Vertrag zur Auftragsverarbeitung

zwischen

_____

_____

_____

_____

(hier bezeichnet als **„Auftraggeber“**)

und

der **KI-AZ SalesLift GmbH**, Sentesweg 4, 41844 Wegberg, als Auftragsverarbeiter (hier bezeichnet als **„Auftragnehmer“**)

Präambel

Der Auftraggeber möchte die vom Auftragnehmer über dessen Webseite unter der Domain www.just-use.eu angebotene QR-Code Software und/ oder digitale Flyer bzw. Landingpages im Rahmen eines SaaS-Vertrages nutzen. Teil der Vertragsdurchführung ist die Verarbeitung von personenbezogenen Daten. Insbesondere Art. 28 DSGVO stellt bestimmte Anforderungen an eine solche Auftragsverarbeitung. Zur Wahrung dieser Anforderungen schließen die Parteien die nachfolgende Vereinbarung.

§ 1 Begriffsbestimmungen

Für in dieser Vereinbarung benutzte Begriffe, für die Art. 4 DSGVO eine Begriffsbestimmung vorsieht, gilt diese gesetzliche Definition in der im Zeitpunkt des Vertragsschlusses geltenden Fassung auch für diesen Vertrag.

§ 2 Angabe der zuständigen Datenschutz-Aufsichtsbehörde

(1) Zuständige Datenschutz-Aufsichtsbehörde für den Auftragnehmer ist die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Kavalleriestraße 2-4, 40213 Düsseldorf. Die für den Auftraggeber zuständige Datenschutz-Aufsichtsbehörde bestimmt sich nach dessen Geschäftssitz bzw. Wohnort.

(2) Der Auftraggeber und der Auftragnehmer und ggf. deren Vertreter arbeiten auf Anfrage mit den zuständigen Datenschutz-Aufsichtsbehörden bei der Erfüllung ihrer Aufgaben zusammen.

§ 3 Vertragsgegenstand

Der Auftragnehmer stellt dem Auftraggeber über seine Webseite unter der Domain www.just-use.eu eine QR-Code Software im Rahmen eines SaaS-Vertrages („Hauptvertrag“) zur Verfügung. Dabei erhalten der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten der ebenfalls in **Anlage 1** näher spezifizierten betroffenen Personen. Der Auftragnehmer verarbeitet diese Daten ausschließlich im Auftrag und nach Weisung des Auftraggebers. Dem Auftraggeber obliegt die Beurteilung der Zulässigkeit der Datenverarbeitung.

(2) Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen die Parteien die vorliegende Vereinbarung. Die Regelungen des vorliegenden Vertrages gehen im Zweifel den Regelungen des Hauptvertrags vor.

(3) Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht über die Laufzeit des Hauptvertrages hinausgehende Verpflichtungen ergeben. Sich aus diesem Vertrag ergebende Kündigungsrechte bleiben von der vorstehenden Regelung unberührt.

(4) Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus solange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

(5) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind.

§ 4 Verantwortlichkeit des Auftraggebers

(1) Der Auftraggeber ist für die Rechtmäßigkeit der Verarbeitung der Auftraggeber-Daten sowie für die Wahrung der Rechte der Betroffenen im Verhältnis der Parteien zueinander allein verantwortlich. Sollten Dritte gegen den Auftragnehmer aufgrund der Verarbeitung von Auftraggeber-Daten nach Maßgabe dieses Vertrages Ansprüche geltend machen, wird der Auftraggeber den Auftragnehmer von allen solchen Ansprüchen auf erstes Anfordern freistellen.

(2) Dem Auftraggeber obliegt es, dem Auftragnehmer die Auftraggeber-Daten rechtzeitig zur Leistungserbringung nach dem Hauptvertrag zur Verfügung zu stellen und er ist verantwortlich für die Qualität der Auftraggeber-Daten. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse des Auftragnehmers Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen oder seinen Weisungen feststellt.

(3) Der Auftraggeber hat dem Auftragnehmer auf Anforderung die in Art. 30 Abs. 2 DSGVO genannten Angaben zur Verfügung zu stellen, soweit sie dem Auftragnehmer nicht selbst vorliegen.

(4) Ist der Auftragnehmer gegenüber einer staatlichen Stelle oder einer Person verpflichtet, Auskünfte über die Verarbeitung von Auftraggeber-Daten zu erteilen, oder mit diesen Stellen anderweitig zusammenzuarbeiten, so ist der Auftraggeber verpflichtet, den Auftragnehmer auf erstes Anfordern bei der Erteilung solcher Auskünfte bzw. der Erfüllung anderweitiger Verpflichtungen zur Zusammenarbeit zu unterstützen.

§ 5 Weisungsrecht

(1) Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers verarbeiten. Wird der Auftragnehmer durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern ihm dies rechtlich gestattet ist.

(2) Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Der Auftraggeber ist jederzeit zur Erteilung entsprechender Weisungen berechtigt. Dies umfasst Weisungen in Hinblick auf die Berichtigung und Löschung von Daten sowie auf die Einschränkung der Verarbeitung. Die weisungsberechtigten Personen des Auftraggebers ergeben sich aus **Anlage 2**. Bei einem Wechsel oder einer längerfristigen Verhinderung dieser Personen ist dem Auftragnehmer unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

(3) Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren. Weisungen, die über die hauptvertraglich vereinbarte Leistung hinausgehen, werden als Antrag auf Leistungsänderung behandelt. Regelungen über eine etwaige Vergütung von Mehraufwänden, die durch ergänzende Weisungen des Auftraggebers an den Auftragnehmer entstehen, bleiben unberührt.

(4) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen. Der Auftragnehmer ist berechtigt, die Durchführung der betreffenden Weisung solange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 6 Schutzmaßnahmen des Auftragnehmers

(1) Der Auftragnehmer ist verpflichtet, die gesetzlichen Bestimmungen über den Datenschutz zu beachten und die aus dem Bereich des Auftraggebers erlangten Informationen nicht ohne entsprechende Weisung an Dritte weiterzugeben oder deren Zugriff auszusetzen. Unterlagen in Papierform und Daten sind gegen die Kenntnisnahme durch Unbefugte unter Berücksichtigung des Stands der Technik zu sichern.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in der **Anlage 3** aufgeführten Maßnahmen getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der Auftragnehmer zusätzlich die sich aus § 22 Abs. 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen, welche in der **Anlage 3** genauer spezifiziert sind. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung welche Maßnahmen getroffen werden und die Umsetzung der Maßnahmen offen.

Eine Änderung oder Anpassung der getroffenen Sicherheitsmaßnahmen während der Laufzeit des Vertrages bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten und der Auftraggeber über wesentliche Veränderungen unverzüglich informiert wird.

(3) Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im

folgenden Mitarbeiter genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 und Abs. 1 S. 2 lit. b DSGVO), über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren und mit der gebotenen Sorgfalt die Einhaltung der vorgenannten Verpflichtung sicherstellen. Diese Verpflichtungen müssen so gefasst sein, dass sie auch nach Beendigung dieses Vertrages oder des Beschäftigungsverhältnisses zwischen dem Mitarbeiter und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen der Mitarbeiter auf Verlangen in geeigneter Weise nachzuweisen.

§ 7 Informationspflichten des Auftragnehmers

(1) Bei Störungen bei den Verarbeitungstätigkeiten, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers oder Verdacht auf sonstige sicherheitsrelevante Vorfälle beim Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder Textform informieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde, die für den Auftraggeber relevante Verarbeitungen oder Sachverhalte betreffen. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält, soweit möglich, folgende Informationen:

a) eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der Zahl der betroffenen Personen, der betroffenen Kategorien und der Zahl der betroffenen personenbezogenen Datensätze

b) eine Beschreibung der wahrscheinlichen Folgen der Verletzung

c) eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

(2) Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der betroffenen Daten und zur Minderung möglicher nachteiliger Folgen für die betroffene(n) Person(en), informiert hierüber den Auftraggeber, ersucht ihn um weitere Weisungen und erteilt dem Auftraggeber jederzeit weitere Auskünfte, soweit dessen Daten von einer Verletzung nach Abs. 1 betroffen sind.

(3) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren, sofern ihm dies nicht durch gerichtliche oder behördliche Anordnung untersagt ist. Der Auftragnehmer wird in diesem Zusammenhang alle zuständigen Stellen unverzüglich darüber informieren, dass die Entscheidungshoheit über die Daten ausschließlich beim Auftraggeber liegt.

(4) Über wesentliche Änderungen der Sicherheitsmaßnahmen nach § 5 Abs. 2 hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

(5) An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gem. Art. 35 DSGVO und ggf. bei der vorherigen Konsultation der Datenschutz-Aufsichtsbehörden gem. Art. 36 DSGVO hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen. Kosten, die dem Auftragnehmer durch seine Unterstützungshandlungen entstehen, sind ihm im angemessenen Umfang zu erstatten.

§ 8 Kontrollrechte des Auftraggebers

(1) Der Auftraggeber überzeugt sich vor der Aufnahme der Datenverarbeitung und sodann regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers. Hierfür kann er z.B. Auskünfte des Auftragnehmers einholen, sich vorhandene Testate von Sachverständigen, Zertifizierungen oder internen Prüfungen vorlegen lassen oder die technischen und organisatorischen Maßnahmen des Auftragnehmers, sofern möglich, nach rechtzeitiger Abstimmung zu den üblichen Geschäftszeiten selbst persönlich prüfen bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht. Der Auftraggeber wird Kontrollen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören.

(2) Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der technischen und organisatorischen Maßnahmen des Auftragnehmers gemäß der **Anlage 3** erforderlich sind.

(3) Der Auftraggeber dokumentiert das Ergebnis der von ihm durchgeführten Kontrollen und teilt es dem Auftragnehmer mit. Bei Fehlern oder Unregelmäßigkeiten, die der Auftraggeber insbesondere bei der Prüfung von Auftragsergebnissen feststellt, hat er den Auftragnehmer unverzüglich zu informieren. Werden bei der Kontrolle Sachverhalte festgestellt, deren zukünftige Vermeidung Änderungen des angeordneten Verfahrensablaufs erfordern, teilt der Auftraggeber dem Auftragnehmer die notwendigen Verfahrensänderungen unverzüglich mit.

(4) Der Auftraggeber vergütet dem Auftragnehmer den angemessenen Aufwand, der ihm im Rahmen der Kontrolle entsteht.

§ 9 Einsatz von Subunternehmern

(1) Der Auftraggeber ist damit einverstanden, dass der Auftragnehmer die vertraglich vereinbarten Leistungen unter Einschaltung der in **Anlage 4** genannten Subunternehmer durchführt.

(2) Der Auftragnehmer ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von weiteren Unterauftragsverhältnissen mit Subunternehmern („Subunternehmerverhältnis“) befugt. Er setzt den Auftraggeber hiervon unverzüglich in Kenntnis. Der Auftragnehmer ist verpflichtet, Subunternehmer sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragnehmer hat bei der Einschaltung von Subunternehmern diese entsprechend den Regelungen dieser Vereinbarung zu verpflichten und dabei sicherzustellen, dass der Auftraggeber seine Rechte aus dieser Vereinbarung (insbesondere seine Prüf- und Kontrollrechte) auch direkt gegenüber den Subunternehmern wahrnehmen kann. Sofern eine Einbeziehung von Subunternehmern in einem Drittland erfolgen soll, hat der Auftragnehmer sicherzustellen, dass beim jeweiligen Subunternehmer ein angemessenes Datenschutzniveau gewährleistet ist (z.B. durch Abschluss einer Vereinbarung auf Basis der EU-Standarddatenschutzklauseln). Der Auftragnehmer wird dem Auftraggeber auf Verlangen den Abschluss der vorgenannten Vereinbarungen mit seinen Subunternehmern nachweisen.

(3) Ein Subunternehmerverhältnis im Sinne dieser Bestimmungen liegt nicht vor, wenn der Auftragnehmer Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z.B. Post-, Transport- und Versandleistungen, Reinigungsleistungen, Telekommunikationsleistungen ohne konkreten Bezug zu Leistungen, die der Auftragnehmer für den Auftraggeber erbringt und Bewachungsdienste. Wartungs- und Prüfleistungen stellen Subunternehmerverhältnisse i.S.v. Abs. 1 dar, soweit diese für IT-Systeme erbracht werden, die auch im Zusammenhang mit der Erbringung von Leistungen für den Auftraggeber genutzt werden.

§ 10 Anfragen und Rechte betroffener Personen

(1) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen des Zumutbaren und Erforderlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Pflichten des Auftraggebers nach Art. 12–22 sowie 32 und 36 DSGVO.

(2) Macht eine betroffene Person Rechte, etwa auf Auskunftserteilung, Berichtigung oder Löschung hinsichtlich ihrer Daten, unmittelbar gegenüber dem Auftragnehmer geltend, so reagiert dieser nicht selbstständig, sondern verweist die betroffene Person zeitnah an den Auftraggeber und wartet dessen Weisungen ab.

(3) Der Auftraggeber vergütet dem Auftragnehmer den Aufwand, der ihm für die Unterstützungsleistungen entsteht.

§ 11 Haftung

(1) Für die Haftung des Auftragnehmers nach diesem Vertrag gelten die Haftungsausschlüsse und -begrenzungen gemäß dem Hauptvertrag. Soweit Dritte Ansprüche gegen den Auftragnehmer geltend machen, die ihre Ursache in einem schuldhaften Verstoß des Auftraggebers gegen diesen Vertrag oder gegen eine seiner Pflichten als datenschutzrechtlich Verantwortlicher haben, stellt der Auftraggeber den Auftragnehmer von diesen Ansprüchen auf erstes Anfordern frei.

(2) Der Auftraggeber verpflichtet sich, den Auftragnehmer auch von allen etwaigen Geldbußen, die gegen den Auftragnehmer verhängt werden, in dem Umfang auf erstes Anfordern freizustellen, in dem der Auftraggeber Anteil an der Verantwortung für den durch die Geldbuße sanktionierten Verstoß trägt.

§ 12 Beendigung des Hauptvertrags

(1) Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen in Papierform, Daten und Datenträger zurückgeben oder – auf Wunsch des Auftraggebers, sofern nicht nach dem Unionsrecht oder dem Recht der Bundesrepublik Deutschland eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht – löschen. Die Herausgabe- bzw. Vernichtungsverpflichtung betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung zu führen.

(2) Der Auftraggeber hat das Recht, die vollständige und vertragsgerechte Rückgabe bzw. Löschung der Daten beim Auftragnehmer in geeigneter Weise zu kontrollieren bzw. durch einen sachkundigen Dritten prüfen lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zum Auftragnehmer steht.

(3) Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Informationen vertraulich zu behandeln.

§ 13 Schlussbestimmungen

(1) Sollten einzelne Bestimmungen dieser Vereinbarung ganz oder teilweise nicht rechtswirksam oder nicht durchführbar sein oder werden, so wird hierdurch die Gültigkeit der jeweils übrigen Bestimmungen nicht berührt.

(2) Gerichtstand ist der Geschäftssitz des Auftragnehmers, wenn der Auftraggeber Kaufmann, juristische Person des öffentlichen Rechts oder öffentlich-rechtliches Sondervermögen ist oder der Auftraggeber keinen allgemeinen Gerichtsstand im Sitzland vom Auftragnehmer hat. Der Auftragnehmer ist jedoch in diesen Fällen auch berechtigt, Klage am Geschäftssitz des Auftraggebers

zu erheben. Vorrangige gesetzliche Vorschriften, insbesondere zu ausschließlichen Zuständigkeiten, bleiben unberührt.

(3) Sofern der Auftraggeber Unternehmer ist, ist auf den vorliegenden Vertrag ausschließlich deutsches Recht anwendbar unter Ausschluss der Bestimmungen der United Nations Convention on Contracts for the international Sale of Goods (CISG, „UN-Kaufrecht“).

Anlagen

Anlage 1 – Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

Anlage 2 – Weisungsberechtigte Personen des Auftraggebers

Anlage 3 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 4 – Genehmigte Subunternehmer

_____

Ort / Datum

Wegberg, den 10.09.2024

Geschäftsführer Guido Zerreßen

KI-AZ SalesLift GmbH

_____

(Unterschrift Auftraggeber)

Anlage 1

Beschreibung der betroffenen Personen/Betroffenengruppen sowie der besonders schutzbedürftigen Daten/Datenkategorien

Es sind folgende Personen betroffen: (bitte ankreuzen)

- ☐ Kunden
- ☐ Interessenten
- ☐ Mitarbeiter des Auftraggebers
- ☐ externe Mitarbeiter
- ☐ Nutzer QR-Codes
- ☐ **Weitere**

Gegenstand der Erhebung, Verarbeitung und/ oder Nutzung personenbezogener Daten sind folgende:

- **Webformulare:** (bitte ankreuzen)

☐ Namen- und Identifikationsdaten

☐ Kontaktinformation

☐ **Weitere**

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

- **QR-Codes:** (bitte ankreuzen)

☐ Namen- und Identifikationsdaten

☐ Kontaktinformationen

☐ Standortdaten

☐ Bilder

☐ **Weitere**

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

- **Dateiverzeichnis:** (bitte ankreuzen)

☐ Namen- und Identifikationsdaten

☐ Kontaktinformationen

☐ Standortdaten

☐ Bilder

☐ **Weitere**

Anlage 2

Weisungsberechtigte Personen des Auftraggebers

Weisungsberechtig sind: (Namen hier eintragen)

Anlage 3
Technische und organisatorische Maßnahmen des Auftragnehmers (TOM)
Unternehmen: KI-AZ SalesLift GmbH (Stand: 17.08.2024)

Ansprechpartner für den Datenschutz ist Guido Zerreßen, erreichbar unter datenschutz@ki-az-saleslift.de. Die KI-AZ SalesLift GmbH hat den Server-Betrieb an die Firma „netcup GmbH“ (siehe Liste der Subunternehmer, Anlage ausgelagert. Beachten Sie deshalb, dass sich die hier genannten „Technischen- und organisatorischen Maßnahmen“ auf den Teil der Leistung beziehen, den die KI-AZ SalesLift GmbH selbst erbringt. Die TOM des Vertrages zur Auftragsverarbeitung, den wir mit der netcup GmbH abschlossen haben können Sie unter diesem Link einsehen: www.ki-az-saleslift.de/files/tomnetcup . E-Mail-Verkehr wird über den Dienstleister „Strato AG“ (siehe Liste der Subunternehmer, Anlage 4) betrieben. Die TOM der Strato AG können hier einsehen: https://www.strato.de/agb/tom/

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

1.1 Zutrittskontrolle

- Technische Maßnahmen
  - Manuelles Schließsystem
  - Sicherheitsschlösser
- Organisatorische Maßnahmen
  - Schlüsselregelung/Liste
  - Besucher in Begleitung durch Mitarbeiter
  - Sorgfalt bei der Auswahl des Reinigungsdienstes

1.2 Zugangskontrolle

- Technische Maßnahmen
  - Login mit Benutzername + Passwort
  - Login mit biometrischen Daten
  - Anti-Virus-Software Clients
  - Firewall
  - Automatische Desktopsperre
- Organisatorische Maßnahmen
  - Verwalten von Benutzerberechtigungen
  - Erstellen von Benutzerprofilen
  - Zentrale Passwortvergabe
  - Richtlinie „Sicheres Passwort“
  - Richtlinie „Löschen/Vernichten“
  - Allg. Richtlinie Datenschutz und/ oder Sicherheit

1.3 Zugriffskontrolle

- Organisatorische Maßnahmen

- Minimale Anzahl von Administratoren
- Verwaltung Benutzerrechte durch Administratoren

1.4 Trennungskontrolle

- Technische Maßnahmen
  - Trennung von Produktiv- und Testsystem
  - Physikalische Trennung (Systeme/Datenbanken/Datenträger)
- Organisatorische Maßnahmen
  - Steuerung über Berechtigungskonzept
  - Festlegen von Datenbankrechten

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

2.1 Weitergabekontrolle

- Technische Maßnahmen
  - E-Mail-Verschlüsselung
  - Bereitstellung über verschlüsselte Verbindungen
- Organisatorische Maßnahmen
  - Sorgfalt bei der Auswahl von Transport-Personal und Fahrzeugen
  - Persönliche Übergabe mit Protokoll

2.2 Eingabekontrolle

- Organisatorische Maßnahmen
  - Übersicht mit welchen Programmen, welche Daten eingegeben, geändert oder gelöscht werden können
  - Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzeptes
  - Klare Zuständigkeit für Löschungen

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

3.1 Verfügbarkeitskontrolle

- Technische Maßnahmen
  - Feuer- und Rauchmeldeanlagen
  - Spiegelung von Festplatten
- Organisatorische Maßnahmen
  - Existenz eines Notfallplans

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

4.1 Datenschutz-Management

- Technische Maßnahmen
  - Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf/Berechtigung
- Organisatorische Maßnahmen
  - Ansprechpartner für Datenschutz: Guido Zerreßen
  - Mitarbeiter werden auf Vertraulichkeit/ Datengeheimnis verpflichtet
  - Regelmäßige Sensibilisierung der Mitarbeiter
  - Datenschutz-Folgeabschätzung bei Bedarf durchgeführt
  - Die Organisation kommt den Informationspflichten nach Art. 13 und 14 nach
  - Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

4.2 Incident-Response-Management

- Technische Maßnahmen
  - Einsatz von Firewall und regelmäßige Aktualisierung
  - Einsatz von Spamfilter und regelmäßige Aktualisierung
  - Einsatz von Virenscanner und regelmäßige Aktualisierung
- Organisatorische Maßnahmen
  - Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/ Daten-Pannen
  - Dokumentierter Vorgehensweise zum Umgang mit Sicherheitsvorfällen

4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

- Organisatorische Maßnahmen
  - Es werden grundsätzlich nicht mehr Daten erhoben als für den Zweck notwendig sind

4.4 Auftragskontrolle (Outsourcing an Dritte)

- Organisatorische Maßnahmen
  - Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
  - Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten
  - Abschluss der notwendigen Vereinbarungen zur Auftragsverarbeitung

- Schriftliche Weisung an den Auftragnehmer
- Verpflichtung der Mitarbeiter auf das Datengeheimnis
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten durch den Auftragnehmer bei Vorliegen der Bestellpflicht
- Vereinbarung wirksamer Kontrollrechte ggü. dem Auftragnehmer
- Regelung zum Einsatz weiterer Subunternehmer
- Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrages

Anlage 4

Genehmigte Subunternehmer

netcup GmbH
Daimlerstr. 25
D-76185 Karlsruhe
Hosting Cloudserver

STRATO AG
Otto-Ostrowski-Straße 7,
10249 Berlin:
E-Mail-Weiterleitung aus Webformularen, Landingpage