Vertrag zur Auftragsverarbeitung

Präambel

Die meibers.rechtsanwälte Rechtsanwaltsgesellschaft mbH (nachfolgend "Auftragsverarbeiter" genannt) erbringt für den Verantwortlichen Leistungen auf Grundlage der gesondert vereinbarten Nutzungsbedingungen (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

Die Verarbeitung hat folgenden Gegenstand: Bereitstellung eines Text-Konfigurators als Cloud-Lösung.

§ 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 Verarbeitung erfolgt auf folgende Art:

- Erheben
- Erfassen
- Organisation
- Ordnen

- Speicherung
- Verwendung
- Löschen
- Vernichtung

§ 5 Zweck der Verarbeitung

Die Verarbeitung erfolgt zu folgendem Zweck: Verwaltung von individuellen Rechts- und Vertragstexten.

§ 6 Art der personenbezogenen Daten

Gegenstand der Verarbeitung ist folgende Art personenbezogener Daten:

- Adressdaten (Straße, Hausnummer, Postleitzahl, Ort etc.)
- IT-Nutzungsdaten (IP-Adresse, Verkehrsdaten, Server-Log etc.)
- Kontaktdaten (Telefonnummer, Faxnummer, Mailadresse etc.)
- Namen (Nachname, Vorname etc.)
- Persönliche Daten (Geschlecht, Geburtsdatum, Geburtsort, Familienstand, Staatsangehörigkeit etc.)

§ 7 Kategorien betroffener Personen

Gegenstand der Verarbeitung sind folgende Kategorien betroffener Personen:

- Auftraggeber
- Auftragnehmer
- Beschäftigte
- Ehemalige Beschäftigte
- Geschäftspartner
- Interessenten
- Kunden
- Lieferanten

§ 8 Weisungsrecht

(1) Der Auftragsverarbeiter darf personenbezogene Daten nur auf 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 Datenverarbeitung. 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 solange 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 wird alle Personen, die von ihm mit der Verarbeitung von personenbezogenen Daten betraut werden, zur Vertraulichkeit verpflichten (Art. 28 Abs. 3 lit. b DS-GVO).

§ 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 Änderung 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:

meibers.datenschutz GmbH
Haus Sentmaring 9
48151 Münster
Leistung: Rechenzentrumsdienstleistungen

(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 beim jeweiligen weiteren Auftragsverarbeiter ein angemessenes Datenschutzniveau gewährleistet ist (z. B. durch Abschluss einer Vereinbarung auf Basis der EU-Standardvertragsklauseln).

(3) 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

Organisationskontrolle

- Datenschutz-Management (Richtlinien, Betriebsvereinbarungen, Verfahrensanweisungen, etc.)
- Verpflichtung der Beschäftigten zur Vertraulichkeit
- Verpflichtung der Beschäftigten auf das Fernmeldegeheimnis
- Verpflichtung von externen Dienstleistern auf das Datengeheimnis, sofern es sich nicht um Auftragsverarbeiter handelt
- Benennung eines Datenschutzbeauftragten/Ansprechpartners für den Datenschutz

Zutrittskontrolle

Sicherungsmaßnahmen des Gebäudes:

- Bewegungsmelder (Beleuchtung)
- Zu- und Ausgänge des Gebäudes sind von außen nicht zu öffnen
- Sicherung der Fenster, Kellerfenster, Lichtschächte
- Besondere Sicherung der Türen
- Dokumentiertes Zutrittskontrollkonzept mit einer Festlegung und Dokumentation der berechtigten Personen
- Elektronisches Zutrittskontrollsystem für das Gebäude (Magnetstreifen/Speicherchip, RFID-Chip, Codeschloss, biometrisches Verfahren etc.)
- Kartendokumentation
- Schlüsseldokumentation
- Sichere Verwahrung von Ersatzkarten/Ersatzschlüsseln
- Prozess zur Aufhebung nicht mehr benötigter Zutrittsrechte

Sicherungsmaßnahmen innerhalb des Gebäudes/der Geschäftsräume:

- Videoüberwachung
- Bewegungsmelder (Beleuchtung)
- Einbruchmeldeanlage/Alarmanlage
- Zu- und Ausgänge der Geschäftsräume sind von außen nicht zu öffnen

- Besondere Sicherung der Türen
- Zentraler Empfangsbereich mit Personenkontrolle
- Besucherüberwachung (Elektronisches Besuchermanagementsystem, Besucherbuch, Begleitung durch Mitarbeiter etc.)
- Dokumentiertes Zutrittskontrollkonzept mit einer Festlegung und Dokumentation der berechtigten Personen
- Elektronisches Zutrittskontrollsystem für die Geschäftsräume (Magnetstreifen/Speicherchip, RFID-Chip, Codeschloss, biometrisches Verfahren etc.)
- Kartendokumentation
- Schlüsseldokumentation
- Sichere Verwahrung von Ersatzkarten/Ersatzschlüsseln
- Prozess zur Aufhebung nicht mehr benötigter Zutrittsrechte
- Abschließbare Büroräume

Sicherungsmaßnahmen der besonders sensiblen Räume (Geschäftsleitung, Personalabteilung, IT, Archive, RZ-/Serverraum, TK-Anlage, Verteilerräume, Archive, etc.):

- Videoüberwachung
- Bewegungsmelder (Beleuchtung)
- Einbruchmeldeanlage/Alarmanlage
- Zu- und Ausgänge der besonders sensiblen Räume sind von außen nicht zu öffnen
- Besondere Sicherung der Türen
- Closed-Shop-Betrieb
- Dokumentiertes Zutrittskontrollkonzept mit einer Festlegung und Dokumentation der berechtigten Personen
- Elektronisches Zutrittskontrollsystem für besonders sensible Räume (Magnetstreifen/Speicherchip, RFID-Chip, Codeschloss, biometrisches Verfahren etc.)
- Kartendokumentation
- Schlüsseldokumentation
- Sichere Verwahrung von Ersatzkarten/Ersatzschlüsseln
- Prozess zur Aufhebung nicht mehr benötigter Zutrittsrechte

Zugangskontrolle

- (Verschlüsselte) Identifikation und Authentifikation von Benutzern (User-ID und Passwort, Zweistufenauthentifizierung mit Magnet-/Chipkarte oder Token, biometrisches Verfahren etc.)

- Passwortregeln (Mindestlänge, Zeichensatz, Gültigkeitsdauer, Ausschluss von Trivialkennworten etc.)
- Automatisierte Kontrolle der Passwortregeln
- Vorläufig vergebene Passwörter werden unverzüglich durch sichere Individualpasswörter ersetzt
- Automatische Kontrolle der unverzüglichen Vergabe von Individualpasswörtern
- Sperrung bei wiederholter Fehleingabe von Passwörtern
- Freigabe nur durch Administrator/Freigabe nach Zeitablauf/Freigabe gestaffelt nach Versuchen
- Zugang ins Internet mit Administrationsrechten nicht möglich
- 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
- Einsatz von Intrusion-Detection-Systemen
- Regelmäßiges automatisches/manuelles Einspielen von Sicherheitspatches und/oder -updates bei Browsern
- Protokollierung von Internetnutzung
- Trennung von Firmennetz und Gäste-WLAN (Getrenntes Netzsegment mit Router, Firewall, Beschränkung von Zugriffsrechten etc.)
- Access Point zugriffs- und diebstahlsicher installiert
- Sicherheitsmaßnahmen WLAN (Standardeinstellungen, Standardbenutzernamen und Standardpasswörter durch sichere individuelle Einstellungen ersetzt, Verschlüsselungsverfahren, Log-Dateien werden regelmäßig ausgewertet, SSID Broadcast deaktiviert, MAC-Adressfilter aktiviert, regelmäßige Sicherheitschecks etc.)
- Sicherungsmaßnahmen bei Zugang von extern zum Firmennetz (Virtual Private Network (VPN), Protokollierung der externen Kommunikation, regelmäßige Sicherheitschecks von mobilen Endgeräten etc.)
- Kein Einsatz von privaten Endgeräten/kein BYOD
- Keine Speicherung von sensiblen Daten auf mobilen Endgeräten
- Sichere Löschung von Datenträgern vor deren Wiederverwendung

Zugriffskontrolle

- Aktive Netzkomponenten (Switches etc.) sind zugriffssicher untergebracht
- Nicht benötigte Diskettenlaufwerke, CD-Brenner, externe Schnittstellen (USB etc.) sind gesperrt

- Deaktivierung/Überwachung nicht benötigter Anschlussdosen
- Nur Verwendung von geprüften und zugelassenen/freigegebenen mobilen Datenträgern
- Transparenter User-Help-Desk (Explizite Freigabe durch Nutzer, Beendigung der Help-Desk-Sitzung erkennbar etc.)
- Rollenbasierte Berechtigungen wie Kategorien von Rollen und Rechte der Rollen, insbesondere nach „Lesen, Schreiben, Ausführen“
- Rollen- und Rechtekonzept mit einer Festlegung und Dokumentation der Rollen und Rechte der berechtigten Personen
- Prozess zur Aufhebung nicht mehr benötigter Rollen und Rechte
- Dokumentation der Änderung von Rollen und Rechten
- Regelmäßige Überprüfung der Erforderlichkeit der vergebenen Rollen und Rechte
- Kein Zugriff durch Benutzer auf Systemebene möglich
- Rechte und Privilegien von Programmen sind geregelt

Weitergabekontrolle

- Sensible Daten/Dokumente werden verschlüsselt/anonymisiert/pseudonymisiert übertragen/weitergegeben
- Identifizierung und Authentifizierung der Beteiligten bei der Datenübertragung (Benutzerkennung/Passwort etc.)
- Regelmäßiges automatisches/manuelles Einspielen von Sicherheitspatches und/oder -updates bei E-Mail-Programmen
- Sicherheitseinstellungen der E-Mail-Programme werden gezielt angewendet
- E-Mails mit sensiblen Inhalten werden verschlüsselt versendet (PKI, De-Mail, IBE (Identity-Based-Encryption) etc.), andernfalls wird der Empfänger vorab über die mangelhafte Sicherheit der unverschlüsselten E-Mail-Versendung informiert
- Einsatz von E-Mail-Contentfiltern
- Kein Einsatz von Web-Mail-Angeboten
- Geeignete Sicherungsmaßnahmen für den Transport von Datenträgern (Sicherungsbehälter, Sicherung der Daten durch Duplizierung, Verschlüsselung etc.)
- Prozess zur sicheren Löschung/Vernichtung von Datenträgern/Unterlagen (Protokollierung der Vernichtung etc.)
- Regelmäßige datenschutzgerechte Löschung/Vernichtung von Datenträgern/Unterlagen, deren Aufbewahrungspflicht abgelaufen ist

- Einsatz von Aktenvernichtern

Eingabekontrolle

- Protokollierung der Einrichtung und des Betriebes von IT-Systemen
- Protokollierung der Einrichtung/Änderung von Benutzern und Rechten (Dokumentation aller berechtigten Nutzer, Rechteprofile der berechtigten Nutzer, Dokumentation von Änderungen von Nutzern/Rechten, Dokumentation, wer die Benutzer und Rechte angeordnet/eingerichtet hat, Historie über die eingerichteten Nutzer und Rechte etc.)
- Protokollierung von Systemänderungen (Dokumentation von funktionalen Systemänderungen/Erweiterungen einschließlich Testfälle, Testung, Testergebnisse und Freigabe, Dokumentation von Versionsänderungen oder Änderungen der technischen Umgebung des IT-Systems, Änderungen der Dateiorganisation oder des Dateiverwaltungssystems etc.)
- Protokollierung von Eingaben und Veränderungen (Datum und Uhrzeit von Zugriffen mit Kennung des Benutzers, Ausgeführte Aktionen, insbesondere Lösch- und Kopiervorgänge, Zugriff auf Dateien mit personenbezogenen oder vertraulichen personenbezogenen Inhalten, unbefugte und abgewiesene Zugriffsversuche, wiederholte Eingabe von fehlerhaften Passwörtern zu einem Login, unbefugtes Einloggen und Überschreiten von Befugnissen, Benutzung von Admin-Accounts, Warnungen über unbefugtes Eindringen etc.)
- Systemüberwachung (Protokollierung von benutzten Programmen, Systemstart und -stopp, Anmeldung/Abmeldung von Benutzern, Anmelde-Fehlversuche, Anschluss und Entfernung von Ein- und Ausgabegeräten, Aktivitäten im Zusammenhang mit Fremdwartung und Fernwartung, Systemwarnungen oder Systemfehler, Konsolwarnungen und Konsolmeldungen, am Paketfilter wegen Regelverstoß abgewiesene Pakete, Änderungen und Änderungsversuche von Gateway- und Firewallpolicies, Systemprotokollausnahmen, Zugriffe auf die Server-Registry, Konfigurations- und Statusänderungen, Systemfehler, Regelverstöße, Maßnahmen zur System- und Datenwiederherstellung, wie Restore- und Back-up-Maßnahmen, Änderungen von Konfigurationseinstellungen etc.)
- Überwachung von Routern und Switches
- Protokollierung von Verbindungs- und Gesprächsdaten
- Protokollierung des Exports, Downloads und Versands von vertraulichen Dokumenten und Daten
- Regelmäßige/Anlassbezogene automatische/manuelle Auswertung der Protokolle auf Normabweichungen, Sicherheitsverletzungen und Angriffe

Auftragskontrolle

Allgemein:

- 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
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Vertraglich festgelegte Verantwortlichkeiten

Bei Fernwartung:

- Nur temporär für die jeweilige Wartungssitzung befristeter Zugang
- Beschränkung des Zugangs auf die für die Wartung notwendigen Rechte
- Ereignisauslösung erfolgt durch Auftraggeber
- Virtual Private Network (VPN)
- Überwachung der Sitzung durch den Auftraggeber (Vier-Augen-Prinzip)

Verfügbarkeitskontrolle

- Ausfallschutz durch gespiegelte Plattenlaufwerke, RAID-System etc.
- Regelmäßige Bestandskontrollen
- 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
- Sichere Lagerung von Datensicherungen (anderer Brandabschnitt/externe Lagerung, Tresor, Verschlüsselung der Datensicherungen etc.)
- Rauchmeldeanlage (mit Alarmierung der Feuerwehr, Wachdienst, interne Alarmierung etc.)
- Brandmeldeanlage (mit Alarmierung der Feuerwehr, Wachdienst, interne Alarmierung etc.)
- Brandschutzkonzept

- Feuerlöschanlage/Feuerlöscher mit geeignetem Löschmittel vorhanden
- Brandschutztüren
- Feuerschutzwände
- Administratorenpasswort/Notfallpassworte sicher hinterlegt (Tresor, Bankschließfach etc.)
- Notfallhandbuch
- Alarmierungsplan
- Wiederanlaufplan
- Notfallarbeitsplätze
- Dokumentation der Netztopologie
- Schriftliches Administrationskonzept
- Test- oder Entwicklungsumgebung vorhanden (Tests mit anonymisierten Echtdaten)

Trennungskontrolle

- Logische/physikalische Trennung von verschiedenen speichernden Stellen (Unternehmen)
- Trennung unabhängiger Anwendungen innerhalb eines Unternehmens (durch Zugriffssteuerung/physikalisch eigenständige Datenträger/logische Datentrennung)
- Trennung von Test- und Produktionsdaten (getrennte Programmbibliotheken etc.)