Vertrag zur Auftragsverarbeitung

Die Viaplano GmbH (nachfolgend "Auftragsverarbeiter" genannt) erbringt für den Kunden (nachfolgend „Verantwortlicher“ genannt) Leistungen im Zusammenhang mit der Bereitstellung der SaaS-Anwendung „Viaplano“ auf Grundlage gesondert vereinbarter Vertragsbedingungen (nachfolgend „Hauptvertrag“ genannt). Dabei erhält der Auftragsverarbeiter Zugriff auf personenbezogene Daten des Verantwortlichen. Zur Konkretisierung der beiderseitigen datenschutzrechtlichen Rechte und Pflichten schließen der Verantwortliche und der Auftragsverarbeiter diesen Vertrag. Die Regelungen des Vertrages zur Auftragsverarbeitung gehen im Zweifel den Regelungen des Hauptvertrages vor.

§ 1 Laufzeit

Die Laufzeit dieses Vertrages richtet sich nach der Dauer der Verarbeitung.

§ 2 Gegenstand der Verarbeitung

Der Gegenstand der Verarbeitung ergibt sich aus dem Hauptvertrag.

§ 3 Dauer der Verarbeitung

(1) Die Dauer der Verarbeitung richtet sich nach der Laufzeit des Hauptvertrages.

(2) Die Verarbeitung kann über die Laufzeit des Hauptvertrages hinaus bis zur Rückgabe und Löschung bzw. Vernichtung der personenbezogenen Daten des Verantwortlichen andauern.

§ 4 Art der Verarbeitung

Die Art der Verarbeitung ergibt sich aus dem Hauptvertrag.

§ 5 Zweck der Verarbeitung

Der Zweck der Verarbeitung ergibt sich aus dem Hauptvertrag.

§ 6 Art der personenbezogenen Daten

Die Art der personenbezogenen Daten bestimmt der Verantwortliche durch den Umfang der konkreten Nutzung unter Beachtung der Vorgaben des Hauptvertrages. Insbesondere betroffen sind folgende Arten personenbezogener Daten:

- Adressdaten
- Beschäftigtendaten
- Kontaktdaten

- IT-Nutzungsdaten

§ 7 Kategorien betroffener Personen

Die Kategorien der von der Verarbeitung betroffenen Personen bestimmt der Verantwortliche durch den Umfang der konkreten Nutzung unter Beachtung der Vorgaben des Hauptvertrages. Insbesondere sind folgende Kategorien von Personen betroffen:

- Mitarbeiter und Beschäftigte des Verantwortlichen

§ 8 Weisungsrecht

(1) Der Auftragsverarbeiter darf personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten; dies gilt insbesondere in Bezug auf die Übermittlung personenbezogener Daten in ein Drittland oder an eine internationale Organisation. Wird der Auftragsverarbeiter durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem er unterliegt, zu weiteren Verarbeitungen verpflichtet, teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen des Verantwortlichen werden anfänglich durch diesen Vertrag und den Hauptvertrag festgelegt und können vom Verantwortlichen danach in Schriftform oder in Textform durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Alle erteilten Weisungen sind sowohl vom Verantwortlichen als auch vom Auftragsverarbeiter zu dokumentieren.

(3) Dem Verantwortlichen obliegt die Beurteilung der Zulässigkeit der Verarbeitung. Ist der Auftragsverarbeiter jedoch der Ansicht, dass eine Weisung des Verantwortlichen gegen datenschutzrechtliche Bestimmungen verstößt, hat er den Verantwortlichen unverzüglich darauf hinzuweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung so lange auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird. Der Auftragsverarbeiter darf die Durchführung einer offensichtlich rechtswidrigen Weisung ablehnen.

§ 9 Verpflichtung zur Vertraulichkeit

Der Auftragsverarbeiter gewährleistet, dass sich die von ihm mit der Verarbeitung von personenbezogenen Daten betrauten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

§ 10 Sicherheit der Verarbeitung

Der Auftragsverarbeiter trifft alle erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DS-GVO zum angemessenen Schutz der personenbezogenen Daten des

Verantwortlichen, insbesondere mindestens die in der Anlage aufgeführten Maßnahmen. Eine Änderung der getroffenen Maßnahmen bleibt dem Auftragsverarbeiter vorbehalten, wobei er sicherstellt, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Über wesentliche Änderungen der Maßnahmen hat der Auftragsverarbeiter den Verantwortlichen unverzüglich zu unterrichten.

§ 11 Weitere Auftragsverarbeiter

(1) Die im Hauptvertrag vereinbarten Leistungen bzw. die nachfolgend beschriebenen Teilleistungen werden unter Einschaltung der im Folgenden genannten weiteren Auftragsverarbeiter durchgeführt:

- dogado GmbH, Antonio-Segni-Straße 11, 44263 Dortmund (Hosting)
- Dustin Hagemeier (Einzelunternehmer), Escher Straße 221, 50739 Köln (Administration und Fernwartung)

(2) Der Auftragsverarbeiter ist im Rahmen seiner vertraglichen Verpflichtungen zur Begründung von Unterauftragsverhältnissen mit weiteren Auftragsverarbeitern befugt. Er setzt den Verantwortlichen hiervon unverzüglich in Kenntnis, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Der Auftragsverarbeiter ist verpflichtet, weitere Auftragsverarbeiter sorgfältig nach deren Eignung und Zuverlässigkeit auszuwählen. Der Auftragsverarbeiter hat bei der Einschaltung von weiteren Auftragsverarbeitern diese entsprechend den Regelungen dieses Vertrages zu verpflichten und dabei sicherzustellen, dass der Verantwortliche seine Rechte aus diesem Vertrag (insbesondere seine Kontrollrechte) auch direkt gegenüber den weiteren Auftragsverarbeitern wahrnehmen kann. Sofern eine Einbeziehung von weiteren Auftragsverarbeitern in einem Drittland erfolgen soll, hat der Auftragsverarbeiter sicherzustellen, dass ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standardvertragsklauseln).

(3) Erhebt der Verantwortliche gegen die Hinzuziehung oder Ersetzung eines Unterauftragnehmers Einspruch, obwohl der Auftragsverarbeiter sämtliche vorgenannten Voraussetzungen erfüllt und keine nicht datenschutzkonforme Verarbeitung droht, so ist der Auftragsverarbeiter berechtigt, das Vertragsverhältnis mit angemessener Frist zu kündigen.

(4) Unterauftragsverhältnisse mit weiteren Auftragsverarbeitern im Sinne dieser Bestimmungen liegen nicht vor, wenn der Auftragsverarbeiter Dritte mit Dienstleistungen beauftragt, die als reine Nebenleistungen anzusehen sind. Dazu gehören z. B. Post-, Transport- und Versandleistungen, Reinigungsarbeiten, Telekommunikationsleistungen und Bewachungsdienste ohne konkreten Bezug zu Leistungen, die der Auftragsverarbeiter für den Verantwortlichen erbringt.

§ 12 Unterstützungspflichten

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen angesichts der Art der Verarbeitung nach Möglichkeit mit geeigneten technischen und organisatorischen Maßnahmen dabei, seiner Pflicht zur Beantwortung von Anträgen auf Wahrnehmung der in Kapitel III der DS-GVO genannten Rechte der betroffenen Personen nachzukommen.

(2) Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der dem Auftragsverarbeiter zur Verfügung stehenden Informationen bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DS-GVO.

§ 13 Rückgabe und Löschung bzw. Vernichtung

Der Auftragsverarbeiter wird nach Beendigung des Hauptvertrages alle personenbezogenen Daten nach Wahl des Verantwortlichen entweder löschen bzw. vernichten oder zurückgeben und die vorhandenen Kopien löschen bzw. vernichten, sofern nicht nach dem Unionsrecht oder dem Recht der Mitgliedstaaten eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

§ 14 Kontrollrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen auf Verlangen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten des Auftragsverarbeiters nach diesem Vertrag und nach Art. 28 DS-GVO zur Verfügung.

(2) Der Auftragsverarbeiter ermöglicht dem Verantwortlichen hierzu auch Überprüfungen - einschließlich Inspektionen -, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, und trägt zu diesen bei. Der Verantwortliche wird Überprüfungen nur im erforderlichen Umfang durchführen und die Betriebsabläufe des Auftragsverarbeiters dabei nicht unverhältnismäßig stören.

Anlage: Technische und organisatorische Maßnahmen

(1) Organisationskontrolle

- Verpflichtung der Beschäftigten zur Vertraulichkeit
- Benennung eines Ansprechpartners für den Datenschutz
- Regelmäßige Auditierung der technischen und organisatorischen Maßnahmen zum Datenschutz

(2) Zutrittskontrolle

- Einfriedung/Einzäunung des Grundstücks
- Toranlage
- Bewegungsmelder
- Videoüberwachung
- Einbruchmeldeanlage/Alarmanlage
- Zu- und Ausgänge des Gebäudes sind von außen nicht zu öffnen
- Sicherung der Fenster, Kellerfenster, Lichtschächte
- Schlüsseldokumentation
- Sichere Verwahrung von Ersatzkarten/Ersatzschlüsseln
- Prozess zur Aufhebung nicht mehr benötigter Zutrittsrechte
- Abschließbare Büroräume

(3) Zugangskontrolle (Datenverarbeitungsanlagen auf Netz- und Serverebene)

- (Verschlüsselte) Identifikation und Authentifikation von Benutzern
- Passwortregeln vorhanden (Mindestlänge, Zeichensatz, Gültigkeitsdauer, Ausschluss von Trivialkennworten etc.)
- Vorläufig vergebene Passwörter werden unverzüglich durch sichere Individualpasswörter ersetzt
- Sperrung bei wiederholter Fehleingabe von Passwörtern
- Freigabe nur durch Administrator/Freigabe nach Zeitablauf/Freigabe gestaffelt nach Versuchen
- Sperre von Endgeräten beim Verlassen
- Hardware-Firewall/Software-Firewall vorhanden
- Updates für Firewall werden regelmäßig automatisch/manuell installiert
- Anti-Virus-Software vorhanden
- Updates für Anti-Virus-Software werden regelmäßig automatisch/manuell installiert
- Sicherheitseinstellungen der Browser werden gezielt angewendet
- Regelmäßiges automatisches/manuelles Einspielen von Sicherheitspatches und/oder -updates bei Browsern
- Access Point zugriffs- und diebstahlsicher installiert
- Sicherheitsmaßnahmen WLAN
- Sicherungsmaßnahmen bei Zugang von extern zum Firmennetz

- Keine Speicherung von sensiblen Daten auf mobilen Endgeräten
- Sichere Löschung von Datenträgern vor deren Wiederverwendung

(4) Zugriffskontrolle (Datenverarbeitungsanlagen)

- Aktive Netzkomponenten (Switches etc.) sind zugriffssicher untergebracht
- Nur Verwendung von geprüften und zugelassenen/freigegebenen mobilen Datenträgern
- Prüfung auf zugelassene/freigegebene mobile Datenträger bei Anschluss
- Sichere Aufbewahrung von mobilen Datenträgern
- Kein Zugriff durch Benutzer auf Systemebene möglich
- Installation und Ausführung neuer Programme durch Benutzer nicht möglich

(5) Weitergabekontrolle

- Regelmäßiges automatisches/manuelles Einspielen von Sicherheitspatches und/oder -updates bei E-Mail-Programmen
- Sicherheitseinstellungen der E-Mail-Programme werden gezielt angewendet
- Prozess zur sicheren Löschung/Vernichtung von Datenträgern/Unterlagen
- Regelmäßige datenschutzgerechte Löschung/Vernichtung von Datenträgern/Unterlagen, deren Aufbewahrungspflicht abgelaufen ist
- Einsatz von Aktenvernichtern

(6) Eingabekontrolle

- Protokollierung der Einrichtung und des Betriebes von IT-Systemen
- Protokollierung der Einrichtung/Änderung von Benutzern und Rechten
- Protokollierung von Systemänderungen
- Protokollierung von Eingaben und Veränderungen
- Systemüberwachung

(7) Auftragskontrolle

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich des Datenschutzes)
- Vorherige Prüfung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen
- Abschluss eines Vertrages oder eines anderen Rechtsinstruments nach Art. 28 DSGVO und Einhaltung dieser Regularien
- Vertraglich festgelegte Verantwortlichkeiten

(8) Verfügbarkeitskontrolle

- Ausfallschutz durch gespiegelte Plattenlaufwerke, RAID-System etc.
- Backup-Konzept
- Regelmäßige automatisierte/manuelle Datensicherungen

- Sichere Übertragung/Transport von Datensicherungen/Sicherungsdatenträgern
- Überprüfung der Sicherungsdaten auf Vollständigkeit und Lesbarkeit
- Überwachung der Sicherungsdatenträger bezüglich ihrer Haltbarkeit/Anzahl der zulässigen Schreibzyklen
- Recovery-Konzept
- Prüfung der Rekonstruierbarkeit der Datenbestände durch regelmäßige Tests
- Unterbrechungsfreie Stromversorgung
- Regelmäßige Tests der unterbrechungsfreien Stromversorgung nach Herstellervorschrift auf Funktionsfähigkeit und Dokumentation der Tests

(9) Maßnahmen zur regelmäßigen Evaluation der Sicherheit der Datenverarbeitung

- Regelmäßige Revision des Sicherheitskonzepts