DPA;
  - (c) for the purposes of Table 2 of the UK Data Transfer Addendum, the version of the "Approved EU SCCs" (including the appendix information, modules and selected clauses) appended to the UK Data Transfer Addendum is the EEA SCCs;
  - (d) the optional docking clause under [Clause 7](#) of the EEA SCCs will not apply;
  - (e) option 2 under [Clause 9](#) of the EEA SCCs applies and you generally authorize SINC to engage Sub-processors according to [Section 4.2](#) of this DPA;
  - (f) the optional redress language under [Clause 11\(a\)](#) of the EEA SCCs will not apply;



- (g) Annex IV of Exhibit 2 of this DPA supplements the EEA SCCs with additional clauses;
- (h) Table 3 of the UK Data Transfer Addendum is deemed to be populated with the information set out in Exhibits 1 and 2 of this DPA;
- (i) the “importer” and “exporter” option applies for the purposes of Table 4 of the UK Data Transfer Addendum;
- (j) under Part 2, the mandatory clauses of the UK Data Transfer Addendum will apply; and
- (k) by using the Services to transfer Personal Data to SINC, you will be deemed to have signed the UK Data Transfer Addendum.

6.5 Transfers from other countries or regions. The terms applicable to the transfer of Personal Data processed under this DPA from any country or territory listed in Exhibit 3 of this DPA, including any Approved Data Transfer Mechanism, are incorporated into this DPA.

**7. Conflict.** If there is any conflict or ambiguity between:

- 7.1 the provisions of this DPA and the provisions of your [Stripe Services Agreement](#) regarding Personal Data Processing, the provisions of this DPA will prevail; and
- 7.2 the provisions of this DPA and any provision contained in an Approved Data Transfer Mechanism and executed by you and SINC, the provisions of the Approved Data Transfer Mechanism will prevail.

## EXHIBIT 1: STRIPE DATA SECURITY

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Security Programs and Policies</b>    | <p>Stripe maintains and enforces a security program that addresses how Stripe manages security, including the security controls Stripe employs. The security program includes:</p> <ul style="list-style-type: none"> <li>• documented policies that Stripe formally approves, internally publishes, communicates to appropriate personnel and reviews at least annually;</li> <li>• documented, clear assignment of responsibility and authority for security program activities;</li> <li>• policies covering, as applicable, acceptable computer use, data classification, cryptographic controls, access control, removable media and remote access; and</li> <li>• regular testing of the key controls, systems and procedures.</li> </ul> <p><b>Privacy Program.</b> Stripe maintains and enforces a privacy program and related policies that address how Personal Data is collected, used and shared.</p>                                                                            |
| <b>Risk and Asset Management</b>         | <p>Stripe performs risk assessments, and implements and maintains controls for risk identification, analysis, monitoring, reporting and corrective action.</p> <p>Stripe maintains and enforces an asset management program that appropriately classifies and controls hardware and software assets throughout their life cycle.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Personnel Education and Controls</b>  | <p>All (a) Stripe employees; and (b) Stripe independent contractors who may have access to data, including those who Process Personal Data ((a) and (b), collectively “<b>Personnel</b>”) acknowledge their data security and privacy responsibilities under Stripe’s policies.</p> <p>For Personnel, Stripe, either itself or through a third party:</p> <ul style="list-style-type: none"> <li>• implements pre-employment background checks and screening;</li> <li>• conducts security and privacy training;</li> <li>• implements disciplinary processes for violations of data security or privacy requirements; and</li> <li>• upon termination or applicable role change, promptly removes or updates Worker access rights and requires the Worker to return or destroy Personal Data.</li> </ul> <p><b>Authentication.</b> Stripe authenticates each Personnel’s identity through appropriate authentication credentials such as strong passwords, token devices or biometrics.</p> |
| <b>Training and Awareness</b>            | <p><b>Annual Security and Privacy Training.</b> Stripe’s employees complete an annual Security and Privacy awareness training on Stripe’s data security and confidentiality policies and practices.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Network and Operations Management</b> | <p><b>Policies and Procedures.</b> Stripe implements policies and procedures for network and operations management. These policies and procedures address hardening, change control, segregation of duties, separation of development and production environments, technical architecture management, network security, malware protection, protection of data in transit and at rest, data integrity, encryption, audit logs and network segregation.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                         | <p><b>Vulnerability Assessments.</b> Stripe performs periodic vulnerability assessments and penetration testing on its systems and applications, including those that Process Personal Data.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <p><b>Technical Access Controls</b></p> | <p><b>Access control.</b> Stripe implements measures to prevent data processing systems from being used by unauthorized persons, including the following measures:</p> <ul style="list-style-type: none"> <li>• user identification and authentication procedures;</li> <li>• ID/password security procedures (special characters, minimum length, change of password), including stronger digital authentication measures based on NIST 800-63B;</li> <li>• automatic blocking (e.g., password or timeout); and</li> <li>• break-in-attempt monitoring.</li> </ul> <p><b>Data access control.</b> Stripe implements measures to ensure that persons entitled to use a data processing system gain access only to the Personal Data allowed for their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, including:</p> <ul style="list-style-type: none"> <li>• internal policies and procedures;</li> <li>• control authorization schemes;</li> <li>• differentiated access rights (profiles, roles, actions and objects);</li> <li>• access monitoring and logging;</li> <li>• access reports;</li> <li>• access procedure;</li> <li>• change procedure; and</li> <li>• deletion procedure.</li> </ul>                                                         |
| <p><b>Physical access controls</b></p>  | <p>Stripe uses reputable third-party service providers to host its production infrastructure. Stripe relies on these third parties to manage the physical access controls to the data center facilities that they manage. Some of the measures that Stripe's service providers provide to prevent unauthorized persons from gaining physical access to the data processing systems available at premises and facilities (including databases, application servers and related hardware), where Personal Data is Processed, include:</p> <ul style="list-style-type: none"> <li>• physical access control system and program in place at Stripe premises;</li> <li>• 24x7 Global Security Operation Center that monitors physical security systems;</li> <li>• security video and alarm systems;</li> <li>• access control roles and area zones;</li> <li>• access control audit measures;</li> <li>• electronic tracking and management program for keys;</li> <li>• access authorisations process for employees and third parties;</li> <li>• door locking (electrified locks etc.); and</li> <li>• trained uniformed security staff.</li> </ul> <p>Stripe reviews third-party audit reports to verify that Stripe's service providers maintain appropriate physical access controls for the managed data centers.</p> |

|                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Availability Controls</b>      | <p>Stripe implements measures to ensure the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, including:</p> <ul style="list-style-type: none"> <li>• database replication;</li> <li>• backup procedures;</li> <li>• hardware redundancy; and</li> <li>• a disaster recovery plan.</li> </ul>                                                                                                                                                                                                                                                |
| <b>Disclosure Controls</b>        | <p>Stripe implements measures to ensure that Personal Data (a) cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic); and (b) can be verified to which companies or other legal entities Personal Data are disclosed, including logging, transport security and encryption.</p>                                                                                                                                                                                                                                        |
| <b>Entry Controls</b>             | <p>Stripe implements measures to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, including logging and reporting systems, and audit trails and documentation.</p>                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Separation Controls</b>        | <p>Stripe implements measures to ensure that Personal Data collected for different purposes can be Processed separately, including:</p> <ul style="list-style-type: none"> <li>• “least privilege” limitation of access to data by internal service;</li> <li>• segregation of functions (production/testing);</li> <li>• procedures for storage, amendment, deletion, transmission of data for different purposes; and</li> <li>• logical segmentation processes to manage the separation of Personal Data.</li> </ul>                                                                                                         |
| <b>Certifications and Reports</b> | <p><b>PCI Compliance.</b> To the extent applicable to the Services, Stripe will provide the Services in a manner that is consistent with the highest certification level (PCI Level 1) provided by the PCI-DSS requirements. Stripe’s certification is confirmed annually by a qualified security assessor (QSA).</p> <p><b>SOC Reports.</b> Stripe maintains Service Organization Controls (“<b>SOC</b>”) auditing standards for service organizations issued under the AICPA. SOC 1 and 2 reports are produced annually and will be provided upon request.</p> <p>Stripe may add standards or certifications at any time.</p> |
| <b>Encryption</b>                 | <p>Stripe applies data encryption mechanisms at multiple points in Stripe’s service to mitigate the risk of unauthorized access to Stripe data at rest and in transit. Access to Stripe cryptographic key materials is restricted to a limited number of authorized Stripe personnel.</p> <p><b>Encryption in transit.</b> To protect data in transit, Stripe requires all inbound and outbound data connections to be encrypted using the TLS 1.2 protocol. For data traversing Stripe’s internal production networks, Stripe uses mTLS to encrypt connections between production systems.</p>                                 |

|                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                           | <p><b>Encryption at rest.</b> To protect data at rest, Stripe uses industry standard encryption (AES 256) to encrypt all production data stored in server infrastructure.</p> <p><b>Payment Card and Banking Account Data Tokenization.</b> Payment card and bank numbers are separately encrypted using industry standard encryption (AES-256) at the data level and stored in a separate data vault that is highly restricted. Decryption keys are stored on separate machines. Tokens are generated to support Stripe data processing.</p>                                                                                                                            |
| <b>Data Security Incident Management and Notification</b> | <p>Stripe implements a data security incident management program that addresses how Stripe manages Incidents.</p> <p>Stripe will notify impacted Stripe users and Governmental Authorities (where applicable) of Incidents in a timely manner as required by DP Law.</p>                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Reviews, Audit Reports and Security Questionnaires</b> | <p>Upon written request, and no more frequently than annually, Stripe will complete a written data security questionnaire of reasonable scope and duration regarding Stripe's business practices and data technology environment in relation to the Processing of Personal Data. Stripe's responses to the security questionnaire are Stripe's confidential data.</p>                                                                                                                                                                                                                                                                                                    |
| <b>System Configuration</b>                               | <p>Stripe implements measures for ensuring system configuration, including default configuration measures for internal IT and IT security governance.</p> <p>Stripe relies on deployment automation tools to deploy infrastructure and system configuration. These automation tools leverage infrastructure configurations that are managed through code that flows through Stripe's change control processes. Stripe's change management processes require formal code reviews and two-party approvals prior to the release to production.</p> <p>Stripe uses monitoring tools to monitor production infrastructure for changes from known configuration baselines.</p> |
| <b>Data Portability</b>                                   | <p>The Stripe API enables Stripe users to programmatically access the data stored for transfer, excluding PCI-scoped data. The portability process for PCI data to other PCI-DSS Level 1 compliant payment processors can be found at <a href="https://stripe.com/docs/security/data-migrations/exports">https://stripe.com/docs/security/data-migrations/exports</a>.</p>                                                                                                                                                                                                                                                                                               |
| <b>Data Retention and Deletion</b>                        | <p>Stripe implements and maintains data retention policies and procedures related to Personal Data and reviews these policies and procedures as appropriate.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

## EXHIBIT 2: APPROVED DATA TRANSFER MECHANISM: DESCRIPTION OF PROCESSING AND TRANSFER

### ANNEX I

#### A. LIST OF PARTIES

##### Data exporter(s):

**Name:** The party to the [Stripe Services Agreement](#) with Stripe or its Affiliate (as applicable).

**Address:** The data exporter's address.

**Contact person's name, position and contact details:** The name, position and contact details provided by the data exporter.

**Activities relevant to the data transferred under these Clauses:** Processing Personal Data in connection with the data exporter's use of the Services under the [Stripe Services Agreement](#).

**Role (controller/processor):** Controller

**Signature and date:** By using the Services to transfer Personal Data to the data importer, the data exporter will be deemed to have signed this Annex I.

##### Data importer:

**Name:** Stripe, Inc.

**Registered office:** Corporation Trust Center, 1209 Orange Street, Wilmington, New Castle, DE 19801, USA

**Contact details:** Stripe Privacy Team, [privacy@stripe.com](mailto:privacy@stripe.com)

**Activities relevant to the data transferred under these Clauses:** Processing Personal Data in connection with the data exporter's use of the Services under the [Stripe Services Agreement](#).

**Role (controller/processor):** Processor

**Signature and date:** The data importer will be deemed to have signed this Annex I on the transfer of Personal Data by the data exporter in connection with the Services.

#### B. DESCRIPTION OF TRANSFER

##### *Categories of data subjects whose personal data is transferred*

The Personal Data transferred concern the following categories of Data Subjects or consumers:

- Users of the data importer's online and mobile services.

- The data exporter's end customers, donors, representatives and any natural person who accesses or uses your Stripe Account.

### ***Categories of personal data transferred***

The categories of Personal Data transferred are described in [Section 3](#) of the DPA.

***Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.***

The categories of Personal Data transferred are described in [Section 3](#) of the DPA.

***The frequency of the transfer (whether the data is transferred on a one-off or continuous basis).***

The frequency of the transfer is a continuous basis for the duration of the [Stripe Services Agreement](#) until the Personal Data is deleted in accordance with [Section 4.1\(i\)](#) of the DPA.

### ***Nature of the processing***

The nature of the processing is described in [Section 3](#) of the DPA.

### ***Purpose(s) of the data transfer and further processing***

The purposes of the data transfer are described in [Section 3](#) of the DPA.

***The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period***

The period for which the personal data will be retained is set out in [Section 4.1\(i\)](#) of the DPA.

***For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing***

The subject matter and nature of the processing related to transfers to Sub-processors is set out at Annex III to these clauses. Subject to [Section 4.1\(i\)](#) of the DPA, the duration of the processing is the duration of the [Stripe Services Agreement](#).

## **C. COMPETENT SUPERVISORY AUTHORITY**

The competent supervisory authority in accordance with [Clause 13](#) of the EEA SCCs is the Irish Data Protection Commission.

## **ANNEX II**

### **TECHNICAL AND ORGANIZATIONAL MEASURES INCLUDING TECHNICAL AND ORGANIZATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

The data importer will maintain and implement the technical and organizational measures set out in Exhibit 1 of the DPA.

### **ANNEX III**

#### **LIST OF SUB-PROCESSORS**

The controller has generally authorized the engagement of the Sub-processors at <https://stripe.com/service-providers/legal>.

### **ANNEX IV**

#### **SUPPLEMENTAL CLAUSES**

In addition to the obligations under the EEA SCCs and the UK Data Transfer Addendum (as applicable), the parties agree to the following supplementary measures:

1. Personal Data will be encrypted both in transit and at rest using encryption technology by the data importer.
2. the data importer will resist, to the extent permitted by Law, any request under Section 702 of Foreign Intelligence Surveillance Act (“**FISA**”).
3. the data importer will use reasonably available legal mechanisms to challenge any demands for data access through the national security process that it may receive in relation to data exporter’s data.
4. no later than the date on which the data exporter’s acceptance of the DPA and the Approved Data Transfer Mechanism that incorporates or references this Annex becomes effective, the data importer will notify the data exporter of any binding legal demand for the Personal Data it has received, including national security orders and directives, which will encompass any process issued under Section 702 of FISA, unless prohibited under Law.
5. the data importer will ensure that Stripe’s data protection officer has oversight of Stripe’s approach to international data transfers.

This Annex also sets out the parties’ interpretation of their respective obligations under the specific terms of the EEA SCCs (as amended or supplemented by an Approved Data Transfer Mechanism). Where a party complies with the interpretations set out in this Annex, that party will be deemed by the other party to have complied with its commitments under the EEA SCCs.

#### **6. Clause 8.1(a): Instructions**

The DPA and the [Stripe Services Agreement](#) are the data exporter’s complete and final instructions at the time of execution of the DPA for the Processing of Personal Data. Any additional or alternate instructions must be agreed upon separately in writing by the parties. For the purposes of Clause 8.1(a) of the EEA SCCs, the Processing described in the DPA is deemed an instruction by the data exporter to Process Personal Data.

#### **7. Clause 9(c): Copies of Sub-processor Agreements**

The parties agree that, following a request by the data exporter, the data importer will provide copies of the Sub-processor agreements that must be provided to the data exporter pursuant to Clause 9(c) of the EEA SCCs, provided that the data importer may (i) redact or remove all



commercial information, or clauses unrelated to the EEA SCCs or their equivalent and (ii) determine the manner in which to provide the copy agreements to the data exporter.

**8. Clause 8.9(k) and (l): Audit**

The data exporter acknowledges and agrees that it exercises its audit right under Clause 8.9(k) and (l) of the EEA SCCs by instructing the data importer to comply with the audit measures described in Section 4.1(h) of the DPA.

**9. Additional commercial clause**

The EEA SCCs are incorporated into the Stripe Services Agreement. As between the data exporter, and the data importer and its Affiliates, to the greatest extent permitted by Law, the limitations and exclusions of liability set out in the Stripe Services Agreement will apply to the EEA SCCs.

**10. Defined terms**

Capitalized terms not defined in these Annexes have the meanings given to them in the Stripe Services Agreement, including the DPA.

## EXHIBIT 3: JURISDICTION SPECIFIC TERMS AND APPROVED DATA TRANSFER MECHANISMS

### SWITZERLAND

The EEA SCCs in the form described in Section 6.2 of the DPA and as adapted and supplemented as described in this Exhibit 3, will only apply to a transfer of Personal Data Processed under this DPA from Switzerland to SINC. For these purposes, you agree that:

1. any reference to “Member State” will not be interpreted in such a way as to exclude data subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland);
2. any references to “personal data” extend to personal data of legal entities if and to the extent such personal data pertaining to legal entities is within the scope of the Swiss Federal Act on Data Protection ("**FADP**"); and
3. to the extent the transfer of personal data is governed by the FADP, the Swiss Federal Data Protection and Information Commissioner will act as the competent supervisory authority; to the extent the transfer of personal data is governed by the GDPR, the supervisory authority determined in Annex IC will act as the competent supervisory authority; any references to the "competent supervisory authority" will be interpreted accordingly.

# Privacy statement

# Adyen

August 2025

Please read this privacy statement if you would like to know more about the way Adyen and its group companies around the world (hereinafter referred to as “Adyen” or “we”) collect and process your personal data. This privacy statement applies to the processing activities in which Adyen acts as a data controller.

It is important to us that your personal data is handled carefully, and that you are well informed about the way we process your personal data. This privacy statement tells you what data we process – including how, why and how long we process it for – and informs you of your data privacy rights.

Adyen reserves the right to update its privacy statement at any time. Such updates will be made and posted on our publicly available website <https://www.adyen.com/privacy-policy>.

Version as of August, 2025.

Hi there,

We have updated our Privacy Statement as of August 2025. To read the previous (Sept 2024) version, please click [here](#).

## Who is Adyen?

Adyen is a financial technology company operating under a banking license in multiple regions. This means that Adyen provides its customers with payments and other financial products, including payments processing for its customers and platforms via credit card, bank transfer, and other payment methods, card issuing, (merchant) bank accounts, fraud detection, and other financial services. It is also important to note that Adyen N.V. is supervised by the Dutch Central Bank as a regulated bank under Dutch law. In addition, Adyen and its group companies are supervised by various regulators and authorities, as applicable, around the globe.

You may have seen Adyen on your bank statements if you have bought something, automatically renewed a subscription, or received a payout from one of Adyen's customers. If you would like more information about any of these charges, you can use [Adyen's Look Up Charge Tool](#).

## Your individual rights

If you would like to exercise your **data subject rights** (outlined below) under data privacy law, please use [Adyen's Privacy Form](#).

You may have the following rights regarding your personal data, subject to certain exceptions:

- **Right to access:** You may have the right to ask us for the specific personal data that we have collected from you in a portable and (where technically possible) usable format.
- **Right to know:** You may have the right to verify that we have collected personal data about you, as well as know what personal data we have collected about you. This includes, as applicable, the categories of personal data we have collected, the sources from which we collected that personal data, the business or commercial purposes for which we collected, "sold", and "shared" that personal data, the categories of personal data that we "sold", "shared", or disclosed to third parties for business purposes and the categories of third parties to whom we "sold", "shared", or disclosed personal data. You can also contact us if you want to know more about the data we process for our legitimate interests.

- **Right to deletion:** You may be entitled to request that we delete the personal data that we have collected from you. We will use all commercially reasonable efforts to honor your request, in compliance with applicable laws. Please note, however, that we may need or be required to keep such information, such as for our legitimate business purposes, or to comply with applicable laws.
- **Right to opt-out of sales and sharing of personal data to third parties for cross-context behavioral advertising:** You are entitled to opt-out of sales of your personal data to third parties and to opt-out of the sharing of your personal data to third parties for cross-context behavioral advertising, if applicable. You can opt-out of sales and sharing of your personal data by visiting our Cookies Policy and disabling the 'Sale or Share of Personal Data' toggle in the Cookies Preference Center, or by contacting us using one of the methods below. If you have enabled the Global Privacy Control mechanism on your browser, device, or platform, you will automatically be opted out of any "sharing" when you use our website. Adyen seamlessly processes the Global Privacy Control (GPC) signal if enabled on your browser, device, or platform. Please visit [this page](#) to learn more about enabling the GPC.
- **Right to object to the processing of your personal data:** You are entitled to object to us processing your personal data. In addition, where you have given your consent for us to process personal data, you can withdraw this consent at any time. Please note that Adyen maintains a record of withdrawals of consent to ensure that we do not contact you in the future.
- **Right to opt-out of profiling:** As defined under privacy laws, Adyen may profile customers to determine their eligibility for certain financial products, or to offer them certain financial services. Please note that opting-out of profiling will mean that you are no longer eligible for these financial products or services.
- **Right to correct your personal data:** You may have the right to update inaccurate information that we process about you.

- **Right to exercise rights without discrimination:** You have the right not to receive discriminatory treatment if you exercise the rights conferred to you by applicable privacy laws.

These rights may be limited under applicable laws, and are also subject to technical feasibility. For example, if we collect your personal data in our role as a service provider to one of our customers, you will need to contact that customer directly to exercise your rights.

Please note that we may require additional information from you to verify your identity and process your request. Alternatively, you can submit a request through an authorized representative using the contact methods described below. If you use an authorized representative, we may require a copy of their signed permission to act on your behalf. We may also need to verify your identity directly and ask you to confirm the representative's authority.

To exercise your rights, your information will be disclosed to our privacy management third-party service provider. Please be informed that Adyen has implemented the appropriate safeguards to ensure your information is adequately protected.

## Contact us

Questions, comments, requests, or complaints concerning this privacy statement or the way we process your personal data are welcomed and can be addressed to our Data Protection Officer at [dpo@adyen.com](mailto:dpo@adyen.com) or Simon Carmiggeltstraat 5-60, 1011 DJ Amsterdam, the Netherlands, or to [lgpd@adyen.com](mailto:lgpd@adyen.com) if you are located in Brazil.

If you would like further details on any of the third parties your personal data is “sold” to or “shared” with, would like to know the purpose of their data processing, the manner in which data is processed, or how you can communicate with such third party to exercise your data privacy rights, please contact [dpo@adyen.com](mailto:dpo@adyen.com), or [lgpd@adyen.com](mailto:lgpd@adyen.com) if you are located in Brazil.

If you have a complaint about the way we handle your personal data, you also have the right to address this to the data protection authority of the country in which you live or work, or the country in which we are located.

## **Transfer of information**

Some of the information you send us may be disclosed to other Adyen group companies outside of the European Economic Area ("EEA"). These countries encompass the countries in which we have operations (you can find a full list [here](#)).

If you are a resident in Quebec, your information may be disclosed to Adyen group companies outside of Quebec.

To protect your data when it is transferred to countries outside of the EEA, we have implemented appropriate safeguards. When we transfer data to our Adyen group companies, the transfers are protected by an intragroup agreement containing Standard Contractual Clauses. For transfers to our services providers located outside of the EEA, we rely on Standard Contractual Clauses. If you would like to know more about these safeguards, you can contact us using the details below, under "Contact us".

## **Disclosing information**

We use third parties to offer you our website, as well as our products and services. Where necessary, we will disclose your information to our service providers and professional advisers (e.g. IT providers, cloud service providers, KYC partners, CRM providers, marketing support providers (such as agencies that manage our social media accounts), social media providers such as LinkedIn, analysts, customer service providers, business development providers and legal service providers, and to service providers for account mapping purposes.

If our business is sold or integrated with another business, your details will be disclosed to our advisers and any prospective purchaser's advisers, and will be passed to the new owners of the business.

We may disclose information to third parties in connection with legal claims, or when we have a legal obligation to do so. We may also disclose information with your permission (such as if we wish to disclose your details with another group company for their recruitment purposes).



## Notice of collection

The table below provides a summary of the categories of personal data that we collect and disclose to service providers and other third parties.

| Category of personal data Adyen collects      | Examples of personal data Adyen collects                                                                                                                                                                                                                        | When and why does Adyen collect this information?                                        | What kind of third parties we disclose to, and for what business purpose(s)                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Know Your Customer (“KYC”) information</b> | Name, date of birth, contact information, bank account number, tax identification number, nationality and national identification number, and job title, including biometric data. Birth certificates for parents or guardians of minors (children ages 13-17). | When you sign up for Adyen services. We are legally obliged to collect this information. | Adyen discloses this information to identity and verify providers and screening partners, including credit reference agencies, and may disclose this information to regulatory authorities upon request or for mandated reporting. Adyen may disclose this information to payment schemes, local payment providers, debt collecting agencies, internal bank system providers, cloud service providers and other third-party service providers, depending on |

|                                               |                                                                     |                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                    |
|-----------------------------------------------|---------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                               |                                                                     |                                                                                                                                                                         | the services acquired. Adyen may also make such information available to Platform customers you have signed up with.                                                                                                                                                                               |
| <b>Business information</b>                   | Your name, business email, phone number, company name, and website. | When you fill out our sales form and when we communicate with you. Adyen collects this information for marketing purposes, and for providing our products and services. | Adyen discloses this information with our customer relationship management (“CRM”) service providers so they can reach out and further build a relationship, and with account mapping service providers to identify opportunities, collaborate, enhance customer success, and expand market reach. |
| <b>Customer or user financial information</b> | Name, bank account numbers and credit card numbers.                 | When you sign up for Adyen services. Adyen is legally obliged to collect this information, and it also helps us to provide our products and services.                   | Adyen discloses this information with customers for our embedded financial products, card printing partners for our Issuing product, and with law enforcement agencies                                                                                                                             |

|                                             |                                                                                            |                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------|--------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                             |                                                                                            |                                                                                                                                                       | in compliance with legal orders.                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Transaction information</b>              | Credit card details, debit card details, transaction amount, date and time of transaction. | When you purchase a good or a service from an Adyen customer. Adyen collects this information for the purpose of providing our products and services. | Adyen discloses this information to our customers in our Customer Area, to authorities pursuant to legal orders, to cloud service providers, and to the selected payment schemes, such as Visa and Mastercard, interbank payment system providers, and local payment methods upon request. Adyen may disclose this information to regulatory authorities upon request or for mandated reporting. |
| <b>Internet or similar network activity</b> | Cookies                                                                                    | When you visit Adyen's website. Adyen collects this information for marketing purposes.                                                               | Adyen discloses this information to IT providers, CRM providers, social media providers, and advertising networks for                                                                                                                                                                                                                                                                            |

|                                                                                 |                                                                                     |                                                                                            |                                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                 |                                                                                     |                                                                                            | its own advertising purposes.                                                                                                                                                                                                                                                                                         |
| <b>Sensitive personal information, as defined in United States privacy laws</b> | Social Security number, driver's license, or identification document, and passport. | When you sign up for Adyen services. Adyen is legally obliged to collect this information. | Adyen discloses this information to identity verification providers, including credit reference agencies, to tax authorities as legally required, and regulatory authorities upon request or for mandated reporting.<br><br>Adyen does not use or disclose this sensitive personal information for any other purpose. |

Adyen does not knowingly “sell” or “share” the personal data of individuals under 16 years of age.

We reserve the right to use de-identified or aggregated data for any purpose without limitation, and we will not attempt to re-identify the information.

We will only keep your data for as long as we reasonably need to for the purposes listed above, or as otherwise required by law.

#### **When Adyen has processed your transaction**

Adyen is a payment service provider and as such provides acquiring services to its customers. This means that Adyen accepts payments on behalf of the relevant merchant and transfers the funds

paid by the shopper (“you”) to the merchant. Adyen’s role is to request the relevant payment scheme, such as Mastercard, Visa or iDeal, to authorize the transaction and send this authorization to the shopper’s bank for approval. If the bank gives approval, Adyen is notified by the relevant payment scheme and makes the payment to the merchant’s bank.

When we provide such acquiring services to our customers, we process your personal data as a data controller. It is important to us that your personal data is handled carefully and that you are well informed about the way we process your personal data.

We process the data we need for our legitimate interest of providing acquiring services to our merchants, which in this context are usually web shops and brick-and-mortar stores that sell you goods and services. This means that we receive your payment on behalf of the merchant and handle matters relating to these financial transactions. In addition, when a merchant wishes to charge your card for a recurring payment and your card has expired, Adyen may request the relevant payment scheme or look up your up-to-date card information on the Adyen platform, to facilitate your payment.

In addition, we process your data to comply with our legal obligations as a financial institution, such as to monitor financial transactions to help prevent fraud, money laundering and terrorist financing. For these reasons, we may collect your debit or credit card number (which we encrypt in accordance with PCI DSS standards), the expiry date (month and year) of your card, your bank account details, including IBAN and SWIFT/BIC, the transaction amount and the currency in which the transaction is initiated, the date, time, and location of the transaction, and the category and ID of the merchant you are shopping with.

If necessary, we can also process any of the information outlined above for our legitimate interest of protecting our legal rights – for example, in connection with legal claims, and when we have a legal obligation to process your information.

In addition, Adyen processes your personal information for the following purposes:

- To provide the service in accordance with the agreements we have with our customers and the specific payment method or bank;

- To optimize payment performance and improve our products and services;
- To comply with applicable laws and regulations;
- To conduct analysis for statistical, strategic, and scientific purposes; and
- To protect our platform, systems, and services from misuse, fraud, financial crimes, or other unauthorized or illegal activity.
- To transfer payment funds, Adyen may process your personal information when necessary to either pay the funds out to you, or collect the funds from our account.

### **How long do we keep this data?**

We only keep your data for as long as we reasonably need to for the purposes listed above.

We keep the data we collect to perform the transaction in accordance with applicable laws. For most jurisdictions, this is a period of 7 years after conclusion of the relevant transaction, in order to meet our fiscal, corporate, and other statutory obligations.

The retention terms above can be longer than stated, if we are required to keep this data for any other applicable law or to administer our business. If we need to keep any information longer for our legitimate interest of protecting our legal rights, we will keep the necessary information for this purpose until the relevant claim(s) has/have been settled.

### **Who do we disclose this information to?**

In some jurisdictions, we may partner with third parties to be able to offer you our acquiring services. It will depend on your location, the payment method you use, and the third party issuing bank. Additionally, we disclose your information to the merchant you are shopping with, and if relevant, used by the platform. We may also disclose some of your information to competent authorities and/or regulators, in case this is required to comply with our obligations as a financial institution – for example, to prevent money laundering or terrorist financing.

Otherwise, we will not disclose your information to any third party, unless we have your permission, and where it is necessary in connection with the purposes above, or with legal claims, or when we have a legal obligation to do so.

### **Compliance obligations**

You may be an Adyen customer as a merchant, platform, user / sub-merchant (for instance by using our services through a third-party platform), card holder, business account holder, or card program provider. If you sign up to become one of our customers by entering into an agreement with Adyen (including by accepting our terms and conditions), we will collect information we need to establish and perform a contract with you; this includes your contact information, address, ID documentation, tax information, creditworthiness, and payment details. We use this information to set up our products and services for you, and to provide you with support, onboarding, and integration to our platform. We also use this information to help you with configuring settings in the Adyen Customer Area, POS terminal field services, installation of POS terminals in stores, to pick up old/damaged POS terminals, and with other actions that need to be taken to establish or perform our contract with you. In addition, we use your information for our legitimate interest of managing our internal administration and to comply with our legal obligations, such as the prevention and detection of fraud, our Know-Your-Customer processes, and taxation obligations.

We have an obligation to comply with applicable laws and regulations, and to prevent fraud, money laundering, and terrorist financing. Since we are active in the financial sector, we cannot accept any customer without performing thorough checks, or without determining, investigating, and reporting suspicious transactions that take place. Therefore, if you are applying to become one of our customers, we will need to collect up-to-date information and documents during the performance of our agreement to:

- Verify your identity;
- Identify the ultimate beneficial owners of your business;
- Identify the purpose and intended nature of your future business relationship with us;

- Monitor your behavior and transactions across the Adyen platform, including by using automated systems such as machine learning models that detect risks, fraud metrics and patterns, and verify the origins of your capital/assets;
- Check whether a natural person representing you is competent to do so (and verify the identity of this person);
- Check whether you are acting on behalf of yourself or on behalf of a third party; and
- Check whether you are eligible for additional ancillary services and provide a corresponding offer.

To carry out the above checks, we process information (including personal data) that you have provided to us, as well as other information created by your use of the Adyen services. This may include your name, your contact information, a copy of your identification document, your tax identification number or BSN (if legally required), biometric data (including a facial scan, voice recording and/or video), the address of your legal representative and shareholders, your bank account number, information contained in correspondence between us, bank statements, your signature, and an extract of your company registration document. We may use third-party identification, screening, and verification services (including credit reporting agencies or open banking providers) in order to assist us in verifying your identity and the documents provided to Adyen. Depending on the services you use, we may share your data with payment schemes, local payment methods, and other third-party service providers.

We use this data to ensure the safety and integrity of the financial sector by aiming to identify, prevent, and counter illegal conduct, and to comply with our Know-Your-Customer and anti-money laundering obligations. For instance, by linking your legal entity data (e.g. name and company details) with your transaction information (e.g. email address and bank details), we actively enhance fraud detection, ensure data accuracy, and accelerate onboarding and review cycles. This processing is conducted to meet Adyen's legal requirements, for example under the Dutch Financial Supervision Act (Wft) and the Dutch Money Laundering and Terrorist Financing



Prevention Act (Wwft). In accordance with local laws, Adyen may be required to process the above mentioned personal data to investigate and report unusual transaction behavior.

Adyen may use automated decision-making, including profiling, during the initiation or execution of a contract with you, where permitted by applicable laws, or with your consent. If this decision would have legal implications or otherwise significantly affect you, you have the right to opt-out of such profiling, obtain human intervention, express your point of view, or contest the decision based solely on automated processing, including profiling.

Adyen processes your personal information for the following purposes:

- To provide you with the services pursuant to any agreement between you and Adyen;
- To optimize payment performance and prevention and detection of fraud;
- To improve our products and services;
- To comply with applicable laws and regulations;
- To train and use automated systems, including machine learning models;
- To conduct analysis for statistical, strategic, and scientific purposes;
- To protect our platform, systems and services from misuse, fraud, financial crime, or other unauthorized or illegal activity including the prevention, investigation, and detection of (payment) fraud on the basis of legitimate interest and/or compliance with legal obligations; and
- For reporting and training purposes.

### **How long do we keep this data?**

If you are currently, or become, one of our customers, we will keep information relating to our business relationship for a period of 7 years following the end of your contract with us, or until the rejection of your application. Documents used to verify your identity, including biometric identifiers, are typically stored for 5 years to meet our legal obligations related to fraud

prevention, anti-money laundering, and counter-terrorism financing. However, the retention period may vary depending on local regulatory requirements. Data that we have collected in relation to our legal obligation to verify our customers will be kept for as long as it is required by law – in most cases, 5 years. We may also disclose some of your information to competent authorities and/or regulators, in case this is required to comply with our obligations as a financial institution, for example, for the purpose of preventing money laundering and terrorist financing.

## **Embedded financial products**

### **Card Issuing**

#### **When you have an Adyen issued card**

If you or your employer sign up for our Card Services, we may provide you with a debit card, charge card, or prepaid card depending on the type of account linked to your card (“Card Services”), and in connection with your Card Program Provider’s agreement with Adyen. We will process your personal data, including KYC information (e.g., name and address), in order to provide you with these services. Your name, address, and card details may be shared with card manufacturers to provide you with a physical card.

If you are issued a card directly by one of Adyen’s bank sponsors, we may collect additional personal information to fulfill our KYC obligations.

When provided with a card issued by Adyen or by one of Adyen’s bank sponsors, Adyen will also process transaction information, including your cardholder name, card number and expiry date.

Finally, when providing Card Services, we may process your information for the following purposes:

- Processing and monitoring transaction behavior;
- Verifying your identity for authentication purposes; and
- Improving our products and services.

#### **How long do we keep this data?**

We will only keep your data for as long as we reasonably need to for the purposes listed above.

We keep the data we collect in order to perform the transaction in accordance with applicable laws. We maintain different data retention periods depending on regional requirements. For most jurisdictions, this is a period of 7 years after conclusion of the relevant transaction, in order to meet our fiscal, corporate, and other statutory obligations.

The retention terms outlined above may be extended if we are required to keep data longer due to applicable law, or to administer our business. If we need to keep any information for an extended period for our legitimate interest of protecting our legal rights, we will keep the necessary information for this purpose until the relevant claim(s) has/have been settled.

## **Capital**

### **When you receive an Adyen loan or merchant cash advance**

If you are a user or sub-merchant and are signed up for Adyen Capital (a financial product offered by Adyen to its platform customers), you may receive an Adyen loan or merchant cash advance, depending on your location. To be able to offer you these products, Adyen will need to collect KYC information from you.

In order to determine your eligibility for Adyen Capital, we will run initial checks on your use of Adyen products and services, including your current and anticipated sales volume. We may rely on our customer's own internal credit checks and compliance checks to determine eligibility and/or may collect additional information. This process may involve automated decision-making, which may include profiling under certain privacy laws. You have the right to opt-out of such profiling. Please note that opting-out of profiling will mean that you are no longer eligible for Adyen Capital. Please see Your Individual Rights for more information about these rights and how to opt-out.

When provided with Adyen Capital, Adyen will process information about the transactions made from such loans or merchant cash advance. Such information may be shared with Adyen's customer.

If and when necessary, your personal information may be shared with third parties to provide you with our products and services, or with collection agencies.

### **How long do we keep this data?**

We only keep your data for as long as we reasonably need to for the purposes listed above.

We keep the data we collect in order to perform the transaction in accordance with applicable laws. We maintain different data retention periods depending on regional requirements, for most jurisdictions, this is a period of 7 years after conclusion of the relevant transaction, in order to meet our fiscal, corporate, and other statutory obligations.

The retention terms above may be extended if we are required to keep data longer due to applicable law, or to administer our business. If we need to keep any information for an extended period for our legitimate interest of protecting our legal rights, we will keep the necessary information for this purpose until the relevant claim(s) has/have been settled.

## **Business Account**

### **When you receive an Adyen-issued business account**

If you request an Adyen business account, we process your personal data such as your name, address, company name, and address in order to provide you with the business account. In addition, we may collect additional personal information to complete KYC or other compliance obligations. In order to perform any services related to your business account, Adyen will process all information relevant to the business account, account funding, as well as the account and routing number associated with the business account.

### **How long do we keep this data?**

We only keep your data for as long as we reasonably need to for the purposes listed above. Under most regulations, we are required to keep a record of bank account transactions for 7 years.

The retention terms may be extended if we are required to keep data longer due to applicable law, or to administer our business. If we need to keep any information longer for an extended period for our legitimate interest of protecting our legal rights, we will keep the necessary information for this purpose until the relevant claim(s) has/have been settled.

## **Pix Open Finance Payment**

### **When you make use of Adyen's Pix Open Finance Payment Services**

When you opt into Adyen's Pix Open Finance Payment service, we collect and process your Enrollment ID, Device ID and [your consent](#). This data is essential for enabling the service, facilitating transactions, verifying devices, and ensuring security through authentication. Your data is securely stored within Adyen's systems.

### **How long do we keep this data?**

Your data will be held for the duration you set when enrolling via your bank's interface. If no specific duration is selected, we will retain this data only for as long as necessary to fulfill the purposes, or for to comply with applicable law.

### **Your consent**

By enrolling through your bank, you consent to Adyen storing the necessary information for the Pix Open Finance Payment service. If you prefer not to use this service, simply decline within your bank's interface. You can then proceed with a standard Pix payment.

### **Security at Adyen**

We are committed to securing your personal data and have implemented measures to do so effectively. In order to prevent unauthorized people or parties from being able to access your data, we have put in place a range of technical and organizational measures to safeguard and secure the information we process about you. These include:

#### 1. Security Program, Policies, and Personnel:

We maintain an Information Security Program to identify risks and implement appropriate controls. This program is reviewed on a regular basis to ensure continued effectiveness and accuracy. We have a full-time information security team responsible for monitoring, maintaining, and continually improving our security. We have suitable and effective information security policies and procedures that are essential to complying with relevant regulations.

## 2. Audits and Certifications:

We undergo independent verification of our security and compliance controls to help meet regulatory and policy objectives. Adyen's current information security third-party independent audits include:

a. The Payment Card Information Data Security Standard (PCI-DSS)

PCI DSS is a set of information security and business best-practice guidelines to establish a "minimum security standard" to protect customers' payment card information. Adyen undergoes at least an annual third-party audit to certify our product and payment platform with the PCI-DSS.

b. Systems and Organization Controls 2 (SOC 2) Type 2

The SOC 2 is a report based on the Auditing Standards Board of the American Institute of Certified Public Accountants' (AICPA) existing Trust Services Criteria (TSC). The purpose of this report is to evaluate Adyen's information systems relevant to security, availability, confidentiality, and privacy. Adyen undergoes at least an annual third-party audit to report on the suitability of the design and the operating effectiveness of our controls.

## 3. Access Control and Privilege Management:

We restrict administrative access of our production systems to approved personnel. When hired, our approved personnel are assigned unique IDs and credentials. Upon termination of approved personnel, or where compromise of such credentials is suspected, administrative access is revoked. Access rights and levels are based on our employees' job function and role, and are based

on the security concepts of 'least-privilege' and 'need-to-know', to ensure access privileges are matched with defined responsibilities.

#### 4. Data Encryption:

We encrypt data at rest where technically feasible, and in transmission with our user interfaces or APIs (using TLS or similar technologies) over the internet.

#### 5. Security Monitoring and Incident Response:

We have an incident management process for security events that may impact the confidentiality, integrity, or availability of our systems or data. This process includes defined response times for Adyen to notify relevant parties. This process specifies courses of action, procedures for notification, escalation, mitigation, and documentation. The incident response program includes 24x7 centralized monitoring systems and on-call staffing to respond to security incidents.

#### 6. Physical Security:

At our physical locations, such as data centers, there are controls in place to prevent unauthorized physical access. These include: Security checkpoints, badged (or biometric) authentication, mandatory visitor sign-in, and video surveillance.

#### 7. Network Management and Security:

We uphold industry-standard, and secure network architecture, supported by reasonably sufficient bandwidth and redundant network infrastructure to mitigate the impact of any individual component failure. Our security team utilizes industry-standard utilities to defend against known common unauthorized network activity, monitor security advisory lists for vulnerabilities, and undertake regular external vulnerability scans and audits.

#### 8. Security in our Development Process

Our products and our payment platform are designed and developed with industry-defined security and privacy practices in mind. We maintain a documented product development lifecycle, known as a Secure Software Development Lifecycle (SSDLC), with formal development principles.

## **Checkout**

To make your payment journey smoother and more efficient, Adyen offers solutions that personalize and optimize your checkout experience. This may involve ranking payment methods based on your frequency of use.

We process the data for our legitimate interest to improve and optimize the checkout experience for you and our merchants. The data processed may include email address, cardholder name, country code and preferred payment method.

You have the right to object to this form of processing and can opt-out of personalized checkout at any time. Please see Your Individual Rights for more information about these rights and how to opt-out.

### **Who do we disclose this information to?**

We will not disclose the underlying information to our merchants. Also, we will not disclose your information to any third party.

### **How long do we keep your information?**

We will only keep your data for as long as we reasonably need to for the purposes listed above.

The retention terms may be extended if we are required to keep data longer due to applicable law, or to administer our business. If we need to keep any information longer for an extended period for our legitimate interest of protecting our legal rights, we will keep the necessary information for this purpose until the relevant claim(s) has/have been settled.

## **Marketing**

### **How we process data for our newsletter and marketing purposes**

You can sign up to receive marketing communications (such as our newsletter), personalized messages with the intent to establish a business relationship, or invitations to events, by providing your name and email address via the sign-up form on our website. When you fill out this form, you



give your consent to receive our newsletters, invitations to events, and other relevant marketing communications. You can unsubscribe from these emails at any time by following the instructions in the respective communication.

If you are one of our merchants, we may contact you about relevant products or services, for our legitimate interest in developing our business. We can do this by reaching out to you via email, or by connecting with you on LinkedIn, and/or by sending you messages on LinkedIn. If you are not yet one of our merchants, we will only contact you with offers or about our products or services. When we contact you for these purposes via email, you will have an opportunity to opt-out by following the instructions within the email, or by contacting us using the contact details below (under “Contacting us”). Our action will be subject to applicable limitations of the laws of your home jurisdiction.

You can also download content, for example white papers and research reports, from our website using the forms designed for this purpose. We collect the data you provide on the form, including your name, company, country, and email address. We process the data you provide on this form for our legitimate interest of keeping track of who downloads our content, and to send you relevant marketing communications.

### **How long do we keep this data?**

We store the information that we process from you as a result of you subscribing to our newsletters, or because you have consented to receive information about our products and services or about offers, until such a time as you decide you would no longer like to receive these mailings.

### **When you contact us or ask us to contact you**

Through our website, you have the option to contact us directly and to ask us to contact you regarding any questions, queries, (support) requests, comments or complaints you have. Additionally, you can fill out an application to become a merchant or a partner, or sign up for a test account. When you do this, we collect the information that you provide, including your name, company, contact details, the reason you are contacting us, verification that you are not a robot,

and other information you decide to fill out. You can also contact us by calling or emailing us using, for example, the contact details listed on our website. If you do so, we will collect your name, company, and any other information we need to be of further assistance to you and/or communicate with you. When speaking with us over the phone, we may also process and record conversations you have with Adyen staff. The recording of your telephone conversations will be processed for quality assurance and training purposes related to your use of our products and services. We process this data with your consent so that we can assist you in adequately using our products and services, as well as to improve and optimize our services.

We use the data, as outlined above, to answer your question, comment, or complaint, and respond to your queries and (support) requests, as well as to assess your application to become a customer or partner. As such, we use this data to establish or perform our (future) contract with you and for our legitimate interests in following up with you. We also use the data above for our legitimate interest of conducting business with you and managing our internal administration, for training purposes, for establishing and performing our contract with you, for our legitimate interest of conducting marketing research so we can improve our products and services, and to be able to offer our (future) customers tailored products and services.

### **How long do we keep this data?**

Data about any questions, comments, or (support) requests you have made to us, will only be kept for as long as we reasonably need it for the purposes listed above, or as required by our data retention obligations.

### **Website**

When you browse our website, we process your IP address, internet browser and device type, location data, and information about your use of our website and the app – including which pages you visited, how you came to our website, the time and length of your visit, and your language preferences.

We use this data for our legitimate interests of making sure our website works properly, including for debugging, to be able to deliver you content and for DDOS mitigation, and improving our website, and to perform statistical analyses for optimizing and improving our website. We also use this information to provide you with personal offers tailored to your needs, and to tailor what we show you to your preferences, with your prior consent.

We collect this data using cookies and similar techniques, including tags/beacons and javascripts. More information about these techniques can be found in our [Cookies Policy](#).

When we collect information about how you use our website, such as which landing pages you visit and which items you look at, we do so in order to determine how we can best provide our services to you. For example, if you read about our products and services on our website, we might classify you as a user or a website visitor who is interested in our products and services, and therefore as a potential customer of Adyen. Based on the audience we infer you belong to, we may for example contact you with offers about our products and services, providing we have your consent to do so, and subject to limitations under the laws of your home jurisdiction.

In order to make the most accurate assessment about which audience you likely belong to, and as you can read in our [Cookies Policy](#), we also use tracking cookies. These cookies track information about how you use our website and which other websites you visit, for example to show you advertisements for products and services of ours that we anticipate you might be interested in. We only place these tracking/targeting cookies with your prior consent. For more information about these tracking cookies, please view our [Cookies Policy](#).

On our website, we might ask you to provide feedback on the specific page you are visiting. When giving your feedback, you can optionally provide your name and email address. We can use this information to follow up with you personally.

### **How long do we keep this data?**

We will only keep your data for as long as we reasonably need to for the purposes listed above.

For example, data about your visit(s) to our website will be retained until your use (or 'browsing session') ends, except where it concerns data collected for the analytical and marketing purposes

specified above. In those cases, we will keep your information for a period of 1 year following its collection.

### **Social media buttons**

We use tags on our website from social media networks such as Facebook, LinkedIn, and X. You will be able to recognize these tags by their logos. Our tags are tracking pixels that will send user behavior back to the network(s). The tracking pixels will only work if you accept our cookie statement.

We do not have any influence over which data these providers collect from you and we are also not aware of the extent of their data processing. If you would like more information about their data processing, this can be found in the respective privacy policies of these providers.

### **Other**

We also collect data about your use of our products and services and your Customer Area account, including your login details, and the questions, queries, comments, and complaints you send or share with us regarding our business relationship. We process this data to be able to perform our contract with you by following up with you, provide you with support where necessary, and for our legitimate interest of being able to optimize and improve our products and services.

We can also use your (company) email address for: keeping you up to date with our products and services; tailoring offers to your needs (meaning that offering products and services similar to those that you have already purchased from us); inviting you to participate in surveys regarding our products and services; or inviting you to events.

If necessary, we can also process any of your information above for our legitimate interest of protecting our legal rights, for example in connection with legal claims, and when we have a legal obligation to process your information. We may also transfer your data in the event of a company reorganization, or business transactions, such as in the event of sale or bankruptcy.

### **How long do we keep your information?**

We will only keep your data for as long as we reasonably need to for the purposes listed above.

The retention terms above may be extended if we are required to keep data longer on the basis of applicable law or to administer our business. If we need to keep any information for an extended period for our legitimate interest of protecting our legal rights, we will keep the necessary information for this purpose until the relevant claim(s) has/have been settled.

## **Fraud**

### **When merchants use our fraud detection services**

Adyen offers its customers different kinds of fraud detection services. For some of our fraud services, Adyen acts as a data processor on behalf of, and under the instructions of, its merchants. Please take a look at our merchants' privacy policies for more information regarding this processing of your personal data.

For activities involving fraud detection, prevention, and monitoring, where Adyen acts as a data controller, the following information may be utilized, including but not limited to transaction data (such as card number and cardholder name), email address, location data, IP address, information on disputed transactions, information on confirmed fraud, merchant details, device fingerprint, and unique identifier(s).

Adyen uses your personal data for the purposes of protecting you against fraud or unauthorized transactions, and preventing and monitoring fraud across the Adyen platform. Furthermore, Adyen has a legal obligation to prevent money laundering and terrorist financing. This includes the identification of fraud with the payment details provided by our merchants, or information about fraud from other third parties, such as issuing banks, acquirers, or payment schemes.

Additionally, Adyen processes and aggregates your personal data to create, train, and run models or other methods to accurately identify, predict, prevent, and mitigate fraud across the Adyen platform globally. These models or other methods may be leveraged to offer fraud-related products and services to our merchants.

Within the limits of what is legally permitted regarding automated decision-making, the use of these fraud models and/or other methods may result in merchants making decisions over whether or not to grant you access to a product or service, and/or whether or not to authorize a transaction. For more information please [click here](#).

### **How long do we keep this data?**

We will only keep the data for as long as we reasonably need to for the purposes listed above.

### **Cookies**

We use cookies and similar techniques, such as pixels, which are small text files stored on your device. Using cookies is a way for us to ensure that our website is continuously improved and serves as a tool to optimize our marketing strategies. In order for us to do this, we place only strictly necessary performance and functional cookies to enable the website to function, as well as targeting and social media cookies which help us reach the right audience and display advertisements effectively. Some of these cookies track your use of our website and visits to other websites, as well as allow us to show you advertisements when you browse other websites.

Please see our [Cookies Policy](#) for more information on our use of cookies.