Auftrag zur Verarbeitung personenbezogener Daten

Gemäß Art. 28 Abs. 3 S. 1 DSGVO

– nachstehend bezeichnet als **AV-Vertrag** –

zwischen (der)

Name / Firma:
Musterfirma
Vertreten durch:
Max Mustermann
Anschrift:
Schönbrunnerstrasse 1 - 1130 Wien - Österreich

– nachstehend bezeichnet als **Auftraggeber** –

und der

Name / Firma:
QR Planet GmbH
Vertreten durch:
Peter Hlavac
Anschrift:
Mariahilfer Straße 7/2
1060 Wien
Österreich

– nachstehend bezeichnet als **Auftragnehmer** –

– Auftragnehmer und Auftraggeber werden nachstehend auch als **Vertragsparteien** bezeichnet. –

Anlagen:

- Anhang 1: Sicherheitskonzept
- Anhang 2: Unterauftragsverhältnisse

1.
Gegenstand des Auftrags, Datenkategorien, Betroffene, Art, Umfang und Zwecksetzung der Verarbeitung (Art. 28 Abs. 3, 30 Abs. 2 DSGVO)

1.1

Der Gegenstand des AV-Vertrages, die im Rahmen des Auftrags verarbeiteten personenbezogenen Daten (Art, 4 Nr. 1 DSGVO; nachfolgend kurz **„Daten“**), die von der Verarbeitung betroffenen Personen (nachfolgend kurz **„Betroffene“**) sowie Art, Umfang und Zwecke der Verarbeitung, werden durch die folgenden Rechtsbeziehung(en) zwischen den Vertragsparteien bestimmt (nachstehend bezeichnet als **Hauptvertrag**):

Vertrag über die Nutzung der Software (Software as a Service) *QR Planet GmbH* auf Grundlage der AGB des Auftragnehmers.

Die Regelungen dieses AV-Vertrages gelten gegenüber dem Hauptvertrag vorrangig.

1.2

Art der Daten:

- Kundenstammdaten (Firmenname, Ansprechpartner, Anschrift, UmsatzStNr. , E-Mailadresse)
- Benutzer- und Accountdaten (Name, E-Mailadresse, kryptografischer Hash des Passworts)
- Zahlungsdaten (Kontodaten und/oder Kreditkartendaten)
- Vertragsdaten (Art der Leistung, Entgelt, Laufzeit, Vertragshistorie), Zahlungshistorie)
- Inhaltsdaten, die selbst von Kunden/ Nutzern in *QR Planet GmbH* eingegeben werden (QR Codes, Landing Pages)
- Nutzungsdaten/ Metadaten (Server-Logging, IP-Adresse, User Agent, Requestparameter, Zeitstempel)

1.3

Verarbeitung besonderer Kategorien von Daten (Art. 9 Abs. 1 DSGVO):

- Es werden grundsätzlich keine besonderen Kategorien von Daten verarbeitet, außer diese werden durch den Auftraggeber eingegeben

1.4

Kategorien der Betroffenen:

- Kunden, Nutzer, Geschäftspartner des Auftraggebers
- Beschäftigte des Auftraggebers

1.5

Zweck der Verarbeitung:

- Angebot und Betrieb von *QR Planet GmbH* (Software as a Service) und verbundener Leistungen (Rechenkapazitäten, Datenbanken, Software, Pflege und Entwicklung).

2.

Verantwortlichkeit und Weisungsrecht

2.1

Der Auftraggeber ist als Verantwortlicher gem. Art. 4 Nr. 7 DSGVO für die Einhaltung der datenschutzrechtlichen Vorgaben, insbesondere für die Auswahl des Auftragnehmers, die an diesen übermittelten Daten sowie erteilte Weisungen verantwortlich (Art. 28 Abs. 3 lit. a, 29 u. 32 Abs. 4 DSGVO).

2.2

Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrages sowie der Weisungen des Auftraggebers verarbeiten (was insbesondere auch für deren Berichtigung, Löschung oder Einschränkung der Verarbeitung gilt) und nur insoweit die Verarbeitung hierzu erforderlich ist, außer wenn der Auftragnehmer zu der Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 S. 2 lit. a DSGVO).

2.3

Der Auftraggeber hat das Recht, jederzeit ergänzende Weisungen im Hinblick auf die Verarbeitung der Daten und die Sicherheitsmaßnahmen zu erteilen.

2.4

Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen geltendes Datenschutzrecht verstößt, wird er den Auftraggeber unverzüglich darauf hinweisen. In diesem Fall ist der Auftragnehmer berechtigt, die Ausführung der Weisung bis zur Bestätigung der Weisung durch den Auftraggeber auszusetzen und im Fall offensichtlich rechtswidriger Weisungen abzulehnen.

2.5

Der Auftragnehmer kann Weisungen ablehnen, sofern diese dem Auftragnehmer nicht möglich oder nicht zuzumuten sind (insbesondere, weil deren Befolgung ein unverhältnismäßiger Aufwand oder fehlende technische Möglichkeiten entgegenstehen). Die Ablehnung kann nur unter sachgerechter Berücksichtigung des Schutzes der Daten der Betroffenen erfolgen und berechtigt den Auftraggeber zur außerordentlichen Kündigung des AV-Vertrages, wenn dessen Fortsetzung dem Auftraggeber nicht zuzumuten ist.

2.6

Die Vertragsparteien können zum Erteilen und Empfangen von Weisungen berechtigte Personen benennen (insbesondere, wenn diese sich nicht bereits aus dem Hauptvertrag ergeben) und sind verpflichtet deren Änderung unverzüglich mitzuteilen.

3.

Sicherheitskonzept und diesbezügliche Pflichten

3.1

Der Auftragnehmer wird die innerbetriebliche Organisation in seinem Verantwortungsbereich entsprechend den gesetzlichen Anforderungen gestalten und wird insbesondere technische und organisatorische Maßnahmen (nachfolgend bezeichnet als **„TOMs“**) zur angemessenen Sicherung, insbesondere der Vertraulichkeit, Integrität und Verfügbarkeit von Daten des Auftraggebers, unter Beachtung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen treffen sowie deren Aufrechterhaltung sicherstellen (Art. 28 Abs. 3 u. 32 - 39 i.V.m. Art 5 DSGVO). Zu den TOMs gehören insbesondere die Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennungskontrolle und die Sicherung der Betroffenenrechte.

3.2

Die diesem AV-Vertrag zugrundeliegenden TOMs ergeben sich aus dem **Anhang 1 „Sicherheitskonzept“**. Sie dürfen entsprechend dem technischen Fortschritt weiterentwickelt und durch adäquate Schutzmaßnahmen ersetzt werden, sofern sie das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschreiten und wesentliche Änderungen dem Auftraggeber mitgeteilt werden.

3.3

Der Auftragnehmer stellt sicher, dass die zur Verarbeitung der Daten des Auftraggebers befugten Personen auf Vertraulichkeit und Verschwiegenheit (Art. 28 Abs. 3 S. 2 lit. b und 29, 32 Abs. 4 DSGVO) verpflichtet und in die Schutzbestimmungen der DSGVO eingewiesen worden sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

3.4

Die im Rahmen des AV-Vertrages überlassene Daten sowie Datenträger und sämtliche hiervon gefertigten

Kopien verbleiben im Eigentum des Auftraggebers, sind durch den Auftragnehmer sorgfältig zu verwahren, vor Zugang durch unberechtigte Dritte zu schützen und dürfen nur mit Zustimmung des Auftraggebers, und dann nur datenschutzgerecht, vernichtet werden. Kopien von Daten dürfen nur erstellt werden, wenn sie zur Erfüllung der Leistungshaupt- und Nebenpflichten des Auftragnehmers gegenüber dem Auftragnehmer erforderlich sind (z.B. Backups).

3.5

Sofern durch die DSGVO oder ergänzende, insbesondere nationale Vorschriften, vorgegeben, benennt der Auftragnehmer eine/n den gesetzlichen Vorgaben entsprechende/n Datenschutzbeauftragte/n und informiert den Auftraggeber entsprechend (Art. 37 bis 39 DSGVO).

4.

Informationspflichten und Mitwirkungspflichten

4.1

Betroffenenrechte sind gegenüber dem Auftraggeber wahrzunehmen, wobei der Auftragnehmer den Auftraggeber hierbei gem. Art. 28 Abs. 3 S. 2 lit. e. DSGVO unterstützt und ihn insbesondere über die bei ihm eingehenden Anfragen Betroffener informiert.

4.2

Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er im Hinblick auf die Verarbeitung der Daten Fehler oder Unregelmäßigkeiten im Hinblick auf die Einhaltung der Bestimmungen dieses AV-Vertrages oder einschlägiger Datenschutzvorschriften feststellt.

4.3

Für den Fall, dass der Auftragnehmer Tatsachen feststellt, welche die Annahme begründen, dass der Schutz der für den Auftraggeber verarbeiteten Daten verletzt worden ist, hat der Auftragnehmer den Auftraggeber unverzüglich und vollständig zu informieren, unverzüglich erforderliche Schutzmaßnahmen zu ergreifen, und bei der Erfüllung der dem Auftraggeber obliegenden Pflichten gem. Art. 33 und 34 DSGVO zu unterstützen.

4.4

Sollte die Sicherheit der Daten des Auftraggebers durch Maßnahmen Dritter (z.B. Gläubiger, Behörden, Gerichte, etc.) gefährdet sein (Pfändung, Beschlagnahme, Insolvenzverfahren, etc.) wird der Auftragnehmer die Dritten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich bei dem Auftraggeber liegen und nach Rücksprache mit dem Auftraggeber, sofern erforderlich, entsprechende Schutzmaßnahmen ergreifen (z.B. Widersprüche, Anträge, etc. stellen).

4.5

Der Auftragnehmer wird den Auftraggeber unverzüglich darüber informieren, wenn eine Aufsichtsbehörde gegenüber dem Auftragnehmer tätig wird und deren Tätigkeit die für den Auftragnehmer verarbeiteten Daten betreffen kann. Der Auftragnehmer unterstützt den Auftraggeber bei der Wahrnehmung seiner Pflichten (insbesondere zur Auskunfts- und Duldung von Kontrollen) gegenüber Aufsichtsbehörden (Art. 31 DSGVO).

4.6

Der Auftragnehmer stellt dem Auftraggeber Informationen betreffend die Verarbeitung von Daten im

Rahmen dieses AV-Vertrages, die für dessen Erfüllung von gesetzlichen Pflichten (zu denen insbesondere Anfragen Betroffener oder Behörden und die Einhaltung seiner Rechenschaftspflichten gem. Art. 5 Abs. 2 DSGVO, als auch die Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO gehören können) notwendig sind, zur Verfügung, sofern der Auftraggeber diese Informationen nicht selbst beschaffen kann. Die Informationen müssen dem Auftragnehmer zur Verfügung stehen und müssen nicht von Dritten beschafft werden, wobei Mitarbeiter, Beauftragte und Subunternehmer des Auftraggebers nicht als Dritte gelten.

4.7

Gehen die Zurverfügungstellung der notwendigen Informationen und die Mitwirkung über die Leistungspflicht des Auftragnehmers nach dem Hauptvertrag hinaus und beruhen sie nicht auf einem Fehlverhalten des Auftragnehmers, hat der Auftraggeber dem Auftragnehmer den dadurch entstehenden Mehraufwand gesondert zu vergüten.

5.

Kontrollbefugnisse

5.1

Der Auftraggeber hat das Recht, die Einhaltung der gesetzlichen Vorgaben und der Regelungen dieses AV-Vertrages, insbesondere der TOMs beim Auftragnehmer jederzeit im erforderlichen Umfang zu kontrollieren (Art. 28 Abs. 3 lit. h DSGVO).

5.2

Vor-Ort-Kontrollen erfolgen innerhalb üblicher Geschäftszeiten, sind vom Auftraggeber mit einer angemessenen Frist (mindestens 14 Tage, außer in Notfällen) anzumelden und durch den Auftragnehmer zu unterstützen (z.B. durch Bereitstellung von Personal).

5.3

Die Kontrollen sind auf den erforderlichen Rahmen beschränkt und müssen auf Betriebs- und Geschäftsgeheimnisse des Auftragnehmers sowie den Schutz von personenbezogenen Daten Dritter (z.B. anderer Kunden oder Mitarbeiter des Auftragnehmers) Rücksicht nehmen. Zur Durchführung der Kontrolle sind nur fachkundige Personen zugelassen, die sich legitimieren können und im Hinblick auf die Betriebs- und Geschäftsgeheimnisse sowie Prozesse des Auftragnehmers und personenbezogene Daten Dritter zur Verschwiegenheit verpflichtet sind.

5.4

Geht die Duldung und Mitwirkung bei den Kontrollen, bzw. adäquaten Alternativmaßnahmen des Auftraggebers über die Leistungspflicht des Auftragnehmers nach dem Hauptvertrag hinaus und beruhen sie nicht auf einem Fehlverhalten des Auftragnehmers, dann hat der Auftraggeber dem Auftragnehmer den dadurch entstehenden Mehraufwand gesondert zu vergüten.

6.

Unterauftragsverhältnisse

6.1

Nimmt der Auftragnehmer die Dienste eines Unterauftragsverarbeiters (d.h. Unterauftragnehmer oder Subunternehmer) in Anspruch, um bestimmte Verarbeitungstätigkeiten im Namen des Auftraggebers auszuführen, dann muss er dem Unterauftragsverarbeiter im Wege eines Vertrags oder eines nach der DSGVO zulässigen anderen Rechtsinstruments dieselben Datenschutzpflichten zu denen sich der Auftragnehmer in diesem AV-Vertrag verpflichtet hat, auferlegen (insbesondere im Hinblick auf die

Befolgung von Weisungen, Einhaltung der TOMs, Erteilung von Informationen und Duldung von Kontrollen). Ferner hat der Auftragnehmer den Unterauftragsverarbeiter sorgfältig auszuwählen, auf dessen Zuverlässigkeit zu prüfen und diese, als auch dessen Einhaltung der vertraglichen und gesetzlichen Vorgaben zu überwachen (Art. 28 Abs. 2 u. 4 DSGVO).

6.2

Im Rahmen der Auftragsverarbeitung dürfen Unterauftragsverarbeiter vom Auftragnehmer nur mit schriftlicher Zustimmung des Auftraggebers beauftragt werden.

6.3

Die bereits zum Abschluss dieses AV-Vertrages bestehenden Unterauftragsverhältnisse, werden vom Auftragnehmer im Anhang 2 „Unterauftragsverhältnisse“ angegeben und gelten vom Auftragnehmer als genehmigt.

6.4

Der Auftragnehmer informiert den Auftraggeber rechtzeitig im Hinblick auf Änderungen bei den Unterauftragsverarbeitern, die für die Auftragsverarbeitung maßgeblich sind. Der Auftraggeber macht von seinem Recht auf Einspruch im Hinblick auf die Änderungen oder neue Unterauftragsverarbeiter nur unter Beachtung der Grundsätze von Treu und Glauben sowie der Angemessenheit und Billigkeit Gebrauch.

6.5

Vertragsverhältnisse, bei denen der Auftragnehmer die Leistungen Dritter als reine Nebenleistung in Anspruch nimmt, um seine geschäftliche Tätigkeit auszuüben (z.B. Reinigungs-, Bewachungs- oder Transportleistungen) stellen keine Unterauftragsverarbeitung im Sinne der vorstehenden Regelungen dieses AV-Vertrages dar. Gleichwohl hat der Auftragsverarbeiter sicher zu stellen, z.B. durch vertragliche Vereinbarungen oder Hinweise und Instruktionen, dass hierbei die Sicherheit der Daten nicht gefährdet wird und die Vorgaben dieses AV-Vertrages und der Datenschutzvorschriften eingehalten werden.

7.

Verarbeitung in Drittländern

7.1

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum (EWR) statt.

7.2

Die Auftragsverarbeitung in einem Drittland, auch durch Unterauftragsverarbeiter, bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, außer wenn der Auftragnehmer zu der Verarbeitung im Drittland durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragnehmer unterliegt, verpflichtet ist; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 S. 2 lit. a DSGVO).

7.3

Die Zustimmung des Auftraggebers zur Verarbeitung im Drittland, gilt im Hinblick auf die im Anhang 2

„Unterauftragsverhältnisse“ genannten Verarbeitungen als erteilt.

8.

Dauer des Auftrags, Vertragsbeendigung und Datenlöschung

8.1

Dieser AV-Vertrag wird mit dessen Abschluss gültig, wird auf unbestimmte Zeit geschlossen und endet spätestens mit der Laufzeit des Hauptvertrags.

8.2

Das Recht auf außerordentliche Kündigung bleibt den Vertragsparteien vorbehalten, insbesondere im Fall eines schwerwiegenden Verstoßes gegen die Vorgaben dieses AV-Vertrages und geltendes Datenschutzrecht.

8.3

Nach Abschluss der Erbringung der Verarbeitungsleistungen im Rahmen dieses AV-Vertrages, wird der Auftragnehmer alle personenbezogenen Daten und deren Kopien (sowie sämtliche im Zusammenhang mit dem Auftragsverhältnis in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände), nach Wahl des Auftraggebers entweder löschen oder zurückgeben, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht (Art. 28 Abs. 1 S. 2 lit. g DSGVO). Die Einrede eines Zurückbehaltungsrechts, wird hinsichtlich der verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen. Im Hinblick auf die Löschung oder Rückgabe, gelten die Auskunfts-, Nachweis und Kontrollrechte des Auftraggebers entsprechend diesem AV-Vertrag.

8.4

Im Übrigen bleiben die Verpflichtungen aus diesem AV-Vertrag im Hinblick auf die im Auftrag verarbeiteten Daten auch nach Beendigung des AV-Vertrages bestehen.

8.5

Gehen die Löschung bzw. die Rückgabe der Daten über die Leistungspflicht des Auftragnehmers nach dem Hauptvertrag hinaus und beruhen sie nicht auf einem Fehlverhalten des Auftragnehmers, dann hat der Auftraggeber dem Auftragnehmer den dadurch entstehenden Mehraufwand gesondert zu vergüten.

9.

Vergütung

9.1

Der Auftraggeber kann sich jederzeit vor der Aufnahme der Datenverarbeitung und sodann regelmäßig, aber maximal einmal pro Jahr oder im Anlassfall eines Datendiebstahls oder Datenmissbrauches von den technischen und organisatorischen Maßnahmen des Auftragsverarbeiters überzeugen. Für die Durchführung einer Prüfung darf der Auftragnehmer eine dem Aufwand entsprechende Vergütung verlangen. Die nach diesem AV-Vertrag vereinbarte Vergütung umfasst auch eine Aufwandsentschädigung für die Arbeitszeit des vom Auftragnehmer beanspruchten Personals sowie erforderliche Auslagen (z.B. Reise- oder Materialkosten). Sofern möglich, absehbar und zumutbar, teilt der Auftragnehmer dem Auftraggeber die Höhe der Vergütung im Wege einer sachgerechten Schätzung mit.

9.2

Sofern dem Auftragnehmer eine Vergütung nach Maßgabe dieses AV-Vertrages zusteht, wird diese mit einem Stundensatz von 140,00 EUR netto berechnet. Im Übrigen gelten die Vergütungsregelungen des Hauptvertrages.

10.

Haftung

10.1

Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde. Ein Auftragsverarbeiter haftet für den durch eine Verarbeitung verursachten Schaden nur dann, wenn er seinen speziell den Auftragsverarbeitern auferlegten Pflichten aus dieser Verordnung nicht nachgekommen ist oder unter Nichtbeachtung der rechtmäßig erteilten Anweisungen des für die Datenverarbeitung Verantwortlichen oder gegen diese Anweisungen gehandelt hat.

10.2

Der Verantwortliche oder der Auftragsverarbeiter wird von der Haftung gemäß Absatz 1 befreit, wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist.

11.

Schlussbestimmungen, Rangfolge, Änderungen, Kommunikationsform, Rechtswahl, Gerichtsstand

11.1

Änderungen, Nebenabreden und Ergänzungen dieses AV-Vertrages und seiner Anhänge bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieses AV-Vertrages handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

11.2

Dieser AV-Vertrag verpflichtet den Auftragnehmer nur insoweit, als dies zur Erfüllung der gesetzlichen Pflichten, insbesondere nach Art. 28 ff. DSGVO erforderlich ist und legt dem Auftragnehmer darüber hinaus keine weiteren Pflichten auf.

11.3

Vorbehaltlich einer Verpflichtung zur Schriftform in diesem AV-Vertrag und im Hauptvertrag, erfolgt die Kommunikation zwischen dem Auftragnehmer und Auftraggeber im Rahmen dieses AV-Vertrages (insbesondere im Hinblick auf Weisungen und Informationserteilung) zumindest in Textform (z.B. E-Mail). Eine geringere Form (z.B. mündlich) kann den Umständen nach statt der Textform zulässig sein (z.B. in Notfallsituation), muss jedoch unverzüglich zumindest in Textform bestätigt werden. Sofern die Schriftform verlangt wird, ist die Schriftform im Sinne der DSGVO gemeint.

11.4

Es gilt das Recht der Bundesrepublik Österreich. Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AV-Vertrag ist der Sitz des Auftragnehmers, sofern der Aufraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist oder der Aufraggeber in der Bundesrepublik Österreich keinen Gerichtsstand hat. Der Auftragnehmer behält sich vor, seine Ansprüche an dem gesetzlichen Gerichtsstand geltend zu machen.

Wien, 09.05.2024, Max Mustermann

Ort, Datum, Auftraggeber

Wien, 09.05.2024

Ort, Datum, Auftragnehmer

Auftrag zur Verarbeitung personenbezogener Daten

Anhang 1 – Sicherheitskonzept

Technische und Organisatorische Maßnahmen gem. Art. 32 DSGVO

1.

Datenschutzkonzept, Betroffenenrechte, Technikgestaltung und Datenschutz auf Mitarbeiterebene

Grundsätzliche Maßnahmen, die der Wahrung der Betroffenenrechte, unverzüglichen Reaktion in Notfällen, den Vorgaben der Technikgestaltung und dem Datenschutz auf Mitarbeiterebene dienen:

- Es besteht ein betriebsinternes Datenschutz-Management, dessen Einhaltung ständig überwacht wird sowie anlassbezogenen und mindestens halbjährlichen evaluiert wird.
- Es besteht ein Konzept, welches die Wahrung der Rechte der Betroffenen (Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung, Datentransfer, Widerrufe & Widersprüche) innerhalb der gesetzlichen Fristen gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen.
- Es besteht ein Konzept, das eine unverzügliche und den gesetzlichen Anforderungen entsprechende Reaktion auf Verletzungen des Schutzes personenbezogener Daten (Prüfung, Dokumentation, Meldung) gewährleistet. Es umfasst Formulare, Anleitungen und eingerichtete Umsetzungsverfahren sowie die Benennung der für die Umsetzung zuständigen Personen
- Der Schutz von personenbezogenen Daten wird unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen bereits bei der Entwicklung, bzw. Auswahl von Hardware, Software sowie Verfahren, entsprechend dem Prinzip des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen berücksichtigt (Art. 25 DSGVO).
- Die eingesetzte Software wird stets auf dem aktuell verfügbaren Stand gehalten, ebenso wie Virenscanner und Firewalls.
- Das Reinigungspersonal, Wachpersonal und übrige Dienstleister, die zur Erfüllung nebengeschäftlicher Aufgaben herangezogen werden, werden sorgfältig ausgesucht und es wird sichergestellt, dass sie den Schutz personenbezogener Daten beachten.

2.

Zutrittskontrolle

Maßnahmen, mit denen Unbefugten der Zugang zu Datenverarbeitungsanlagen, mit denen

personenbezogene Daten verarbeitet oder genutzt werden, verwehrt wird:

- Es wird ein „papierloses Büro“ geführt und Unterlagen werden grundsätzlich nur digital gespeichert und nur in Ausnahmefällen in Papierform aufbewahrt.
- Es werden, bis auf die Arbeitsplatzrechner und mobile Geräte, keine Datenverarbeitungsanlagen in den eigenen Geschäftsräumlichkeiten unterhalten. Die Daten des Auftraggebers werden bei externem Hosting-Anbieter unter Beachtung der Vorgaben für Auftragsverarbeitung gespeichert.
- Serverstandort: Elektronisches Zugangskontrollsystem (persönlicher Transponder, Einteilung in Zonen, Onboarding-Prozess, elektrischer Türöffner an der Eingangstür und selbstschließende Außentüren, im Rechenzentrum zusätzlich Vereinzelungsschleuse und Alarm bei nicht geschlossenen Türen)
- Serverstandort: Spezifische Zugangsregelungen für Personengruppen (Anmeldung von Besuchern beim Empfang, Begleitung von Besuchern durch interne Mitarbeiter, im Rechenzentrum zusätzlich Zutritt nach vorheriger namentlicher Anmeldung sowie verschlossene Serverräume mit Zutrittsberechtigung nur für autorisiertes Personal
- Serverstandort: Überwachungs- und Alarmsystem (Verwendung einer Alarmanlage und Aufschalten von Wachschutz, bei Alarm erfolgt Überwachung durch Wachschutz vor Ort, im Rechenzentrum zusätzlich Videoüberwachung der Flure durch dessen Betreiber)

3.

Zugangskontrolle

Maßnahmen, mit denen die Nutzung von Datenverarbeitungssystemen durch Unbefugte verhindert wird:

- Es gibt ein Rechtekonzept bzw. ein Rollenkonzept, mit dem die Zutrittsberechtigungen der Mitarbeiter, Beauftragten und sonstigen Personen (z.B. Nutzer innerhalb des Systems) festgelegt werden und nur soweit reichen, wie sie für die vorgegebene Nutzung erforderlich sind.
- Sämtliche Datenverarbeitungsanlagen sind passwortgeschützt.
- Es gibt ein Passwortkonzept, das festlegt, dass Passwörter eine dem Stand der Technik und den Anforderungen an Sicherheit entsprechende Mindestlänge und Komplexität haben müssen.
- Anmeldungen in den Verarbeitungssystemen werden protokolliert.
- Es wird, sofern systembedingt erforderlich/ Stand der Technik entsprechend, eine Anti-Viren-Software eingesetzt.
- Es werden Hardware-Firewalls eingesetzt.
- Es werden Software-Firewalls eingesetzt.
- Die Website und/oder Zugänge zu Online-Software-Angeboten sind durch eine aktuelle TLS/SSL-Verschlüsselung geschützt.
- Die internen Systeme werden per Firewall sowie Benutzername und Passwort und/oder Client-Zertifikate vor unberechtigten Zugriffen geschützt.
- Es gibt eine Begrenzung der Fehlversuche beim Login auf betriebsinterne Systeme (z.B. Sperrung von Logins oder IP-Adressen).
- Soweit technisch unterstützt, wird die Zwei-Faktor-Authentifizierung genutzt.
- Es werden Serversysteme und Dienste eingesetzt, die über Intrusion-Detection-Systeme verfügen.
- Serverstandort: Zugang zu internen Systemen wird durch Firewall- bzw. VPN-Systeme beschränkt
- Serverstandort: Verschlüsselungstechniken werden eingesetzt, um Benutzerauthentifizierungen und Administrationsprozesse über das Internet abzusichern
- Serverstandort: Der Datenfernzugriff auf Produktionsmaschinen benötigt eine Verbindung zum Firmennetzwerk, die durch VPN-Systeme gesichert wird.
- Serverstandort: Es besteht ein formaler Prozess, um den Zugang zu Ressourcen zu erlauben oder zu verweigern. Verschiedene Zugangsschutzmechanismen helfen dabei, sichere und flexible Zugriffe bereitzustellen.
- Serverstandort: Die Erteilung oder Änderung von Zugangsrechten erfolgt auf Grundlage eines Berechtigungskonzepts.

4.

Zugriffskontrolle und Eingabekontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten

ausschließlich auf die ihrer Zugangsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt, eingegeben, gelesen, kopiert, verändert oder entfernt werden können sowie Maßnahmen, die es erlauben die Verarbeitungsvorgänge nachträglich nachzuvollziehen:

- Es gibt ein Rechtekonzept bzw. ein Rollenkonzept, mit dem die Zugriffsberechtigungen der Mitarbeiter, Beauftragten und sonstigen Personen (z.B. Nutzer innerhalb des Systems) festgelegt werden und nur soweit reichen, wie sie für die vorgegebene Nutzung erforderlich sind.
- Protokollierung jedes einzelnen Schrittes der Datenverarbeitung, insbesondere von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten.
- Die Zugriffe der Mitarbeiter auf Daten werden protokolliert. Sofern einzelne Zugriffe nicht protokolliert werden, wird sichergestellt, dass nachvollziehbar ist, wer auf welche Daten wann Zugriff hatte (z.B. durch Protokollierung der Softwarenutzung oder Rückschluss aus den Zugriffszeiten und dem Berechtigungskonzept).
- Datenträger werden sicher aufbewahrt.
- Es liegt ein Lösch- und Entsorgungskonzept entsprechend der DIN 66399 mit festgelegten Zuständigkeiten und Protokollierungspflichten vor. Mitarbeiter wurden über gesetzliche Voraussetzungen, Löschfristen und Vorgaben für die Datenvernichtung oder Gerätevernichtung durch Dienstleister unterrichtet.
- Die Verarbeitung von Daten, die nicht gelöscht werden (z.B. in Folge der gesetzlichen Archivierungspflichten), wird durch Sperrvermerke und Aussonderung eingeschränkt.
- Serverstandort: Zugriff durch personalisierte Accounts auf Basis eines Berechtigungskonzepts
- Serverstandort: Zugriffe werden protokolliert
- Serverstandort: Zur Eingabekontrolle werden System- und Anwendungslogfiles gespeichert und administrative Tätigkeiten aufgezeichnet (Protokollierung)

5.

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:

- Es werden die für die Abgabe von Datenträgern berechtigten Personen und die Empfangsberechtigten bestimmt.
- Im Fall des physischen Transports werden sichere Transportbehälter oder Transportverpackungen gewählt bzw. die Sicherheit der Daten durch eine persönliche Aufsicht gewährleistet, sofern diese angesichts der für die Daten bestehenden Gefahren ausreichend ist.
- Im Fall des Fernzugriffs auf Daten wird durch Protokollmaßnahmen gesichert, dass Datenübermittlungen oder Offenlegungen nachvollziehbar sind.
- Sofern erforderlich, möglich und zumutbar, werden Daten in anonymisierter Form bzw. in pseudonymisierter Form weitergegeben.
- Es wird eine E-Mail-Verschlüsselung eingesetzt, sofern diese möglich, zumutbar und vom Kommunikationspartner gewünscht oder sonst als erforderlich und/oder angemessen zu betrachtet ist.

6.

Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen von Auftraggebern verarbeitet werden können:

- Verpflichtung von Mitarbeitern und Beauftragten auf die Beachtung von Weisungen.
- Schriftliche Festlegung und Dokumentation der Weisungen.
- Die vertraglichen und gesetzlichen Vorgaben für die Beauftragung von Unterauftragsverarbeitern werden durch Abschluss von AV-Verträgen und Sicherstellung notwendiger Garantien sowie deren Kontrolle beachtet.

- Es wird sichergestellt, dass Daten nach Beendigung des Auftrags zurückgegeben oder vernichtet werden.

7.

Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Es werden ausfallsichere Serversysteme und Dienste eingesetzt, die doppelt, bzw. mehrfach ausgelegt sind, Belastbarkeitstests und Hardwaretests unterliegen, über einen DDoS-Schutz verfügen sowie eine unterbrechungsfreie Stromversorgung bieten (z.B. RAID, HA-Netzteile).
- Es werden Serversysteme und Dienste eingesetzt, die ein Backupsystem an anderen Orten bzw. zumindest in anderen Brandabschnitten bieten, auf dem die aktuellen Daten vorgehalten werden und so ein lauffähiges System auch im Katastrophenfall zur Verfügung stellen.
- Es werden Serversysteme und Dienste eingesetzt, die über Feuchtigkeitsmelder verfügen, als auch über Feuer- und Rauchmeldeanlagen sowie entsprechende Feuerlöschvorrichtungen oder Feuerlöschgeräte im EDV Raum verfügen.
- Es werden Serversysteme und Dienste eingesetzt, die ein zuverlässiges und kontrolliertes Backupkonzept & Recoverykonzept bieten. Backups erfolgen täglich. Die Backups werden verschlüsselt.
- Durch automatisiertes Patch-Management werden die neuesten Releases und Sicherheitsupdates auf Betriebssystem- und Netzwerkebene bei erscheinen zeitnah eingespielt.
- Die Verfügbarkeit der Datenverarbeitungssysteme wird permanent überwacht.

8.

Gewährleistung der Zweckbindung/Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- Sofern erforderlich, möglich und zumutbar, werden Daten physisch getrennt (z.B. durch Einsatz unterschiedlicher Server). Erfolgt keine physische Trennung, werden die Daten logisch getrennt (z.B. in unterschiedlichen Datenbanken oder durch Kennzeichnung mit entsprechenden Zweckattributen, oder Datenfeldern).
- Ein Übergriff durch nichtberechtigte Personen oder Prozesse wird durch ein Berechtigungskonzept verhindert.
- Im Fall pseudonymisierter Speicherung werden die Zuordnungsschlüssel getrennt von den Daten gespeichert und gegen eine unberechtigte oder nicht vom Verarbeitungsprozess vorgesehene Verknüpfung gesichert.
- Produktiv- und Testsysteme werden getrennt.

9.

Zugriffsberechtigte Personen

- Zugriffsberechtigt auf alle Systeme sind nur die Administratoren des Verantwortlichen.
- Kunden, die *QR Planet GmbH* nutzen, haben einen nicht-administrativen Zugriff auf ihren Kundenbereich und die für sie verarbeiteten Daten im Rahmen einer Benutzerberechtigung. Es kann auch für Kunden abgestufte Berechtigungen geben.

Auftrag zur Verarbeitung personenbezogener Daten

Anhang 2 – Unterauftragsverhältnisse

GEVEST Steuer- und BetriebsberatungsgmbH - Schottenfeldgasse 40/8 - 1070 Wien - Österreich
Zweck: Finanzverwaltung, Steuerberater

Hetzner Online GmbH - Industriestr. 25 - 91710 Gunzenhausen - Deutschland
Zweck: Hosting, Infrastruktur- und Plattformdienstleistungen, Rechenkapazität,
Speicherplatz und Datenbankdienste, Sicherheitsleistungen, Technische Wartungsleistungen

Payment-Service-Provider Stripe Payments UK - Ltd., 7th Floor, The Bower Warehouse, 211 Old Street, London EC1V 9NR, United Kingdom.
Zweck: Bei der Zahlungsart „Kreditkarte“, erfolgt die Zahlungsabwicklung über Stripe.
Die im Rahmen des Bestellvorgangs mitgeteilten Informationen nebst den Informationen über Ihre Bestellung (Name, Anschrift, Kreditkartennummer, Rechnungsbetrag, Währung und Transaktionsnummer) werden dort verarbeitet. Die Weitergabe Ihrer Daten erfolgt ausschließlich zum Zwecke der Zahlungsabwicklung mit dem vorgenannten Payment-Service-Provider.