

Auftragsverarbeitungsvertrag

gemäß Art 28 DSGVO

1. Parteien

1.1. Verantwortlicher (bitte Daten befüllen):

Name oder Firma

Geburtsdatum oder Firmenbuch- / Handelsregisternummer

Adresse

1.2 Auftragsverarbeiter: App Radar Software GmbH, FN 442781z, Lastenstraße 13a, A-8020 Graz.

2. Gegenstand der Vereinbarung

2.1. Gegenstand dieses Auftrages ist die Durchführung der Verarbeitung personenbezogener Daten im Rahmen des Hauptvertrages zwischen dem Verantwortlichen und dem Auftragsverarbeiter. Der Auftragsverarbeiter stellt dem Verantwortlichen die vom Auftragsverarbeiter entwickelte App Radar Software als Software as a Service (SaaS) zur Verfügung. Im Rahmen dieser Software erhält der Auftragsverarbeiter Zugang zu Kundendaten des

Verantwortlichen welche die App des Verantwortlichen im Apple Store bzw. Google Play Store kaufen/nutzen/kommentieren. Diese Daten sind aktuell ausschließlich die Nicknamen/Benutzernamen von Usern , die die App des Verantwortlichen bewerten/reviewen. Durch die vom Auftragsverarbeiter zur Verfügung gestellte Software kann der Verantwortliche direkt auf Kommentare von Kunden zugreifen und diese beantworten.

2.2. Folgende Datenkategorien werden verarbeitet:

- Nicknames / Benutzernamen

2.3. Folgende Kategorien betroffener Personen unterliegen der Verarbeitung:

- Kunden

2.4. Die Verarbeitung umfasst grundsätzlich:

- Speicherung
- Auslesen / Abfragen
- Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung
- Abgleich oder Verknüpfung
- Einschränkung, Löschen oder Vernichtung von Daten

3. Dauer der Vereinbarung

3.1. Die Vereinbarung ist mit der Laufzeit des Hauptvertrages befristet.

3.2. Die Möglichkeit zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt, in diesem Fall gilt dies auch als Kündigung des Hauptvertrages.

4. Pflichten des Auftragnehmers

4.1. Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen der schriftlichen Aufträge des Auftraggebers zu verarbeiten. Der Abschluss eines Vertrages über die Erbringung von SaaS-Leistungen gilt als solcher schriftlicher Auftrag. 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. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

- 4.2.** 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.
- 4.3.** Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat (siehe **Anlage ./1**).
- 4.4.** 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.
- 4.5.** 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-Folgenabschätzung, vorherige Konsultation).
- 4.6.** Der Auftragnehmer wird darauf hingewiesen, dass er für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art 30 DSGVO zu errichten hat.
- 4.7.** 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, der

Datenverarbeitungseinrichtungen 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.

- 4.8.** Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben / in dessen Auftrag zu vernichten . 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 nach Wunsch des Auftraggebers in dem Format, in dem er die Daten vom Auftraggeber erhalten hat oder in einem anderen, gängigen Format herauszugeben.
- 4.9.** 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.
- 4.10.** Im Übrigen gelten die Allgemeinen Geschäftsbedingungen des Auftragnehmers analog.

5. Ort der Durchführung der Datenverarbeitung

- 5.1.** Alle Datenverarbeitungstätigkeiten werden derzeit ausschließlich innerhalb der EU bzw des EWR durchgeführt.
- 5.2.** Sofern in Zukunft Datenverarbeitungstätigkeiten, wenn auch nur teilweise, außerhalb der EU/des EWR} durchgeführt werden, wird der Auftragnehmer für das angemessene Datenschutzniveau Sorge tragen. Dieses hat sich dann zu ergeben aus (und/oder):
- einem Angemessenheitsbeschluss der Europäischen Kommission nach Art 45 DSGVO.
 - einer Ausnahme für den bestimmten Fall nach Art 49 Abs 1 DSGVO.
 - verbindlichen internen Datenschutzvorschriften nach Art 47 iVm Art 46 Abs 2 lit b DSGVO
 - Standarddatenschutzklauseln nach Art 46 Abs 2 lit c und d DSGVO.
 - genehmigten Verhaltensregeln nach Art 46 Abs 2 lit e iVm Art 40 DSGVO.
 - einen genehmigten Zertifizierungsmechanismus nach Art 46 Abs 2 lit f iVm Art 42 DSGVO

- von der Datenschutzbehörde bewilligte Vertragsklauseln nach Art 46 Abs 3 lit a DSGVO
- einer Ausnahme für den Einzelfall nach Art 49 Abs 1 Unterabsatz 2 DSGVO.


6. Sub-Auftragsverarbeiter

- 6.1.** Der Auftragnehmer kann Sub-Auftragsverarbeiter hinzuziehen.
- 6.2.** Er hat den Auftraggeber von der beabsichtigten Heranziehung eines Sub-Auftragsverarbeiters so rechtzeitig zu verständigen, dass er dies allenfalls untersagen kann. 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.

Unterschriftenseite folgt

Für den Verantwortlichen:

Für den Auftragsverarbeiter:



Name

Thomas Kriebner, CEO



Position

Silvio Peruci, COO

Unterschrift

ANLAGE ./1

Technisch-Organisatorische Massnahmen

Der Auftragsverarbeiter trifft geeignete technische und organisatorische Massnahmen, um ein dem Risiko angemessenes Schutzniveau im Hinblick auf die erforderliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer zu gewährleisten.

Die Parteien haben das erforderliche Schutzniveau gemeinsam ermittelt (Art. 32 Abs. 1 DSGVO). Die Parteien sind zu dem Ergebnis gekommen, dass das Risiko der Verarbeitung als „hoch“ einzustufen ist und daher auch ein hohes Schutzniveau einzuhalten ist.

Das hohe Schutzniveau wird durch diese Massnahmen eingehalten:

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle

Kein unbefugter Zutritt zu Datenverarbeitungsanlagen. Das Office ist mit Schlüsseln versperrbar. Zugang zu physischen Servern ist nur durch Biometrische Sicherheitssysteme möglich.

Zugangskontrolle

Keine unbefugte Systemnutzung. Daten sind nur durch Accounts mit sicheren Kennwörtern und entsprechender Freigabe zugänglich.

Zugriffskontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen und Modifikationen (volle Versionierung);

Trennungskontrolle

Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden, z.B. Mandantenfähigkeit, Sandboxing;

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

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;

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur;

Eingabekontrolle

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement;

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle

Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust, z.B.: [A5] Backup-Strategie (online/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne;

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Datenschutz-Management;

Incident-Response-Management;

Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);

Auftragskontrolle

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.