# CleverOne Vereinbarung Auftragsverarbeitung

## 1. Allgemeines

Der Auftragnehmer stellt dem Auftraggeber seine All-in-One-SaaS-Plattform für das Management von Bestattungsunternehmen als Software as a Service (SaaS) zur Verfügung. Mit der Software kann der Auftraggeber personenbezogene Daten erheben und verarbeiten. Dementsprechend beinhaltet der von den Parteien geschlossene Vertrag über die Zurverfügungstellung der Software („Hauptvertrag") die Verarbeitung von personenbezogenen Daten im Auftrag durch den Auftragnehmer. Diese Vereinbarung über eine Auftragsverarbeitung („AVV") konkretisiert, als Teil des Hauptvertrages, die Verpflichtungen beider Parteien zur Einhaltung des anwendbaren Datenschutzrechts, insbesondere der Anforderungen der Datenschutz-Grundverordnung („DSGVO").

## 2. Anwendungsbereich

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Der Gegenstand der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten und die Kategorien betroffener Personen sind im Hauptvertrag und in **Anlage 1 zu dieser AVV** festgelegt. Die Laufzeit dieser AVV und die Dauer der Auftragsverarbeitung entsprechen der Laufzeit des Hauptvertrages. Sofern der Auftraggeber während der Laufzeit des Hauptvertrags Zusatzmodule (z.B. Marktplatz-Module) bucht, die zu einer Verarbeitung personenbezogener Daten führt, die über die in Anlage 1 beschriebene hinausgeht oder die zur Einbindung zusätzlicher Unterauftragsverarbeiter führt, erstreckt sich dieser AVV automatisch auch auf diese. Gegenstand, Art und Zweck der Verarbeitung, Betroffene Personen und Unterauftragsverarbeiter werden in der Beschreibung des jeweiligen Zusatzmoduls angegeben.

## 3. Weisungsgebundenheit

3.1 Der Auftragnehmer verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist nach dem Recht der Union oder eines Mitgliedstaates, dem er unterliegt, zur Verarbeitung verpflichtet; in einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht dies nicht wegen eines wichtigen öffentlichen Interesses verbietet. Die Weisungen werden anfänglich durch den Hauptvertrag festgelegt und können vom Auftraggeber danach in Textform geändert, ergänzt oder ersetzt werden. Mündliche Weisungen sind vom Auftraggeber unverzüglich in Textform zu bestätigen. Jede Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation erfolgt ausschließlich auf der Grundlage dokumentierter Weisungen des Auftraggebers und muss im Einklang mit Kapitel V der DSGVO stehen. Soweit hierfür geeignete Garantien gem. Art. 46 DSGVO erforderlich sind, vereinbaren die Parteien diese gesondert.

3.2 Falls der Auftragnehmer nach dem Recht der Union oder des Mitgliedstaates, dem der Auftragnehmer unterliegt, verpflichtet ist, personenbezogene Daten zu verarbeiten, wird der Auftragnehmer den Auftraggeber hierüber vor der jeweiligen Verarbeitung schriftlich informieren, es sei denn, das Gesetz verbietet solche Informationen aus wichtigen Gründen des öffentlichen Interesses. Im letztgenannten Fall wird der Auftragnehmer den Verantwortlichen unverzüglich informieren, sobald ihm dies rechtlich möglich ist.

3.3 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung so lange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.

3.4 Der Auftragnehmer darf Daten über die Nutzung der Software durch den Auftraggeber in anonymisierter Form zum Zwecke der Optimierung der Software, der User Experience und für

sicherheitsrelevante Auswertungen verwenden. Der Auftraggeber erteilt hiermit eine entsprechende Weisung für die entsprechende Anonymisierung.

## 4. Technische und organisatorische Maßnahmen

4.1 Der Auftragnehmer verpflichtet sich gegenüber dem Auftraggeber zur Einhaltung der technischen und organisatorischen Maßnahmen, die zur Einhaltung der anzuwendenden Datenschutzvorschriften erforderlich sind. Dies beinhaltet insbesondere die Vorgaben aus Art. 32 DSGVO.

4.2 Der zum Zeitpunkt des Vertragsschlusses bestehende Stand der technischen und organisatorischen Maßnahmen ist in **Anlage 2 zu dieser AVV** dokumentiert. Die Parteien sind sich darüber einig, dass zur Anpassung an technische und rechtliche Gegebenheiten Änderungen der technischen und organisatorischen Maßnahmen erforderlich werden können. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Auftraggeber kann jederzeit eine aktuelle Übersicht, der vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen anfordern.

## 5. Betroffenenrechte

5.1 Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DSGVO (insb. Auskunft, Berichtigung, Sperrung oder Löschung). Soweit eine Mitwirkung des Auftragnehmers für die Wahrung von Betroffenenrechten durch den Auftraggeber erforderlich ist, wird der Auftragnehmer die jeweils erforderlichen Maßnahmen nach Weisung des Auftraggebers treffen. Der Auftragnehmer wird den Auftraggeber nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei unterstützen, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung von Betroffenenrechten nachzukommen. Soweit die Unterstützungsleistungen des Auftragnehmers über den normalen Betrieb der Software hinausgehen, kann der Auftragnehmer hierfür eine angemessene Vergütung verlangen.

5.2 Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

## 6. Sonstige Pflichten des Auftragnehmers

6.1 Im Falle einer Verletzung des Schutzes personenbezogener Daten, die vom Auftragnehmer im Auftrag verarbeitet werden, meldet der Auftragnehmer diese dem Auftraggeber unverzüglich, nachdem ihm die Verletzung bekannt wurde. Die Meldung muss zumindest folgende Informationen enthalten: (a) eine Beschreibung der Art der Verletzung (möglichst unter Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze); (b) Kontaktdaten einer Anlaufstelle, bei der weitere Informationen über die Verletzung eingeholt werden können; (c) die voraussichtlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung, einschließlich Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen. Soweit nicht alle Informationen zur gleichen Zeit bereitgestellt werden können, enthält die ursprüngliche Meldung die zu jenem Zeitpunkt verfügbaren Informationen; weitere Informationen werden ohne unangemessene Verzögerung nachgereicht.

6.2 Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie erforderlichenfalls bei Durchführung einer Datenschutzfolgenabschätzung zu unterstützen. Alle erforderlichen Angaben und Dokumentationen sind dem Auftraggeber auf Anforderung unverzüglich zur Verfügung zu stellen.

6.3 Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer, den Auftraggeber im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen

ist. Die Kosten für eine solche Unterstützung, die über den normalen Betrieb der Software hinausgeht, trägt der Auftraggeber.

6.4 Die beim Auftragnehmer zur Verarbeitung eingesetzten Personen haben sich schriftlich zur Vertraulichkeit verpflichtet, wurden mit den relevanten Bestimmungen des Datenschutzes vertraut gemacht und werden hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht.

6.5 Der Auftragnehmer wird den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten unterstützen.

6.6 Der Auftragnehmer hat einen Datenschutzbeauftragten bestellt. Die Kontaktdaten des Datenschutzbeauftragten des Auftragnehmers werden dem Auftraggeber auf Anfrage mitgeteilt und sind auf der Website des Auftragnehmers abrufbar. Änderungen werden dem Auftraggeber unverzüglich mitgeteilt.

## 7. Rechte und Pflichten des Auftraggebers

7.1 Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

7.2 Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang zu kontrollieren. Der Auftragnehmer stellt dem Auftraggeber alle hierfür erforderlichen Informationen zur Verfügung und gestattet die Prüfung der Verarbeitungstätigkeiten in angemessenen Abständen oder bei Anzeichen für eine Nichteinhaltung. Bei der Entscheidung über eine Prüfung kann der Auftraggeber einschlägige Zertifizierungen oder Auditberichte des Auftragnehmers berücksichtigen. Der Auftraggeber kann die Prüfung selbst durchführen oder durch unabhängige, zur Verschwiegenheit verpflichtete Prüfer, die mit dem Auftragnehmer nicht im Wettbewerb stehen, durchführen lassen. Die Prüfungen können auch Inspektionen in den Räumlichkeiten des Auftragnehmers umfassen und werden mit angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers durchgeführt, sowie nicht häufiger als alle 12 Monate, soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt. Die Kosten einer Vor-Ort-Prüfung trägt der Auftraggeber, soweit die Prüfung nicht aufgrund eines Verstoßes des Auftragnehmers veranlasst wurde.

## 8. Unterauftragsverarbeiter

8.1 Die Beauftragung von Unterauftragsverarbeitern durch den Auftragnehmer ist nur mit Zustimmung des Auftraggebers zulässig. Der Auftraggeber stimmt der Beauftragung von Unterauftragsverarbeitern gemäß der Übersicht Unterauftragsverarbeiter, die in der jeweils aktuellen Fassung unter www.cleverone.io/legal abrufbar ist.

8.2 Der Auftragnehmer kann die Beauftragung einzelner Unterauftragsverarbeiter beenden oder zusätzliche Unterauftragsverarbeiter beauftragen. Der Auftragnehmer wird den Auftraggeber bei der Beauftragung zusätzlicher Unterauftragsverarbeiter auf elektronischem Wege mindestens 30 Tage vor Einsatz des zusätzlichen Unterauftragsverarbeiters über dessen geplanten Einsatz informieren. Der Auftraggeber ist verpflichtet, zu diesem Zweck eine E-Mail-Adresse anzugeben.

8.2.1 Sollte der Auftraggeber einen wesentlichen Grund haben, dem Einsatz eines Unterauftragsverarbeiters zu widersprechen, wird der Auftraggeber dies dem Auftragnehmer spätestens 15 Tage nach der Information über den geplanten Einsatz des Unterauftragsverarbeiters schriftlich und unter Nennung des wesentlichen Grundes mitteilen. Sollte der Auftraggeber innerhalb dieser Zeitspanne nicht widersprechen, so wird der Einsatz des zusätzlichen Unterauftragsverarbeiters als vom Auftraggeber genehmigt angesehen.

8.2.2 Sollte der Auftraggeber widersprechen, kann der Auftragnehmer den Widerspruch wie folgt heilen: (1.) Der Auftragnehmer wird den zusätzlichen Unterauftragsverarbeiter für die Verarbeitung personenbezogener Daten des Auftraggebers nicht einsetzen, oder (2.) der Auftragnehmer wird Maßnahmen ergreifen, um den wesentlichen Grund für den Widerspruch des Auftraggebers auszuräumen, oder (3.) der Auftragnehmer kann die Erbringung des von dem Einsatz des zusätzlichen Unterauftragsverarbeiters betroffenen Aspekts der Leistung gegenüber dem Auftraggeber vorübergehend oder dauerhaft einstellen und dem Auftraggeber die für die Erbringung des Aspekts der Leistung eventuell bereits vorab gezahlte Vergütung zurückerstatten. Sollte keine dieser drei Optionen machbar sein und wurde dem Widerspruch nicht innerhalb von 15 Tagen nach Zugang des Widerspruchs abgeholfen, kann jede Partei den Hauptvertrag mit angemessener Frist außerordentlich kündigen.

8.2.3 Notfallersetzungen eines Unterauftragsverarbeiters können erforderlich werden, wenn die Erforderlichkeit des sofortigen Einsatzes eines zusätzlichen Unterauftragsverarbeiters außerhalb der Kontrolle des Auftragnehmers liegt, beispielsweise wenn ein Unterauftragsverarbeiter überraschend den Geschäftsbetrieb einstellt oder seine wesentlichen Vertragspflichten gegenüber dem Auftragnehmer verletzt, so dass es dem Auftragnehmer nicht mehr möglich ist/wäre, die gegenüber dem Auftraggeber geschuldete Leistung zu erbringen. In einem solchen Fall wird der Auftragnehmer den Kunden unverzüglich über den zusätzlichen Unterauftragsverarbeiter informieren und der Widerspruchsprozess, wie oben definiert, wird mit der Information des Auftraggebers eingeleitet.

8.3 Der Auftragnehmer hat die Unterauftragsverarbeiter sorgfältig auszuwählen und vor der Beauftragung zu prüfen, dass diese die zwischen Auftraggeber und Auftragnehmer getroffenen Vereinbarungen einhalten können. Der Auftragnehmer hat insbesondere zu kontrollieren, dass sämtliche Unterauftragsverarbeiter die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten getroffen haben.

8.4 Nicht als Unterauftragsverarbeitung im Sinne dieser AVV sind Dienstleistungen anzusehen, die der Auftragnehmer bei Dritten als reine Nebenleistung in Anspruch nimmt, um die geschäftliche Tätigkeit auszuüben.

8.5 Die Beauftragung von Unterauftragsverarbeitern lässt die vertraglichen und datenschutzrechtlichen Verpflichtungen des Auftragnehmers gegenüber dem Auftraggeber unberührt. Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Unterauftragsverarbeiter seinen Pflichten gemäß dem mit dem Auftragnehmer geschlossenen Vertrag nachkommt. Der Auftragnehmer benachrichtigt den Auftraggeber, wenn der Unterauftragsverarbeiter seine vertraglichen Pflichten nicht erfüllt.

## 9. Löschung und Rückgabe von personenbezogenen Daten

9.1 Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

9.2 Nach Beendigung der Leistungsvereinbarung löscht der Auftragnehmer nach Wahl des Auftraggebers alle im Auftrag verarbeiteten personenbezogenen Daten und bescheinigt dem Auftraggeber, dass dies erfolgt ist, oder er gibt alle personenbezogenen Daten an den Auftraggeber zurück und löscht bestehende Kopien, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht. Der Auftraggeber teilt dem Auftragnehmer seine Wahl spätestens bis zur Beendigung der Leistungsvereinbarung mit; erfolgt keine Mitteilung, erfolgt eine Löschung der Daten automatisiert 4 Wochen nach Beendigung der Leistungsvereinbarung. Bis zur Löschung oder Rückgabe der Daten gewährleistet der Auftragnehmer weiterhin die Einhaltung dieser AVV.

9.3 Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend den jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren.

## 10. Schlussbestimmungen

Sollten die Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren. Der Auftragnehmer wird die Gläubiger über die Tatsache, dass es sich um Daten handelt, die im Auftrag verarbeitet werden, unverzüglich informieren.

# Anlage 1 zur Vereinbarung Auftragsverarbeitung: Beschreibung der Auftragsverarbeitung

## 1. Gegenstand, Art und Zweck der Verarbeitung

Der Auftragnehmer stellt dem Auftraggeber seine All-in-One-SaaS-Plattform für das Management von Bestattungsunternehmen als SaaS-Lösung zur Verfügung. Er wird dabei als Auftragsverarbeiter für den Auftraggeber tätig. Der im Hauptvertrag bezeichnete Auftraggeber ist Verantwortlicher im Sinne der DSGVO und nutzt die SaaS-Plattform des Auftragnehmers zur Erhebung und Verarbeitung personenbezogener Daten.

## 2. Betroffene Personen

Die im Auftrag verarbeiteten personenbezogenen Daten betreffen folgende Kategorien betroffener Personen:

- Derzeitige und frühere Mitarbeiter des Auftraggebers
- Derzeitige und frühere Mitarbeiter von Geschäftspartnern des Auftraggebers
- Interessenten und Kunden des Auftraggebers und deren Angehörige
- Nutzer des Kunden- und Gedenkportals des Auftraggebers, soweit es sich um natürliche Personen handelt, die über diese Portale Inhalte beisteuern oder Leistungen in Anspruch nehmen

## 3. Kategorien von Daten

Die im Auftrag verarbeiteten personenbezogenen Daten gehören zu folgenden Datenkategorien:

- Stammdaten von Mitarbeitern des Auftraggebers und dessen Geschäftspartnern: Name, Vorname, Titel, Arbeitgeber, E-Mail-Adresse, Telefonnummer
- Beschäftigtendaten von Mitarbeitern des Auftraggebers und von Mitarbeitern von Dienstleistern des Auftraggebers einschließlich Nutzungsdaten, Disposition, Urlaubsansprüche und Aufgabenzuweisungen
- Bei Nutzung der App GPS-Tracking/Geolokalisierung der Mitarbeiter des Auftraggebers einschließlich Echtzeit-Standortdaten in der Kartenansicht der Disposition
- Stammdaten von Interessenten und Kunden des Auftraggebers, von deren Angehörigen sowie von sonstigen Dritten, die über das Kunden- oder Gedenkportal Inhalte beisteuern: Name, Vorname, Anschrift, Geburtsdaten, Kontaktdaten, Bilder, Videos, nutzergenerierte Inhalte (Texte, Beiträge, hochgeladene Dokumente und Musikdateien)
- Vertrags- und Abrechnungsdaten, angefragte bzw. in Anspruch genommene Leistungen, Bestelldaten aus dem digitalen Produktkatalog sowie Rechnungs- und Buchhaltungsdaten der Kunden des Auftraggebers bzw. von deren Angehörigen
- Zahlungs- und Bankdaten (insbesondere IBAN, Steuernummern) von Kunden des Auftraggebers und deren Angehörigen, soweit diese im Rahmen der Buchhaltungs- und Abrechnungsfunktionen der Software verarbeitet werden
- Bei Nutzung der Funktion „Digitale Unterschrift“: Signaturmetadaten (IP-Adresse, Zeitstempel, Geräte- und Browserinformationen des Unterzeichners)
- Bei Nutzung des Abmeldeservices: Daten, die für die Kündigung oder Abmeldung von Verträgen bei Dritten erforderlich sind (insbesondere Vertragsnummern, Kundennummern, Anschriften, ggf. Bankverbindungen)
- Bei Nutzung des Trauerdruckmoduls: Inhalte der Trauerdruckerzeugnisse (Texte, Lebensläufe, Fotos, religiöse Bezugnahmen, Bestattungs- und Trauerfeiertermine und -orte)

- Daten im Zusammenhang mit der Sterbefallverwaltung, soweit sie sich auf lebende und natürliche Personen beziehen oder im Rahmen der Bestattungsvorsorge von den Betroffenen selbst erhoben wurden (insbesondere Konfession, Familienstand); Daten Verstorbener unterfallen als solche nicht dem Anwendungsbereich der DSGVO, können jedoch personenbezogene Daten lebender Angehöriger enthalten
- Fotodokumentation aus digitalen Arbeitsaufträgen der Mitarbeiter-App
- Bei Nutzung des KI-Assistenten „Cleo“: Prompts, Chat-Verläufe, Spracheingaben (Audio-Aufnahmen), hochgeladene Dokumente zur KI-Verarbeitung sowie dauerhaft gespeicherte Erinnerungen, soweit diese personenbezogenen Daten lebender natürlicher Personen enthalten; Daten Verstorbener unterfallen als solche nicht dem Anwendungsbereich der DSGVO
- Korrespondenz- und Kommunikationsdaten: E-Mail-Inhalte, Briefvorlagen und Formulare einschließlich der darin enthaltenen personenbezogenen Daten (Absender, Empfänger, Nachrichteninhalte, Zeitstempel), soweit diese über die Software erstellt oder versendet werden
- Sozialversicherungsnummern, Rentenversicherungsnummern und Krankenversicherungsdaten, soweit diese im Rahmen der Personen- oder Sterbefallverwaltung für lebende natürliche Personen oder im Rahmen der Bestattungsvorsorge erhoben werden
- Bei Nutzung der bema-Schnittstelle (Vorsorge Portal): Kopien von Ausweisdokumenten (Personalausweis, Reisepass, Aufenthaltsgenehmigung) sowie ggf. Vollmachten und Betreuerausweise im Rahmen der digitalen Identitätsprüfung

## 4. Dauer der Auftragsverarbeitung

Die Dauer der Auftragsverarbeitung entspricht der Laufzeit des Hauptvertrages.

# Anlage 2 zur Vereinbarung Auftragsverarbeitung: Technische und organisatorische Maßnahmen

## 1. Vertraulichkeit

### 1.1 Zutrittskontrolle

**Hosting/Rechenzentrum:**

Das Hosting der Server wird von AWS in Frankfurt am Main bereitgestellt. Der Zugang wird per Vereinzelungsanlage sichergestellt. Weiterhin ist das gesamte Gelände außerhalb und innerhalb der Rechenzentren durch Videoüberwachung und 365x7x24 Sicherheitspersonal geschützt.

Details: https://aws.amazon.com/de/trust-center/data-center/our-controls/

**Büroräume:**

Die Büroräume des Auftragnehmers befinden sich in einem Bürohaus. Die Zugänge zum Bürohaus und auch zu den Büroräumen des Auftragnehmers sind während der Bürozeiten dauerhaft besetzt und während der Nacht verschlossen. Zugang zu dem Bürohaus haben nur der Vermieter und die Mieter der Büroräume. Es kommt ein Schließsystem zum Einsatz, das vom Vermieter verwaltet wird. Jeder Mieter des Bürohauses hat jedoch die Möglichkeit, die jeweils ausgehändigten Schlüssel selbst zu verwalten und Zutrittsrecht zu erteilen und zu entziehen. Dies wird von der Personalabteilung des Auftragnehmers verwaltet.

Die Schlüsselvergabe und das Schlüsselmanagement erfolgt nach einem definierten Prozess, der sowohl zu Beginn eines Arbeitsverhältnisses als auch zum Ende eines Arbeitsverhältnisses die Erteilung bzw. den Entzug von Zutrittsberechtigungen für Räume regelt.

Zutrittsberechtigungen werden einem Beschäftigten erst erteilt, wenn dies durch den jeweiligen Vorgesetzten und/oder die Personalabteilung angefordert wurde. Bei der Vergabe von Berechtigungen wird dem Grundsatz der Erforderlichkeit Rechnung getragen.

Besucher können den Empfang betreten, erhalten erst Zutritt zu den Büroräumen nach vorheriger Anmeldung.

Jeder Besucher wird von der Empfangsperson zu seinem jeweiligen Ansprechpartner begleitet.

Die Büroräume sind am Tag als auch in der Nacht per Videoaufzeichnung überwacht. Die Besucher werden per Hinweis darüber aufgeklärt. Die Aufbewahrung erfolgt nach den Vorgaben der DSGVO.

### 1.2 Zugangskontrolle

Um Zugang zu IT-Systemen zu erhalten, müssen Nutzer über eine entsprechende Zugangsberechtigung verfügen. Hierzu werden entsprechende Benutzerberechtigungen von Administratoren vergeben. Dies jedoch nur, wenn dies von dem jeweiligen Vorgesetzten beantragt wurde. Die Vergabe und Änderung von Benutzerberechtigungen unterliegt einer Passwortrichtlinie, die unter anderem die Wiederverwendung von Passwörtern verhindert.

Fehlerhafte Anmeldeversuche werden protokolliert. Bei mehrmaliger Fehleingabe erfolgt eine Sperrung des jeweiligen Benutzer-Accounts.

Remote-Zugriffe auf IT-Systeme des Auftragnehmers erfolgen stets über verschlüsselte SSL-Verbindungen.

Alle Server sind durch Firewalls geschützt, die stets gewartet und mit Updates und Patches versorgt werden.

Der Zugriff von Servern und Clients auf das Internet und der Zugriff auf diese Systeme über das Internet ist ebenfalls durch Firewalls gesichert. So ist auch gewährleistet, dass nur die für die jeweilige Kommunikation erforderlichen Ports nutzbar sind. Alle anderen Ports sind entsprechend gesperrt.

Alle Mitarbeiter sind angewiesen, ihre IT-Systeme zu sperren, wenn sie diese verlassen.

Passwörter werden grundsätzlich verschlüsselt gespeichert.

### 1.3 Zugriffskontrolle

Berechtigungen für IT-Systeme und Applikationen des Auftragnehmers werden ausschließlich von Administratoren eingerichtet.

Berechtigungen werden nach dem Need-to-Know-Prinzip vergeben. Es erhalten demnach nur die Personen Zugriffsrechte auf Daten, Datenbanken oder Applikationen, die diese Daten, Anwendungen oder Datenbanken warten und pflegen bzw. in der Entwicklung tätig sind. Voraussetzung ist eine entsprechende Anforderung der Berechtigung für einen Mitarbeiter durch einen Vorgesetzten.

Es gibt ein rollenbasiertes Berechtigungskonzept mit der Möglichkeit der differenzierten Vergabe von Zugriffsberechtigungen, das sicherstellt, dass Beschäftigte abhängig von ihrem jeweiligen Aufgabengebiet und ggf. projektbasiert Zugriffsrechte auf Applikationen und Daten erhalten.

Beschäftigten ist es grundsätzlich untersagt und auch per Richtline nicht möglich, nicht genehmigte Software auf den IT-Systemen zu installieren.

Alle Server- und Client-Systeme werden regelmäßig mit Sicherheits-Updates aktualisiert.

### 1.4 Trennung

Alle vom Auftragnehmer für Kunden eingesetzten IT-Systeme sind mandantenfähig. Die logische Zuordnung der im Auftrag eines Kunden verarbeiteten Daten zu dem jeweiligen Kunden und damit die logische Trennung der Daten ist stets gewährleistet.

### 1.5 Pseudonymisierung & Verschlüsselung

Ein administrativer Zugriff auf Serversysteme erfolgt grundsätzlich über verschlüsselte Verbindungen.

## 2. Integrität

### 2.1 Eingabekontrolle

Die Eingabe, Änderung und Löschung von personenbezogenen Daten, die vom Auftragnehmer im Auftrag verarbeitet werden, wird protokolliert.

Mitarbeiter sind verpflichtet, stets mit ihren eigenen Accounts zu arbeiten. Benutzeraccounts dürfen nicht mit anderen Personen geteilt bzw. gemeinsam genutzt werden.

### 2.2 Weitergabekontrolle

Eine Weitergabe von personenbezogenen Daten, die im Auftrag von Kunden des Auftragnehmers erfolgt, darf jeweils nur in dem Umfang erfolgen, wie dies mit dem Kunden abgestimmt oder soweit dies zur Erbringung der vertraglichen Leistungen für den Kunden erforderlich ist.

Alle Mitarbeiter, die in einem Kundenprojekt arbeiten, werden im Hinblick auf die zulässige Nutzung von Daten und die Modalitäten einer Weitergabe von Daten instruiert.

Soweit möglich werden Daten verschlüsselt an Empfänger übertragen.

Die Nutzung von privaten Datenträgern ist den Beschäftigten des Auftragnehmers untersagt.

Mitarbeiter des Auftragnehmers werden regelmäßig zu Datenschutzthemen geschult. Alle Mitarbeiter sind auf zu einem vertraulichen Umgang mit personenbezogenen Daten verpflichtet worden.

## 3. Verfügbarkeit und Belastbarkeit

Die Daten auf den Servern beim Hosting Provider AWS werden täglich als Full Backup gesichert.

Die Daten auf den internen Systemen des Auftragnehmers werden täglich inkrementell und monatlich als Full Backup per eigenem VLAN gesichert. Die Sicherungsmedien werden verschlüsselt an einen physisch getrennten Ort gespeichert. Der Backupserver befindet sich in einem separatem Brandschott. Das Einspielen von Backups wird regelmäßig getestet.

Die Systeme verfügen über eine unterbrechungsfreie Stromversorgung. Im Rechenzentrum befindet sich eine Brandmeldeanlage sowie eine Löschanlage. Alle Systeme unterliegen einem Monitoring, das im Falle von Störungen unverzüglich Meldungen an einen Administrator auslöst.

Es besteht ein Notfallplan, der auch einen Wiederanlaufplan beinhaltet.

## 4. Auftragskontrolle

Die Software des Auftragnehmers wird in der Europäischen Union gehostet.

Bei der Einbindung von externen Dienstleistern oder Dritten wird entsprechend den Vorgaben des Art. 28 DSGVO ein Auftragsverarbeitungsvertrag nach zuvor durchgeführtem Audit abgeschlossen. Auftragnehmer werden auch während des Vertragsverhältnisses regelmäßig kontrolliert.

## 5. Privacy by Design und Privacy by Default

Es wird schon bei der Entwicklung der Software Sorge dafür getragen, dass dem Grundsatz der Erforderlichkeit Rechnung getragen wird. Die Art der Datenerhebung mittels der Software und die zu erhebenden Datenkategorien können vom Auftraggeber individuell angepasst und verwaltet werden.

Die Software des Auftragnehmers unterstützt die Eingabekontrolle durch einen flexiblen und anpassbaren Audit-Trail, der eine unveränderliche Speicherung von Änderungen an Daten und Nutzerberechtigungen ermöglicht. Berechtigungen auf Daten oder Applikationen können gesetzt werden.

## 6. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Der Auftragnehmer hat ein Datenschutzmanagement implementiert. Es gibt eine Leitlinie zu Datenschutz und Datensicherheit und Richtlinien, mit denen die Umsetzung der Ziele der Leitlinie gewährleistet wird.

Es ist Datenschutz- und Informationssicherheits-Team (DST) eingerichtet, das Maßnahmen im Bereich von Datenschutz und Datensicherheit plant, umsetzt, evaluiert und Anpassungen vornimmt. Die Richtlinien werden regelmäßig im Hinblick auf ihre Wirksamkeit evaluiert und angepasst.
Es ist insbesondere sichergestellt, dass Datenschutzvorfälle von allen Mitarbeitern erkannt und unverzüglich dem DST gemeldet werden. Dieses wird den Vorfall sofort untersuchen. Soweit Daten betroffen sind, die im Auftrag von Kunden verarbeitet werden, wird Sorge dafür getragen, dass diese unverzüglich über Art und Umfang des Vorfalls informiert werden.