Auftragsverarbeitungsvertrag

nach Art. 28 Abs. 3 DSGVO

zwischen

dem Kunden
als Verantwortlicher
(hier bezeichnet als „Auftraggeber“)

Und

solute GmbH
Zeppelinstraße 15
D-76185 Karlsruhe
als Auftragsverarbeiter
(hier bezeichnet als „Auftragnehmer“)

Präambel

Der Auftraggeber möchte den Auftragnehmer mit den in § 3 genannten Leistungen beauftragen. 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, deren Erfüllung nicht gesondert vergütet wird, sofern dies nicht ausdrücklich vereinbart ist. Diese Vereinbarung zur Auftragsverarbeitung ersetzt alle bisherigen Vereinbarungen gem. Art. 28 DSGVO oder § 11 BDSG (alt) zu dem genannten Vertragsgegenstand im § 3.

§ 1 Begriffsbestimmungen

In diesem Vertrag verwendete Begriffe, die in Art. 4, 9 und 10 DSGVO definiert werden, sind im Sinne dieser gesetzlichen Definition zu verstehen.

§ 2 Vertreter innerhalb der Europäischen Union

Der Auftragnehmer hat als Vertreter nach Art.27 Abs.1 DSGVO benannt

Nicht anwendbar
Name, Vorname, ggf. Firma, Anschrift, E-Mail, ggf. Telefonnr. des Vertreters nach Art. 27 DSGVO

§ 3 Vertragsgegenstand

Der Auftragnehmer erbringt für den Auftraggeber Leistungen im Bereich (Hinweisgeberportal WHISPRO gemäß des Hinweisgeberschutzgesetzes) auf Grundlage des Vertrags mit Laufzeitbeginn ab Erhalt der Auftragsbestätigung („Hauptvertrag“). Dabei erhält der Auftragnehmer Zugriff auf personenbezogene Daten und verarbeitet diese ausschließlich im Auftrag und nach Weisung des Auftraggebers, sofern der Auftragnehmer nicht durch das Recht der Union oder der Mitgliedsstaaten, dem er unterliegt, zu einer anderen Verarbeitung verpflichtet ist. Umfang und Zweck der Datenverarbeitung durch den Auftragnehmer ergeben sich aus dem Hauptvertrag (und sofern vorhanden aus der dazugehörigen Leistungsbeschreibung) sowie aus der **Anlage 1** zu diesem Vertrag. Dem Auftraggeber obliegt die alleinige Beurteilung der Zulässigkeit der Datenverarbeitung gemäß Art. 6 Abs. 1 DSGVO.

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

Die Bestimmungen dieses Vertrages finden Anwendung auf alle Tätigkeiten, die mit dem Hauptvertrag in Zusammenhang stehen und bei der der Auftragnehmer und seine Beschäftigten oder durch den Auftragnehmer Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Auftraggeber stammen oder für den Auftraggeber erhoben wurden oder auf sonstige Weise in dessen Auftrag verarbeitet werden.

Die Laufzeit dieses Vertrags richtet sich nach der Laufzeit des Hauptvertrages, sofern sich aus den nachfolgenden Bestimmungen nicht darüberhinausgehende Verpflichtungen oder Kündigungsrechteergeben.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der europäischen Union oder einem anderen Vertragsstaat des Abkommens über den europäischen Wirtschaftsraum (EWR) statt. Jede Verlagerung von Teilleistungen oder der gesamten Dienstleistung in ein Drittland bedarf der vorherigen Benachrichtigung des Auftraggebers in Schriftform oder dokumentiertem elektronischen Format. Die besonderen Voraussetzungen der Art. 44 ff. DSGVO sind dabei zu beachten.

§ 4 Art der verarbeiteten Daten, Kreis der betroffenen Personen

Im Rahmen der Durchführung des Hauptvertrags erhält der Auftragnehmer Zugriff auf die in **Anlage 1** näher spezifizierten personenbezogenen Daten der ebenfalls in **Anlage 1** näher spezifizierten betroffenen Personen.

§ 5 Weisungsrecht

Der Auftragnehmer darf Daten nur im Rahmen des Hauptvertrags und gemäß den Weisungen des Auftraggebers erheben, nutzen oder auf sonstige Weise verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. 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.

Die Weisungen des Auftraggebers werden anfänglich durch diesen Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in dokumentiertem elektronischem Format 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, Löschung und Sperrung von Daten. Die weisungsberechtigten Personen ergeben sich aus **Anlage 4**. Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen ist dem Vertragspartner unverzüglich der Nachfolger bzw. Vertreter in Textform zu benennen.

Alle erteilten Weisungen sind sowohl vom Auftraggeber als auch vom Auftragnehmer zu dokumentieren und für die Dauer ihrer Geltung sowie anschließend für drei weitere volle Kalenderjahre aufzubewahren. 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 der Auftraggeberin an die Auftragnehmerin entstehen, bleiben unberührt.

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 so lange auszusetzen, bis diese durch den Auftraggeber bestätigt oder geändert wird. Der Auftragnehmer darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 6 Schutzmaßnahmen des Auftragnehmers

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

Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird und gewährleistet, dass er alle erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers gem. Art. 32 DSGVO, insbesondere mindestens die in **Anlage 2** aufgeführten Maßnahmen getroffen hat. Sofern auch besondere Kategorien personenbezogener Daten verarbeitet werden, trifft der Auftragnehmer zusätzlich die sich aus § 22 Absatz 2 BDSG ergebenden angemessenen und spezifischen Maßnahmen. Der Auftragnehmer legt auf Anforderung des Auftraggebers die näheren Umstände der Festlegung und Umsetzung der Maßnahmen offen. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

Beim Auftragnehmer ist als betrieblicher Datenschutzbeauftragter oder als Ansprechpartner für den Datenschutz (sofern ein Datenschutzbeauftragter nach Art. 37 Abs. 1 DSGVO nicht bestellt werden muss) bestellt:

dacuro GmbH
Otto-Hahn-Straße 3
69190 Walldorf
E-Mail: datenschutz@solute.de

Den bei der Datenverarbeitung durch den Auftragnehmer beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu nutzen oder auf sonstige Weise zu verarbeiten. Der Auftragnehmer wird alle Personen, die von ihm mit der Bearbeitung und der Erfüllung dieses Vertrages betraut werden (im Folgenden „Beschäftigte“ genannt), entsprechend verpflichten (Verpflichtung zur Vertraulichkeit, Art. 28 Abs. 3 lit. b DSGVO) und über die sich aus diesem Vertrag ergebenden besonderen Datenschutzpflichten sowie die bestehende Weisungs- bzw. Zweckbindung belehren sowie 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 Beschäftigten und dem Auftragnehmer bestehen bleiben. Dem Auftraggeber sind die Verpflichtungen auf Verlangen in geeigneter Weise nachzuweisen.

Die Verarbeitung von Daten, die Gegenstand dieses Vertrags sind, in Privatwohnungen (Tele-bzw. Heimarbeit von Beschäftigten des Auftragnehmers) ist gestattet. Die Einhaltung der Schutzmaßnahmen nach § 6 Absätzen 1 und 2 dieses Vertrags sowie der Maßgaben des Art. 32 DSGVO ist auch in diesem Fall sicherzustellen.

§ 7 Informationspflichten des Auftragnehmers

Bei Störungen, Verdacht auf Datenschutzverletzungen oder Verletzungen vertraglicher Verpflichtungen des Auftragnehmers, Verdacht auf sicherheitsrelevante Vorfälle oder andere Unregelmäßigkeiten bei der Verarbeitung der personenbezogenen Daten durch den Auftragnehmer, bei ihm im Rahmen des Auftrags beschäftigten Personen oder durch Dritte wird der Auftragnehmer den Auftraggeber unverzüglich in Schriftform oder dokumentiertem elektronischen Formatinformieren. Dasselbe gilt für Prüfungen des Auftragnehmers durch die Datenschutz-Aufsichtsbehörde. Die Meldung über eine Verletzung des Schutzes personenbezogener Daten enthält soweit möglich folgende Informationen:

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;

eine Beschreibung der wahrscheinlichen Folgen der Verletzung und

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

Der Auftragnehmer trifft unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Person(en), informiert hierüber den Auftraggeber und ersucht diesen um weitere Weisungen.

Der Auftragnehmer ist darüber hinaus verpflichtet, dem Auftraggeber jederzeit Auskünfte zu erteilen, soweit dessen Daten von einer Verletzung nach Absatz1 betroffen sind.

Der Auftragnehmer unterstützt den Auftraggeber erforderlichenfalls bei der Erfüllung der Pflichten des Auftraggebers nach Art. 33 und 34 DSGVO in angemessener Weise (Art. 28 Abs. 3 S. 2 lit. f DSGVO).

Meldungen für den Auftraggeber nach Art. 33 oder 34 DSGVO darf der Auftragnehmer nur nach vorheriger Weisung seitens des Auftraggebers gem. § 5 dieses Vertrags durchführen.

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 als „Verantwortlichem" im Sinne der DSGVO liegen.

Über Änderungen der Sicherheitsmaßnahmen nach § 6 Abs. 2 dieses Vertrags hat der Auftragnehmer den Auftraggeber unverzüglich zu unterrichten.

Ein Wechsel in der Person des betrieblichen Datenschutzbeauftragten bzw. Ansprechpartners für den Datenschutz ist dem Auftraggeber unverzüglich mitzuteilen.

Der Auftragnehmer und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag des Auftraggebers durchgeführten Tätigkeiten der Verarbeitung, dass alle Angaben gem. Art. 30 Abs. 2 DSGVO enthält.

An der Erstellung des Verfahrensverzeichnisses durch den Auftraggeber sowie bei der Erstellung einer Datenschutz-Folgenabschätzung gemäß Art. 35 DSGVO und ggf. bei der vorherigen Konsultation der Aufsichtsbehörden gemäß Art. 36 DSGVO hat der Auftragnehmer im angemessenen Umfang mitzuwirken. Er hat dem Auftraggeber die jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.

§ 8 Kontrollrechte des Auftraggebers

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. Nur wenn diese nicht vorgelegt werden, kann der Auftraggeber die technischen und organisatorischen Maßnahmen des Auftragnehmers nach vorheriger Abstimmung (mindestens 2 Wochen vor dem Kontrolltermin) 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, die Betriebsabläufe des Auftragnehmers dabei nicht unverhältnismäßig stören und die gesetzlichen Vorschriften beachten.

Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf dessen mündliche, schriftliche oder elektronische 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 erforderlich sind.

Der Auftraggeber dokumentiert das Kontrollergebnis 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.

Der Auftragnehmer weist dem Auftraggeber die Verpflichtung der Mitarbeiter nach § 6 Abs. 4 auf Verlangen nach.

Der Auftraggeber vergütet dem Auftragnehmer den Aufwand, der ihm im Rahmen der Kontrolle entsteht.

§ 9 Einsatz von Subunternehmern

Die vertraglich vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der in **Anlage 3** genannten Subunternehmer durchgeführt. 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. 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.

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 zustimmungspflichtige Subunternehmerverhältnisse 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

Der Auftragnehmer unterstützt den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung von dessen Pflichten nach Art.12 - 22 sowie 32 und 36 DSGVO.

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

§ 11 Haftung

Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DSGVO getroffenen Regelung. Der Auftragnehmer stimmt eine etwaige Erfüllung von Haftungsansprüchen mit dem Auftraggeber ab.

Der Auftragnehmer stellt den Auftraggeber auf erstes Anfordern von sämtlichen Ansprüchen frei, die betroffene Personen gegen den Auftraggeber wegen der Verletzung einer dem Auftragnehmer durch die DSGVO auferlegten Pflicht oder der Nichtbeachtung oder Verletzung einer vom Auftraggeber in dieser AV-Vereinbarung oder einer gesondert erteilten Anweisung geltend machen.

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 einer betroffenen Person eingetreten ist, verantwortlich ist. Im Übrigen gilt Art. 82 Absatz 5 DSGVO.

Sofern vorstehend nicht anders geregelt, entspricht die Haftung im Rahmen dieses Vertrages der des Hauptvertrages.

§ 12 Außerordentliches Kündigungsrecht

Der Auftraggeber kann den Hauptvertrag fristlos ganz oder teilweise kündigen, wenn der Auftragnehmer seinen Pflichten aus diesem Vertrag nicht nachkommt, Bestimmungen der DSGVO oder sonstige anwendbare Datenschutzvorschriftenvorsätzlich oder grob fahrlässig verletzt oder eine Weisung des Auftraggebers nicht ausführen kann oder will oder der Auftragnehmer sich den Kontrollrechten des Auftraggebers auf vertragswidrige Weise widersetzt. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

§ 13 Beendigung des Hauptvertrags

Der Auftragnehmer wird dem Auftraggeber nach Beendigung des Hauptvertrags oder jederzeit auf dessen Anforderung alle ihm überlassenen Unterlagen, 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. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Der Auftragnehmer hat den dokumentierten Nachweis der ordnungsgemäßen Löschung noch vorhandener Daten zu führen.

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.

Der Auftragnehmer ist verpflichtet, auch über das Ende des Hauptvertrags hinaus die ihm im Zusammenhang mit dem Hauptvertrag bekannt gewordenen Daten vertraulich zu behandeln. Die vorliegende Vereinbarung bleibt über das Ende des Hauptvertrags hinaus so lange gültig, wie der Auftragnehmer über personenbezogene Daten verfügt, die ihm vom Auftraggeber zugeleitet wurden oder die er für diesen erhoben hat.

§ 14 Schlussbestimmungen

Die Parteien sind sich darüber einig, dass die Einrede des Zurückbehaltungsrechts durch den Auftragnehmer i. S. d. § 273 BGB hinsichtlich der zu verarbeitenden Daten und der zugehörigen Datenträger ausgeschlossen ist.

Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Schriftform oder eines dokumentierten elektronischen Formats. Dies gilt auch für den Verzicht auf dieses Formerfordernis. Der Vorrang individueller Vertragsabreden bleibt hiervon unberührt.

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.

Diese Vereinbarung unterliegt deutschem Recht. Ausschließlicher Gerichtsstand ist Karlsruhe.

Stand: 01.12.2023

Anlagen:

Anlage 1 – Beschreibung der betroffenen Personen/ Betroffenengruppen sowie der verarbeiteten Daten

Anlage 2 – Technische und organisatorische Maßnahmen des Auftragnehmers

Anlage 3 – Genehmigte Subunternehmer

Anlage 1

(1) Betroffene Personen

Die übermittelten personenbezogenen Daten beziehen sich auf folgende Kategorien von betroffenen Personen:

- Hinweisgeber,
- Dritte.

(2) Kategorie der verarbeiteten Daten

Die verarbeiteten personenbezogenen Daten gehören zu folgenden Datenkategorien:

- Kontaktdaten (im Falle der freiwilligen Nennung),
- IP-Adresse (temporär – zur Herstellung der Verbindung; keine Protokollierung),
- ggf. personenbezogene Daten Dritter, sofern vom Hinweisgeber benannt.

Die verarbeiteten personenbezogenen Daten gehören zu folgenden besonderen Kategorien personenbezogener Daten:

Es werden nur Daten besonderer Kategorien verarbeitet (Kommunikationsinhalte), sofern diese von den Meldenden eingetragen werden.

(3) Dauer der Verarbeitung

Die Datenverarbeitung richtet sich nach der Laufzeit der Hauptvertrags.

(4) Umfang, Art und Zweck der Verarbeitung

Die Datenverarbeitung erfolgt zur Bereitstellung und zum Betrieb des Hinweisgeberportals

Anlage 2:

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

solute GmbH
Stand: 31.08.2020

1. Einleitung

Der Gesetzgeber hat in Art. 32 Abs.1 der Datenschutzgrundverordnung (DSGVO) angeordnet, dass die Maßnahmen zur Sicherung der Datenverarbeitungsvorgänge der Auftragsverarbeitung einzuhalten sind. Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

2. Vertraulichkeit

2.1. Zutrittskontrolle

Zutrittskontrollen sind Maßnahmen, die verhindern, dass unbefugte Personen den Zutritt zu Datenverarbeitungsanlagen wie Computer, Server und allen weiteren Geräten, die sich Verarbeitung von personenbezogenem Daten eignen, erhalten. Ziel ist es, die Möglichkeit unbefugter Kenntnis- oder Einflussnahme von vornherein auszuschließen. Die Schutzmaßnahmen sollen mit zunehmender Sensibilität der Daten entsprechend steigen.

Die solute GmbH wendet nachfolgende Maßnahmen an, damit Unbefugten der Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt wird:

- Alle Außentüren sind mit einem manuellen Schließsystem mit Sicherheitsschlössern versehen und grundsätzlich verschlossen. Der unbeaufsichtigte Zugang von Mitarbeiter zum Gebäude erfolgt mittels RFID-Chipkarten über ein elektronisches Türsystem.
- Sicherheitszonen innerhalb des Gebäudes sind mittels Schließsystemen mit Codesperre oder manuellen Schließsystem gesichert.
- Die Vergabe von Schlüsseln und RFID-Chipkarten an Mitarbeiter wird über Schlüsselregelungen überwacht und dokumentiert.
- Der Zutritt zum Unternehmen erfolgt für die Besucher ausschließlich über den Empfang. Der Zutritt betriebsfremder Personen wird an dieser Stelle protokolliert. Besucher dürfen sich nur in Begleitung eines Mitarbeiters innerhalb des Gebäudes bewegen.

Das Reinigungspersonal wird sorgfältig ausgesucht und ist auf Vertraulichkeit (Datengeheimnis) verpflichtet.

- Außerhalb der Betriebsstunden wird das Gebäude durch Alarmsensoren überwacht. Alarmmeldungen werden durch einen externen und zertifizierten Dienstleister überwacht.
- Gebäudeschächte im Außenbereich sind gegen unbefugtes Öffnen gesichert.

2.2. Zugangskontrolle

Zugangskontrollen sind Maßnahmen, die die Nutzung der Datenverarbeitungsanlagen durch Unbefugte verhindern. Während die Zutrittskontrolle (2.1.) den physikalischen Zutritt verhindert, unterbindet die Zugangskontrolle die Nutzung der Datenverarbeitungsanlagen.

Die solute GmbH unternimmt folgende Maßnahmen, die verhindern, dass Unbefugte die Datenverarbeitungsanlagen und -geräte nutzen:

- Nur berechtigte Personen haben Zugang zu zentralen und dezentralen Datenverarbeitungsanlagen (Arbeitsplatzrechner und Serverräume). Die Serverräume sind zusätzlich durch eine Alarmsicherung gegen unberechtigten Zutritt gesichert.
- Welcher Mitarbeiter auf welche Daten und Programme Zugriff hat, wird über ein rollenbasierendes Berechtigungskonzept zentral gesteuert. Nicht mehr benötigte Zugangsberechtigungen werden zeitnah entzogen.
- Der Zugang zu Datenverarbeitungsgeräten und -anlagen ist durch Benutzername und Passwort geschützt.
- Passwortlänge, Gültigkeit und Komplexität sind über eine zentrale Passwort-Richtlinie definiert.
- Datenverarbeitungsgeräte werden von den Mitarbeitern manuell, oder nach einer vorgegebenen Zeitdauer der Inaktivität automatisch gesperrt und können nur durch die erneute Passwort-Eingabe aktiviert werden.
- Es liegt eine Richtlinie zum Verschlüsseln von mobilen Datenträgern vor, um eine missbräuchliche Nutzung von Datenträgern zu verhindern.
- Das Unternehmen hat fest definierte Regelungen und Vorgehensweisen beim Ausscheiden von Mitarbeitern.

2.3. *Zugriffskontrolle*

Zugriffskontrollen sind Maßnahmen, die gewährleisten, dass nur befugte Mitarbeiter Zugriff auf personenbezogene Daten erhalten und diese verarbeiten. Die Berechtigung ergibt sich aus der Aufgabenzuweisung der Mitarbeiter durch die Verantwortlichen im Unternehmen. Ein unbefugtes Lesen, Kopieren, Verändern oder Löschen personenbezogener Daten während ihrer Verarbeitung, Nutzung oder Speicherung soll verhindert werden.

Die solute GmbH setzt die Zugriffskontrolle wie folgt um:

- Berechtigungskonzept für ERP/CRM Software:
  Es sind ausschließlich Personen, die mit der Erhebung, Nutzung und Verarbeitung der Daten im Rahmen der vereinbarten Datenverarbeitung betraut sind, berechtigt, die Daten zu lesen, zu kopieren, zu ändern oder zu löschen.
- Berechtigungskonzept für Drucker:
  Mitarbeiter können nur auf die zugewiesenen Drucker in Arbeitsplatznähe zugreifen.
- Berechtigungskonzept für Laufwerke:
  Mitarbeiter können nur auf die zugewiesenen Speichermedien zugreifen.
- Die Firewall überwacht und protokolliert den laufenden Datenverkehr aus und in Richtung Internet.
- Um Dokumente und Daten vor nicht autorisierten Zugriffen zu schützen, existiert eine Clean-Desk-Policy, um Risiken zu reduzieren.
- Papierdokumente werden mit Aktenschredder, die zur Vernichtung von sensiblen Daten geeignet sind, vernichtet und/oder in abschließbaren Sicherheitsbehälter zur datenschutzkonformen Entsorgung gelagert. Die Entsorgung geschieht über einen zertifizierten externen Dienstleister, mit dem ein Vertrag zur Auftragsverarbeitung geschlossen wurde.
- Einsatz von Anti-Viren-Software.

2.4. *Trennungskontrolle*

Trennungskontrollen sind Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden. Hierfür stellt man für verschiedene Bereiche logisch oder physikalisch getrennte Bereiche zur Verfügung und behält dadurch den Überblick, auf welchen Laufwerken welche Daten gespeichert sind.

Seitens der solute GmbH werden die Maßnahmen wie folgt umgesetzt:

- Über Berechtigungskonzepte für Datenbanken, Anwendungen und Speichersysteme ist eine Trennung der verarbeiteten Daten sichergestellt.
- Physische oder virtuelle Trennung von Speicherstrukturen wie Datendateien, dedizierte Speicherorte innerhalb der gemeinsamen IT-Infrastruktur.
- Logisch getrennte Datenhaltung mit separiertem Zugriff über Accounts.
- Das Gäste W-LAN ist vom Firmennetzwerk getrennt.
- Testsysteme sind von den Produktivsystemen getrennt.
- Mandantenfähigkeit in relevanten Anwendungen.
- Das Firmennetz ist durch eine Firewall geschützt.
- Segmentierung des IT-Netzwerks.

2.5. Pseudonymisierung

Pseudonymisierung ist die Verarbeitung von personenbezogenen 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.

- Soweit dies mit vertretbarem Aufwand technisch und organisatorisch möglich ist, werden personenbezogene Daten durch geeignete Verfahren pseudonymisiert oder anonymisiert.

3. Integrität

3.1. Weitergabekontrolle

Weitergabekontrollen sind 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.

Die Weitergabekontrolle erfolgt bei der solute GmbH durch nachfolgende Maßnahmen:

- Ein externer Zugriff auf das Firmennetzwerk und den dezentralen Rechenzentren ist nur über verschlüsselte VPN-Tunnel möglich.
- Es erfolgt eine Protokollierung von Abruf- und Übermittlungsvorgängen.
- Web-Services sind per HTTPS/SFTP verschlüsselt.
- Die E-Mail-Kommunikation erfolgt per SSL/TLS-Verschlüsselung.

3.2. Eingabekontrolle

Eingabekontrollen sind Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Die solute GmbH setzt die Eingabekontrolle wie folgt um:

- Nur explizit beauftrage Mitarbeiter haben das Recht, personenbezogene Daten in Datenverarbeitungsanlagen einzugeben, zu verändern oder zu entfernen.
- Die Verarbeitung von Datensätzen wird durch technische Protokollierung in den eingesetzten ERP/CRM-Systeme dokumentiert.
- Alle Administrationstätigkeiten werden protokolliert.

4. Verfügbarkeit und Belastbarkeit

4.1. Verfügbarkeitskontrolle

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

Nachfolgend Maßnahmen zur Kontrolle der Verfügbarkeit werden von der solute GmbH eingesetzt:

- Es gibt ein Backup- und Recovery-Konzept, das die Daten gegen zufällige Zerstörung oder Verlust schützt.
- Die Backups werden regelmäßig daraufhin getestet, ob ein reibungsloses Zurücksichern möglich ist.
- Vorhandensein redundanter Soft- und Hardware und Server/PC Standartkomponenten.
- Unterbrechungsfreie Stromversorgung mittels USV bei allen Server-Systemen.
- Voll klimatisierte Serverräume.
- Überwachung von Temperatur und Feuchtigkeit in Serverräumen.
- Brandschutz mittels Feuer- und Rauchmeldeanlagen.
- Feuerlöschgeräte in Serverräumen und Büros vorhanden.
- Schutzsteckdosen in Serverräumen.
- Die Serverräume liegen nicht unter sanitären Anlagen.
- Datensicherungen werden an einem sicheren, ausgelagerten Ort aufbewahrt.
- Es existiert ein Konzept für die Wiederherstellung nach einem Notfall.

4.2. Belastbarkeitskontrolle

Belastbarkeitskontrollen sind Maßnahmen, die gewährleisten, dass Datenverarbeitungssysteme auch bei starker Beanspruchung durch viele gleichzeitige Zugriffsanfragen oder Cyberangriffe belastbar sind.

Hierfür verwendet die solute GmbH nachfolgende Maßnahmen:

- Grundsätzliche Verwendung von redundanten Festplattensystemen für Server mittels RAID-System (1,10 und 5).
- 24/7 IT-Bereitschaft mit Monitoring der Server und der Netzwerkauslastung.
- Zentraler und dezentraler Virenschutz an allen der Datenverarbeitung angeschlossenen Systemen.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

5.1. Datenschutzmanagement

Zum Datenschutzmanagement gehören alle Maßnahmen, um die gesetzlichen und betrieblichen Anforderungen des Datenschutzes systematisch zu planen, zu organisieren, zu steuern und zu kontrollieren.

Diese werden durch die solute GmbH wie folgt umgesetzt:

- Benennung eines externen Datenschutzbeauftragten und eines internen Datenschutzkoordinators.
- Der Datenschutzbeauftragte ist in datenschutzrelevante Projekte eingebunden.
- Führen eines Verzeichnisses der Verarbeitungstätigkeiten.
- Technische- und organisatorische Maßnahmen.
- Schulung und Sensibilisierung aller Mitarbeiter.
- Datenschutzfolgenabschätzung (DSFA) werden bei Bedarf durchgeführt.
- Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener vorhanden.

5.2. Incident Response-Management

Unter Incident Response-Management sind Maßnahmen zu verstehen, wie bei einem Datenschutz- oder IT-Sicherheitsvorfall zu reagieren ist. Dazu zählen alle organisatorischen und technischen Maßnahmen zur Abwehr und schnellen Eindämmung eines Vorfalls.

Hier kommen bei der solute GmbH folgende Maßnahmen zum Einsatz:

- Aktives Incident-Management mit Klassifizierung, Dokumentation und Störungsmanagement.
- Fehlersuche und -behebung über Bug-Tracking-System.
- Release- und Changemanagement.
- Definierte Verhaltensgrundsätze für alle Mitarbeiter.

5.3. Datenschutzfreundliche Voreinstellungen

Datenschutzfreundliche Voreinstellungen sind alle Maßnahmen, die Datenschutz per Technikgestaltung (privacy by design) und datenschutzfreundliche Voreinstellungen (privacy by default) gewährleisten.

Die solute GmbH setzt die datenschutzfreundlichen Voreinstellungen wie folgt um:

- Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind.
- Einfache Ausübung des Widerrufrechts des Betroffenen durch technische Maßnahmen.

5.4. Auftragskontrolle

Zur Auftragskontrolle gehören Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.

Die Umsetzung erfolgt seitens der solute GmbH wie folgt:

- Mit jedem Dienstleister, der im Auftrag personenbezogene Daten verarbeitet oder im Zusammenhang mit seiner Tätigkeit Einblick und Zugriff auf personenbezogene Daten haben könnte, wird ein Vertrag zur Auftragsverarbeitung gem. Art. 28 DSGVO geschlossen.
- Die Dienstleister werden sorgfältig, in Bezug auf Datenschutz und Datensicherheit, ausgewählt.
- Die technischen und organisatorischen Maßnahmen müssen den Mindestanforderungen entsprechen und Bestandteil des Vertrages zur Auftragsverarbeitung sein.
- Bei Bedarf werden die technischen und organisatorischen Maßnahmen beim Dienstleister Vor-Ort überprüft.

Anlage 3: Subunternehmer

Folgende Subunternehmer gelten mit Abschluss dieses Vertrages als genehmigt:

Firma, Adresse	Ort der Datenverarbeitung	Auftrag/Art der Datenverarbeitung
ITstrategen GmbH Kriegstraße 113 76135 Karlsruhe	Deutschland/ EU	Hinweisgebersystem