Vereinbarung
über eine
Auftragsverarbeitung nach Art 28 DSGVO

Der Verantwortliche:

Der Auftragsverarbeiter:

Arivo GmbH
Am Innovationspark 10
8020 Graz
Österreich

(im Folgenden Auftraggeber)

(im Folgenden Auftragnehmer)

1. Gegenstand der Vereinbarung

(1) Gegenstand dieses Auftrages ist die Durchführung folgender Aufgaben:
Der Verantwortliche erhält den Zugang zur Parkraummanagement Software der Arivo GmbH. Die Software erfüllt die in der Dokumentation (https://docs.arivo.app) beschriebenen Funktionen und wird laufend erneuert und aktualisiert. Bei der Nutzung der Software können personenbezogene Daten verarbeitet werden. Diese Vereinbarung ist als Ergänzung zum Angebot von Arivo und den Software- und Servicebedingungen (https://arivo.co/software-service-bedingungen/).

(2) Folgende Daten werden verarbeitet:
Die verwendeten Daten können je nach verwendeten Produkten (Software Modulen) und Anwendungsfall unterschiedlich sein. Prinzipiell verarbeiten wir nur Daten, welche in der Applikation selbst eingeben werden oder durch das Benutzen des Produktes generiert werden.

- Kontaktdaten (Name, Telefon, E-Mail, Kundennummer, Adresse)
- Kommunikationsdaten
- Vertragsstammdaten und Buchungsdaten
- Kundenhistorie (Ein- und Ausfahrzeiten, Log-Daten)
- Vertragsabrechnungs- und Zahlungsdaten (Bankverbindungen, Rechnungen)
- Kennzeichendaten (Autokennzeichen, Automodell)

(3) Folgende Kategorien betroffener Personen unterliegen der Verarbeitung: Kunden, Lieferanten, Mitarbeiter, Eigentümer von Wohnbauten/ Garagen, Kunden, Besucher

2. Dauer der Vereinbarung

(1) Die Vereinbarung ist auf unbestimmte Zeit geschlossen und endet, wenn das Vertragsverhältnis zwischen Auftragnehmer und Auftraggeber endet oder eine neue Vereinbarung geschlossen wird. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt.

3. Haftung

(1) 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.

(2) Im Innenverhältnis haftet der Auftragsnehmer nur bei Vorsatz oder grober Fahrlässigkeit, wobei die Haftung für jegliche Schäden auf die Höhe der Betriebshaftpflichtversicherung maximal jedoch auf das 12 fache der monatlichen Softwareservicegebühr begrenzt ist, sofern gesetzlich keine für den Auftragsverarbeiter günstigere Regelung besteht.

(3) 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.

4. Pflichten des Auftragnehmers

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der Aufträge des Auftraggebers zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen.

(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (Einzelheiten sind der Anlage ./1 zu entnehmen).

(4) Der Auftragnehmer ergreift die technischen und organisatorischen Maßnahmen, damit der Auftraggeber die Rechte der betroffenen Person nach Kapitel III der DSGVO (Information, Auskunft, Berichtigung und Löschung, Datenübertragbarkeit, Widerspruch, sowie automatisierte Entscheidungsfindung im Einzelfall) innerhalb der gesetzlichen Fristen jederzeit erfüllen kann und überlässt dem Auftraggeber alle dafür notwendigen Informationen. Wird ein entsprechender Antrag an den Auftragnehmer gerichtet und lässt dieser erkennen, dass der Antragsteller ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenverarbeitung hält, hat der Auftragnehmer den Antrag unverzüglich an den Auftraggeber weiterzuleiten und dies dem Antragsteller mitzuteilen.

(5) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person, Datenschutz-Folgeabschätzung, vorherige Konsultation).

(6) Dem Auftraggeber wird hinsichtlich der Verarbeitung der von ihm überlassenen Daten das Recht jederzeitiger Einsichtnahme und Kontrolle, sei es auch durch von ihm beauftragte Dritte, eingeräumt. Der Auftragnehmer verpflichtet sich, dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der in dieser Vereinbarung genannten Verpflichtungen notwendig sind.

(7) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben. Wenn der Auftragnehmer die Daten in einem speziellen technischen Format verarbeitet, ist er verpflichtet, die Daten nach Beendigung dieser Vereinbarung entweder in diesem Format oder gängigen Format herauszugeben.

(8) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

5. Datenschutzanfragen

Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Sämtliche Anfragen zum Datenschutz können an die E-Mail-Adresse datenschutz@arivo.co gerichtet werden.

6. Ort der Durchführung der Datenverarbeitung

Die Verarbeitung personenbezogener Daten erfolgt innerhalb der EU/des EWR.

Sofern im Hauptvertrag die Nutzung des Zahlungsdienstleisters Stripe vereinbart wurde, kann die Verarbeitung personenbezogener Daten auch in den USA erfolgen. Das in diesem Staat gegeben Datenschutzniveau gilt aus folgendem Grund als angemessen:

- Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO (https://www.dataprivacyframework.gov/ https://commission.europa.eu/document/download/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en?filename=Adequacy%20decision%20EU-US%20Data%20Privacy%20Framework_en.pdf)

7. Sub-Auftragsverarbeiter

(1) Der Auftragnehmer ist befugt folgende Unternehmen als Sub-Auftragsverarbeiter hinzuziehen. Daten werden nur an den jeweiligen Subauftragnehmer übermittelt, sofern diese Subauftragnehmer zur Erfüllung entsprechende Funktionen (je nach Verwendung der Software) benötigt werden. Wenn z.B. keine SMS versendet werden, werden keine Daten an z.B. Websms übermittelt.

(2) Die Subauftraggeber erhalten nur die zur Erfüllung der jeweiligen Aufgaben benötigte Daten. Daher erhalten die Subauftraggeber nie Einsicht in die Gesamtheit der zur Verfügung gestellten Daten.

(3) Nach aktuellem Stand ist die Liste der Sub-Auftragsverarbeiter vollständig. Der Auftragnehmer hat den Verantwortlichen von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters nach Abschluss dieses Vertrages so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. Das Einspruchsrecht wird auf vier Wochen befristet. Wird innerhalb dieser Frist von dem Verantwortlichen kein begründeter Einspruch erhoben, so gilt die Zustimmung zur Heranziehung des Sub-Auftragsverarbeiters als erteilt. Wird ein Widerspruch eingelegt führt dies zur Beendigung des Vertragsverhältnisses.

(4) Der Auftragnehmer schließt die erforderlichen Vereinbarungen im Sinne des Art 28 Abs 4 DSGVO mit dem Sub-Auftragsverarbeiter ab. Dabei ist sicherzustellen, dass der Sub-Auftragsverarbeiter dieselben Verpflichtungen eingeht, die dem Auftragnehmer auf Grund dieser Vereinbarung obliegen. Kommt der Sub-Auftragsverarbeiter seinen Datenschutzpflichten nicht nach, so haftet der Auftragnehmer gegenüber dem Auftraggeber für die Einhaltung der Pflichten des Sub-Auftragsverarbeiters. Die Höhe der Haftung richtet sich nach Punkt 3 dieser Vereinbarung.

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 payment processing (only online payment) of the end customer. Only applies if charged are 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

Adyen	Payment Provider	Used for payment processing (online payment and POS payment) of the end customer. Only applies if charged are done with the Arivo system.	Adyen N.V Simon Carmiggeltstraat 6, 1011 DJ, Amsterdam NETHERLANDS https://www.adyen.com/policies-and-disclaimer/privacy-policy
Demondo	Debt Collection Service	Used for collection of unpaid parking fees.	Demondo GmbH & Co. KG Burgstraße 10 82418 Riegsee GERMANY https://www.demondo.com/en/legal/privacy-policy/
Easypark	Parking System	System for managing parking and other related services.	EasyPark Austria GmbH Gertrude-Fröhlich-Sandner-Straße 2 1100 Wie AUSTRIA https://www.easypark.com/en-de/privacy-policy
Parkster	Parking System	Pay for parking tickets cashlessly via mobile phone.	Parkster GmbH Lyonel-Feininger-Straße 28 80807 München GERMANY https://www.parkster.com/at/company/privacy/

, am

Graz, am

Für den Auftraggeber:

Für den Auftragnehmer:

Anlage ./1 – Technisch-organisatorische Maßnahmen Arivo

A. Gewährleistung der Vertraulichkeit

Zutrittskontrolle: Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

- Aufbewahrungsdauer Bildmaterial > 50 Tage
- Automatisches Zugangskontrollsystem
- Besucher nur in Begleitung durch Mitarbeiter
- Elektrische Türschlösser
- Gebäude befindet sich innerhalb eines Betriebsgeländes
- Gebäude ist ein reines Bürogebäude
- Manuelles Schließsystem
- Mechanische Türschlösser
- Sorgfalt bei der Auswahl des Reinigungspersonals
- Überwachter Eingangsbereich
- Videoüberwachung der Eingänge

Zugangskontrolle: Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können:

- Anti-Virus-Clients
- Anwendung einer 2-Faktor-Authentifikation
- Automatische Desktopsperre
- Einsatz einer Software-Firewall
- Erstanmeldeprozedur
- Erstellen von Benutzerprofilen
- Firewall
- Login mit Benutzername und Passwort
- Login mit Biometrischen Daten
- Mobile Device Management
- Richtlinie „Clean Desk“
- Richtlinie „Sicheres Passwort“
- Verschlüsselung von Datenträgern
- Verschlüsselung von Notebooks
- Verwalten von Benutzerberechtigungen
- Verwaltung der Rechte durch einen Systemadministrator
- Zuordnung von Benutzerrechten

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:

- Differenzierte Berechtigungen (Anwendungen)
- Differenzierte Berechtigungen (Betriebssystem)

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:

- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testumgebung
- Unterschiedliche Softwareprodukte bestehen auf voneinander getrennten Datenbank und Applikationsservern
- Videokameras in einem eigenen VLAN

B. Gewährleistung der Integrität

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:

- Bereitstellung über verschlüsselte Verbindungen wie sftp, https

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

- Technische Protokollierung der Änderung von Daten
- Technische Protokollierung der Eingabe von Daten
- Technische Protokollierung der Löschung von Daten

C. Verschlüsselung:

Verschlüsselung: Maßnahmen, die eine Verschlüsselung von Daten gewährleisten.

- Verschlüsselter Zugriff auf Server von Kunden
- Verschlüsselung des Transports von E-Mails
- Verschlüsselung von Datenträgern in Laptops / Notebooks
- Verschlüsselung von Systemen

D. Gewährleistung der Verfügbarkeit und Belastbarkeit und Wiederherstellbarkeit

Verfügbarkeit (der Daten): Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch:

- Tägliche Backups
- Firewall
- Security Checks auf Infrastruktur- und Applikationsebene
- Standardprozesse bei Wechsel / Ausscheiden von Mitarbeitern
- Datensicherheitskonzept vorhanden
- Datenverarbeitung über GCP (Google Cloud Plattform), daher folgende Maßnahmen gegeben
    - 99,95% Verfügbarkeit der Netzwerkanbindung

- 99,95% Verfügbarkeit der Server-Hardware
- SLA mit Hosting Dienstleister
- Unterbrechungsfreie Stromversorgung (USV)

Belastbarkeit (der Systeme): Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällig Zerstörung oder Verlust geschützt sind – Gewährleistung der Belastbarkeit der Systeme:

- Einsatz von Software Firewalls

Wiederherstellbarkeit (der Daten / der Systeme): Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind – Gewährleistung der Wiederherstellbarkeit von Daten und Systemen:

- Feuer- und Rauchmeldeanlagen
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums

E. Gewährleistung der Verfügbarkeit, Belastbarkeit und Wiederherstellbarkeit

Auftragskontrolle: Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können:

- Abschluss der notwendigen Auftragsdatenvereinbarungen
- Abschluss der notwendigen Standard-Vertragsklauseln
- Regelungen zum Einsatz von Subunternehmern
- Sicherstellung der Vernichtung von Daten nach Beendigung eines Auftrags
- Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
- Verpflichtung der Mitarbeiter des Auftragnehmers auf spezielle Geheimhaltungsvorschriften
- Bestellung eines Datenschutzbeauftragten
- Eindeutige Vertragsgestaltung
- Einhaltung der Informationspflichten gemäß Art. 13 DSGVO
- Einhaltung der Informationspflichten gemäß Art. 14 DSGVO
- Regelmäßige Sensibilisierung der Mitarbeiter zum Datenschutz
- Schulung der Mitarbeiter zum Datenschutz
- Verpflichtung der Mitarbeiter auf das Datengeheimnis

Incident-Response-Management: Maßnahmen, die gewährleisten, dass Sicherheitsvorfällen vorgebeugt werden kann oder im Falle von bereits eingetretenen Sicherheitsvorfällen, dass Daten und Systems geschützt werden können und eine schnelle Analyse und Behebung des Sicherheitsvorfalls durchgeführt werden kann:

- Dokumentation von Sicherheitsvorfällen
- Einsatz von Firewall und deren Aktualisierung
- Klare Regelung von Verantwortlichkeiten bei Sicherheitsvorfällen

Datenschutz-Management: Maßnahmen, die gewährleisten, dass Methoden evaluiert wurden, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, organisieren, steuern und kontrollieren:

- Bestellung eines internen Datenschutzbeauftragten
- Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz

Datenschutzfreundliche Voreinstellungen: Maßnahmen, die gewährleisten, dass bereits durch die entsprechende Technikgestaltung (privacy by design) und Werkseinstellungen (privacy by default) einer Software vorab ein gewisses Datenschutzniveau herrscht:

- Personenbezogene Daten werden nur zweckerforderlich erhoben