Name	Type	Comment	Address
Google	Hosting Provider	Google Servers host the data. Servers are all within Europe.	Google Ireland Limited Gordon House Barrow Street Dublin 4 IRELAND https://cloud.google.com/security/gdpr
OVH	Hosting Provider	OVH Servers are used to host the data. Servers are all within Europe.	OVH GmbH St. Johanner Str. 41-4 66111 Saarbrücken GERMANY https://www.ovh.de/schutz-personenbezogener-daten/faq.xml
Websms	SMS Sending	Used to send customer invites or alerts over SMS.	sms.at mobile internet services gmbh Brauquartier 5/Top 13 8055 Graz AUSTRIA https://websms.at/de-at/sicherheit/
Amazon	E-Mail Sending	Used to send transactional E-mails for alerts or to communicate with the user.	Amazon Web Services EMEA SARL 38 avenue John F. Kennedy L-1855 LUXEMBOURG https://aws.amazon.com/de/compliance/gdpr-center/
Telematica	SIP Provider	Used for phone calls if our SIP Server is used.	Telematica Internet Service Provider GmbH Münzgrabenstraße 84b/5 8010 Graz AUSTRIA https://www.telematica.at/telematica/datenschutz

Twilio	SIP Provider	Used for phone calls if our SIP Server is used. Two different providers are used to have redundancy.	Twilio Inc Block D, Harcourt Rd, Saint Kevin's, Dublin 2 IRELAND https://www.twilio.com/legal/data-protection-addendum
Hubspot	Support Tool	Used for support with end customer.	HubSpot Germany GmbH Am Postbahnhof 17 10243 Berlin GERMANY https://legal.hubspot.com/privacy-policy
Stripe	Payment Provider	Used for charges of the end customer. Only applies if done with the Arivo system.	Stripe Payments Europe, Limited C/O A & L Goodbody,Ifsc, North Wall Quay Dublin 1. Dublin 1 IRELAND https://stripe.com/docs/security/stripe

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) ([1]) 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 ([5]
(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 ([6]

(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. ([9]
(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 ([12] (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.

([1] (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.

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

) Not applicable

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

) Not applicable

(4

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

) Not applicable

(5

(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.

(6

(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.

(7

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

) Not applicable

(8

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

) Not applicable

(9

(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.

(10

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

) Not applicable

(11

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

) Not applicable

([12] (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 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

Start date	(a) 21 September 2022, where the effective date of the Agreement is before 21 September 2022; or (b) otherwise, on the effective date of the Agreement.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**

Parties' details	Full legal name: Customer Trading name (if different): 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.	Full legal name: Google Trading name (if different): 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.
Key Contact	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.
Signature (if required for the purposes of Section 2)	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

Addendum EU SCCs	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

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

Mandatory Clauses	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

Supplementary Clauses	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.

PREVIOUS VERSIONS *(Last modified September 20, 2022)*

April 4, 2022 _ (/terms/sccs/eu-p2p/index-20220404) September 24, 2021 (/terms/sccs/eu-p2p/index-20210924)

OVHcloud®

Data Processing Agreement

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 DPAis 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**) 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

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).

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.

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.
    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

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 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, 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

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, 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

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 of 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 Clauses2. 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, 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

Social Networks

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 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 anmeldenden, Vertrag abschließenden Person	Dauer des Vertragsverhältnisses und über die entsprechenden gesetzlichen Aufbewahrungsfristen	AUFTRAGGEBER, bzw. natürliche Person, die für die Anmeldung bevollmächtigt ist
Verrechnungsdaten	Korrekte Fakturierung der bestellten Services	Dauer des Vertragsverhältnisses und über die entsprechenden gesetzlichen Aufbewahrungsfristen	Mitarbeiter des AUFTRAGGEBERS
Kontodaten	Verrechnung der offenen Rechnungen, sowie SEPA Lastschriftmandate	Dauer des Vertragsverhältnisses und über die entsprechenden gesetzlichen Aufbewahrungsfristen	Mitarbeiter des AUFTRAGGEBERS
Bestelldaten	Detailinhalte über die Bestellung	Dauer des Vertragsverhältnisses	AUFTRAGGEBER Mitarbeiter des AUFTRAGGEBERS
Userdaten	Zugangsverwaltung zum websms System	Dauer des Vertragsverhältnisses	Mitarbeiter des AUFTRAGGEBERS
Verkehrsdaten	Nachrichtenversand, Abrechnung	Dauer des Vertragsverhältnisses und über die entsprechenden gesetzlichen Aufbewahrungsfristen	AUFTRAGGEBER Endkunden des AUFTRAGGEBERS
Endkundendaten	Alle Daten, die im Rahmen der Erbringung der Leistungen generiert werden	Dauer des Vertragsverhältnisses	Mitarbeiter des AUFTRAGGEBERS Betroffene Endkunden
Inhaltsdaten	Inhalte aus den Nachrichten	Bei Anlieferung via Schnittstelle: unmittelbare Löschung nach Zustellung Bei Aktivierung Chatfunktion: Dauer des Vertragsverhältnisses Ausnahme: Chatverlauf wird vom Endkunden gelöscht	Mitarbeiter des AUFTRAGGEBERS Betroffene Endkunden

IV. Dauer der Verarbeitung

a. 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.
b. Eine Kündigung des LINK Mobility Nutzungsvertrages erstreckt sich automatisch auf den Vertrag über die Auftragsverarbeitung.
c. Eine vorzeitige Kündigung des Vertrages über die Auftragsverarbeitung wird von beiden Parteien ausgeschlossen.
d. 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

Graz, am **13.3.2023**

Josef Grabner
Managing Direktor

Für den AUFTRAGGEBER

Graz ……………………………, am 9/4/22 ……………………………

ARIVO
Arivo Parking Solutions GmbH
Am Innovationspark 10, 8020 Graz, Austria
ATU72068549 FN467497x
Info@arivo.co +43 316 375 018 www.arivo.co

……………………………………………………………
Name und Funktion

Signiert von:	Josef Grabner
Datum:	15.03.2023 09:43:32

A-TRUST

Dieses Dokument ist digital signiert!
Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.

Prüfinformation: Informationen zur Prüfung der elektronischen Signatur finden Sie unter: www.a-trust.at/pdf

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 Berechtigtenausweisen
   - 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. **Löschungsfristen**
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; ISO zertifiziertes Hochsicherheitsrechenzentrum
rapidmail GmbH	Augustinerplatz 2 79098 Freiburg i.Br. Deutschland	Newsletterversand
mtms solutions GmbH	Nordstraße 4, 5301 Eugendorf, Österreich	Betrieb, Wartung und Kundenservice von Spezialapplikationen
easyname GmbH	Canettistraße 5/10 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.

"**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.

"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

Telematica Internet Service Provider GmbH

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)] (in 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 darüberhinausgehende 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 DSG) 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 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
- Datenschutzzertifizierungen 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 Datenschutzzertifizierungen 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, Wachschutz).

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
Arivo Parking Solutions GmbH
Am Innovationspark 10, 8020 Graz, Austria
ATU72088549 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

i.V. T. Kommer

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
✓ Aktenshredder mind. empfohlene Sicherheitsstufe P-4 (DIN 66399)	✓ Einsatz Berechtigungskonzepte
✓ Externer Aktenvernichtung mind. Sicherheitsstufe P-6 (DIN 66399)	✓ Minimale Anzahl an Administratoren
✓ Physische Löschung von Datenträgern	✓ Verwaltung Benutzerrechte durch Administratoren
✓ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	✓ Richtlinie Informationssicherheit
✓ Zugriffe SSH Verschlüsselt	✓ Arbeitsanweisung Kommunikationssicherheit
✓ zertifizierte SSL Verschlüsselung	✓ Arbeitsanweisung Umgang mit Informationen und Werten

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
✓ Trennung von Produktiv- und Testumgebung	✓ Steuerung über Berechtigungskonzept
✓ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	✓ Festlegung von Datenbankrechten
✓ Mandantenfähigkeit relevanter Anwendungen	✓ Richtlinie Informationssicherheit
✓ VLAN-Segmentierung	✓ Richtlinie Datenschutz
✓ Kundensysteme logisch getrennt	✓ Arbeitsanweisung Betriebssicherheit
✓ Staging von Entwicklungs-, Test und Produktivumgebung	✓ Arbeitsanweisung Sicherheit in der Softwareentwicklung

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
✓ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem System (verschlüsselt)	✓ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren
✓ auf Wunsch des Kunden werden Logfiles pseudonymisiert	✓ Richtlinie Informationssicherheit
	✓ Richtlinie Datenschutz
	✓ Separate, explizite Arbeitsanweisung Kryptographie (dzt. in Ausarbeitung)

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
✓ Einsatz von VPN ✓ Protokollierung der Zugriffe und Abrufe ✓ Bereitstellung über verschlüsselte Verbindungen wie sftp, https – Secure Cloudstores ✓ Nutzung von Signaturverfahren (fallabhängig)	✓ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen ✓ Weitergabe in anonymisierter oder pseudonymisierter Form ✓ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen ✓ Persönliche Übergabe mit Protokoll ✓ Richtlinie Informationssicherheit ✓ Richtlinie Datenschutz

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
✓ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten ✓ Manuelle oder automatisierte Kontrolle der Protokolle (nach strikten internen Vorgaben)	✓ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können ✓ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen) ✓ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts ✓ Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden ✓ Klare Zuständigkeiten für Löschungen ✓ Richtlinie Informationssicherheit ✓ Arbeitsanweisung IT-Benutzerordnung

3. VERFÜGBARKEIT UND BELASTBARKEIT

3.1. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (USV, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.).

Technische Maßnahmen

- ✓ Feuer- und Rauchmeldeanlagen
- ✓ Feuerlöscher Serverraum
- ✓ Serverraumüberwachung Temperatur und Feuchtigkeit
- ✓ Serverraum klimatisiert
- ✓ USV-Anlage und Notrom-Dieselaggregate RZ
- ✓ Schutzsteckdosenleisten Serverraum
- ✓ RAID System / Festplattenspiegelung
- ✓ Videoüberwachung Serverraum
- ✓ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum

Organisatorische Maßnahmen

- ✓ Backup-Konzept
- ✓ Keine sanitären Anschlüsse im Serverraum
- ✓ Existenz eines Notfallplans
- ✓ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- ✓ Getrennte Partitionen für Betriebssysteme und Daten, wo notwendig
- ✓ Richtlinie Informationssicherheit
- ✓ Arbeitsanweisung Betriebssicherheit
- ✓ Regelmäßige Tests der Dieselaggregate RZ

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

- ✓ Backup-Monitoring und -Reporting
- ✓ Wiederherstellbarkeit aus Automatisierungs-Tools
- ✓ Backup-Konzept nach Kritikalität und Kundenvorgaben

Organisatorische Maßnahmen

- ✓ Recovery-Konzept
- ✓ Kontrolle des Sicherungsvorgangs
- ✓ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
- ✓ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
- ✓ Existenz eines Notfallplans
- ✓ Richtlinie Informationssicherheit
- ✓ Arbeitsanweisung Betriebssicherheit

4. VERFAHREN ZUR ÜBERPRÜFUNG, BEWERTUNG UND EVALUIERUNG

4.1. Datenschutzmanagement

Technische Maßnahmen

- ✓ Zentrale Dokumentation aller Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter
- ✓ Sicherheitszertifizierung nach ISO 27001
- ✓ Eine Überprüfung der Wirksamkeit der TOM wird mind. jährlich durchgeführt und TOMs aktualisiert
- ✓ Datenschutzprüfpunkte durchgängig in Tool-gestütztem Risk Assessment implementiert

Organisatorische Maßnahmen

- ✓ Interner Datenschutzbeauftragter bestellt: Group Data Protection Officer, DPO
- ✓ Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet
- ✓ Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich
- ✓ Interner Informationssicherheits-Beauftragter bestellt: Group Information Security Officer, ISO
- ✓ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
- ✓ Prozess betr. Informationspflichten nach Art. 13 und 14 DSGVO etabliert
- ✓ Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden
- ✓ Datenschutzbetrachtung im Rahmen des Corporate Risk Managements etabliert
- ✓ ISO 27001 Zertifizierung wesentlicher Unternehmensteile inkl. RZ-Betrieb und jährliche Überwachungsaudits

4.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen sowie Data Breach Prozess.

Technische Maßnahmen

- ✓ Einsatz von Firewall und regelmäßige Aktualisierung
- ✓ Einsatz von Spamfilter und regelmäßige Aktualisierung
- ✓ Einsatz von Virenscanner und regelmäßige Aktualisierung
- ✓ Intrusion Detection System (IDS) für Kundensysteme auf Bestellung
- ✓ Intrusion Prevention System (IPS) für Kundensysteme auf Bestellung

Organisatorische Maßnahmen

- ✓ Dokumentierter Prozess zur Erkennung und
- ✓ Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
- ✓ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- ✓ Einbindung von DPO und ISO in Sicherheitsvorfälle und Datenpannen
- ✓ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
- ✓ Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem
- ✓ Formaler Prozess zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen
- ✓ Richtlinie Informationssicherheit
- ✓ Richtlinie Datenschutz
- ✓ Arbeitsanweisung Betriebssicherheit
- ✓ Arbeitsanweisung IT-Benutzerordnung

4.3. Datenschutzfreundliche Voreinstellungen

„Privacy by design" / „Privacy by default" gem. Art 25 Abs 2 DSGVO.

Technische Maßnahmen	Organisatorische Maßnahmen
✓ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind ✓ Anwendung datenschutzfreundlicher Voreinstellung in Standard- sowie Individualsoftware	✓ Richtline Datenschutz (inkludiert Prinzipien „Privacy by design / default") ✓ OWASP Secure Mobile Development Security Checks werden durchgeführt ✓ Perimeteranalyse bei Webapplikationen

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
✓ Überwachung von Remote-Zugriffen Externer z. B. im Rahmen von Remote-Support ✓ Überwachung von Subunternehmern nach den Prinzipien und mit den Technologien gem. vorausgehenden Kapiteln 1, 2	✓ Arbeitsanweisung Lieferantenmanagement und Lieferantenbewertung ✓ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation ✓ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit) ✓ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln ✓ Rahmenvereinbarung zur Auftragsverarbeitung innerhalb der Unternehmensgruppe ✓ Schriftliche Weisungen an den Auftragnehmer ✓ Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis ✓ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer ✓ Regelung zum Einsatz weiterer Subunternehmer ✓ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags ✓ Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

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

Allianz für Cyber-Sicherheit
Teilnehmer

CSA cloud security alliance®

TÜV NORD
TÜV NORD CERT GmbH
DIN EN ISO 27001

TÜV NORD
TÜV NORD CERT GmbH
DIN EN ISO 9001

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 Vollanwendungsbereich 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

entweder

□ Der Gegenstand der Auftragsverarbeitung durch den AN für den AG als Verantwortlichen ergibt sich konkret aus den bestehenden Verträgen zwischen den Parteien.

oder

□ Die Auftragsverarbeitung hat den folgenden konkreten Gegenstand:

[Kurzbeschreibung des Verarbeitungsgegenstands durch den AG]

2. DAUER DER VERARBEITUNG

entweder

□ 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.

oder

□ Die Auftragsverarbeitung durch den AN erfolgt in folgendem Zeitraum (vorbehaltlich darüberhinausgehender gesetzlicher Verpflichtungen):

[Zeitraum der Verarbeitung durch den AG anzuführen]

3. ORT DER VERARBEITUNG

entweder

□ Der Ort der Auftragsverarbeitung durch den AN für den AG als Verantwortlichen ergibt sich konkret aus den bestehenden Verträgen zwischen den Parteien.

und/oder

□ 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:

□	Kunden	□	Mitarbeiter des AG
□	Interessenten	□	Externe Mitarbeiter
□	Lieferanten	□	Auftragsverarbeiter
□	Besucher der Website	□	Newsletter-Abonnenten
□		□	
□		□	

[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:

□	Namensdaten	□	Kontakt- und Adressdaten
□	Geburtsdatum	□	Kundenvertragsdaten
□	Bank- und Zahlungsdaten	□	Logindaten
□	Standort und Geoinformationsdaten	□	Daten zu Vorlieben und Verhaltensweisen
□	Bildungsdaten	□	Bewegungsprofildaten
□	Verkehrsdaten	□	Foto- und Videodaten
□	Strafrechtsrelevante Daten	□	
□		□	
□		□	

[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:

□	Rassische und ethnische Herkunft	□	Politische Meinungen
□	Religiöse oder weltanschauliche Überzeugungen	□	Gewerkschaftszugehörigkeit
□	Genetischen Daten	□	Gesundheitsdaten
□	Biometrischen Daten	□	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)](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 Security Overview (https://www.twilio.com/legal/security-overview)
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 Security Overview (https://www.twilio.com/legal/security-overview)
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 Security Overview (https://www.twilio.com/legal/security-overview)
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 Security Overview (https://www.twilio.com/legal/security-overview)

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 Security Overview (https://www.twilio.com/legal/security-overview)
Measures for the protection of data during transmission	See Section 13 (Encryption) and Section 19 (Customer Data Backups) of the Security Overview (https://www.twilio.com/legal/security-overview)
Measures for the protection of data during storage	See Section 8 (Hosting Architecture and Data Segregation) and Section 13 (Encryption) of the Security Overview (https://www.twilio.com/legal/security-overview)
Measures for ensuring physical security of locations at which personal data are processed	See Section 9 (Physical Security) of the Security Overview (https://www.twilio.com/legal/security-overview)
Measures for ensuring events logging	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)

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)
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)
Measures for ensuring data minimisation	As an organization, Twilio has adopted Binding Corporate Rules (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) (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) (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) (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).
Measures for allowing data portability and ensuring erasure	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) 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

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. 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 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, 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: Nicholas Knoop 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 **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. OPT-IN ONLY	Conversation Functionality	Used to support the connection of your WhatsApp Business account to the conversations inbox. 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.

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):

	Signature … DocuSigned by: Nicholas Knoop 2D95909F17D54E7...

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)[1] 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

[1] 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[2] 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.

[2] 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[3] (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.

[3] 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[4] (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.

[4] 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[5].

[5] 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[6]

[6] 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[7], 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.

[7] 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.[8] 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

[8] 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.[9] 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

[9] 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.[10] 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:

[10] 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[11] 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.

[11] 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[12];

[12] 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 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. …

Information Commissioner's Office

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)**
Parties' details	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):	Full legal name: Trading name (if different): Main address (if a company registered address): Official registration number (if any) (company number or similar identifier):

Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	□ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): Other identifier (if any): Or □ 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:

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,

	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";

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:

Mandatory Clauses	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 ("**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

Security Programs and Policies	Stripe maintains and enforces a security program that addresses how Stripe manages security, including the security controls Stripe employs. The security program includes: ● documented policies that Stripe formally approves, internally publishes, communicates to appropriate personnel and reviews at least annually; ● documented, clear assignment of responsibility and authority for security program activities; ● policies covering, as applicable, acceptable computer use, data classification, cryptographic controls, access control, removable media and remote access; and ● regular testing of the key controls, systems and procedures. **Privacy Program.** Stripe maintains and enforces a privacy program and related policies that address how Personal Data is collected, used and shared.
Risk and Asset Management	Stripe performs risk assessments, and implements and maintains controls for risk identification, analysis, monitoring, reporting and corrective action. Stripe maintains and enforces an asset management program that appropriately classifies and controls hardware and software assets throughout their life cycle.
Personnel Education and Controls	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 "**Personnel**") acknowledge their data security and privacy responsibilities under Stripe's policies. For Personnel, Stripe, either itself or through a third party: ● implements pre-employment background checks and screening; ● conducts security and privacy training; ● implements disciplinary processes for violations of data security or privacy requirements; and ● upon termination or applicable role change, promptly removes or updates Worker access rights and requires the Worker to return or destroy Personal Data. **Authentication**. Stripe authenticates each Personnel's identity through appropriate authentication credentials such as strong passwords, token devices or biometrics.
Training and Awareness	**Annual Security and Privacy Training.** Stripe's employees complete an annual Security and Privacy awareness training on Stripe's data security and confidentiality policies and practices.
Network and Operations Management	**Policies and Procedures**. 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.

	Vulnerability Assessments. Stripe performs periodic vulnerability assessments and penetration testing on its systems and applications, including those that Process Personal Data.
Technical Access Controls	**Access control.** Stripe implements measures to prevent data processing systems from being used by unauthorized persons, including the following measures: ● user identification and authentication procedures; ● ID/password security procedures (special characters, minimum length, change of password), including stronger digital authentication measures based on NIST 800-63B; ● automatic blocking (e.g., password or timeout); and ● break-in-attempt monitoring. **Data access control.** 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: ● internal policies and procedures; ● control authorization schemes; ● differentiated access rights (profiles, roles, actions and objects); ● access monitoring and logging; ● access reports; ● access procedure; ● change procedure; and ● deletion procedure.
Physical access controls	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: ● physical access control system and program in place at Stripe premises; ● 24x7 Global Security Operation Center that monitors physical security systems; ● security video and alarm systems; ● access control roles and area zones; ● access control audit measures; ● electronic tracking and management program for keys; ● access authorisations process for employees and third parties; ● door locking (electrified locks etc.); and ● trained uniformed security staff. Stripe reviews third-party audit reports to verify that Stripe's service providers maintain appropriate physical access controls for the managed data centers.

Availability Controls	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: ● database replication; ● backup procedures; ● hardware redundancy; and ● a disaster recovery plan.
Disclosure Controls	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.
Entry Controls	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.
Separation Controls	Stripe implements measures to ensure that Personal Data collected for different purposes can be Processed separately, including: ● "least privilege" limitation of access to data by internal service; ● segregation of functions (production/testing); ● procedures for storage, amendment, deletion, transmission of data for different purposes; and ● logical segmentation processes to manage the separation of Personal Data.
Certifications and Reports	**PCI Compliance**. 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). **SOC Reports**. Stripe maintains Service Organization Controls ("**SOC**") auditing standards for service organizations issued under the AICPA. SOC 1 and 2 reports are produced annually and will be provided upon request. Stripe may add standards or certifications at any time.
Encryption	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. **Encryption in transit.** 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.

	Encryption at rest. To protect data at rest, Stripe uses industry standard encryption (AES 256) to encrypt all production data stored in server infrastructure. **Payment Card and Banking Account Data Tokenization.** 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.
Data Security Incident Management and Notification	Stripe implements a data security incident management program that addresses how Stripe manages Incidents. Stripe will notify impacted Stripe users and Governmental Authorities (where applicable) of Incidents in a timely manner as required by DP Law.
Reviews, Audit Reports and Security Questionnaires	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.
System Configuration	Stripe implements measures for ensuring system configuration, including default configuration measures for internal IT and IT security governance. 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. Stripe uses monitoring tools to monitor production infrastructure for changes from known configuration baselines.
Data Portability	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 https://stripe.com/docs/security/data-migrations/exports.
Data Retention and Deletion	Stripe implements and maintains data retention policies and procedures related to Personal Data and reviews these policies and procedures as appropriate.

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

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.