Anlage 2
zum Datenschutz und zur Datensicherheit in Auftragsverhältnissen gemäß Art. 28 DS-GVO

Auftragsverarbeitung gemäß Art. 28 DS-GVO

Begriffsdefinition

AV-Vertrag mit dem Auftragsverarbeiter
Der Verantwortliche muss mit dem Auftragsverarbeiter einen Vertrag über die weisungsgebundene Tätigkeit schließen, der schriftlich oder in einer elektronischen Form abgefasst sein kann.

Verantwortlicher
„Verantwortlicher" ist nach Art. 4 Nr. 7 DS-GVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet …;
Gemäß Art. 29 der DS-GVO ist der aufgrund eines Auftrages tätige Dienstleister weisungsgebunden. Er führt daher die Verarbeitung für den Auftraggeber nicht als Dritter i.S.d. Art. 4 Nr. 10 DS-GVO durch. Es besteht vielmehr zwischen dem den Auftrag erteilenden Verantwortlichen und seinem Auftragsverarbeiter ein „Innenverhältnis", welches durch den AV-Vertrag begründet wird. Die Verarbeitung durch den Auftragsverarbeiter wird deshalb grundsätzlich dem Verantwortlichen zugerechnet.
Die Gesamtverantwortung für die Datenverarbeitung und die Nachweispflicht des Verantwortlichen nach Art. 5 Abs. 2 DS-GVO umfasst auch die Verarbeitung durch den Auftragsverarbeiter.

Auftragsverarbeiter
„Auftragsverarbeiter" ist nach Art. 4 Nr. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Subunternehmer
Will sich der Auftragsverarbeiter zur Erbringung der vereinbarten Dienstleistung Subunternehmen als weiterer Auftragsverarbeiter bedienen, so bedarf es der vorherigen (schriftlichen oder elektronischen) Zustimmung durch den Verantwortlichen (Art. 28 Abs. 2 DS-GVO). Später beabsichtigte Änderungen bei den eingesetzten Subunternehmen muss der Auftragsverarbeiter dem Auftraggeber als Verantwortlichem vorher mitteilen, wobei es dem Verantwortlichen vorbehalten bleibt, gegen die geplante Einbeziehung eines Subunternehmens Einspruch zu erheben.

A) Weisungsempfänger des Auftragnehmers

Name	Organisationseinheit	Funktion	Kontakt
Steffen Kuntke Claudia Voß Juliane Pötke	EVG Betriebsgesellschaft mbH	Geschäftsführung	info@evgu.de
David Bachor	EVG Betriebsgesellschaft mbH	Betriebsleiter	0202 89798970 info@evgu.de

B) Datenschutzbeauftragter

Name	Organisationseinheit	Telefon / E-Mail
Thomas Weber	ISiCO Datenschutz GmbH	030 213002850 weber@isico-datenschutz.de

C) Unterauftragnehmer

Die folgenden Unternehmen werden zusätzlich als Subunternehmen des Auftragnehmers eingesetzt bzw. können zum Einsatz kommen.			
Firma	Anschrift / Land	Ansprechpartner	Beschreibung der Aufgaben

EVD GmbH & Co.KG	Karl-Hohmann-Str. 4-6 40599 Düsseldorf	Herr Schallenberg	Vernichtung von Altakten und Datenträger

Technische und organisatorische Maßnahmen (TOM)

1.0 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)
Maßnahmen, welche dazu fähig sind, die **Vertraulichkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

a) Zutrittskontrolle
Gemeint sind Maßnahmen, um zu verhindern, dass Unbefugte Zutritt (räumlich zu verstehen) zu Datenverarbeitungsanlagen erhalten:

Gebäudesicherung

- Zutritt (Sicherheitsschloss)
- Alarmanlage
- Bewegungsmelder

Sicherung der Räume

- Zutritt (Sicherheitsschlösser, Ausweisleser, Magnetkarte, Chipkarte)
- Schlüsselregelung (Schlüsselausgabe)

b) Zugangskontrolle
Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Zugangsberechtigungen sind nach Notwendigkeit eingerichtet (Minimalprinzip)
- Komplexe Passwortvergabe (mind. 8 Z., periodische Kennwortänderung)
- Authentifikation mit Benutzername / Passwort
- Automatische Bildschirm-Sperrung
- Zuordnung von Benutzerprofilen zu IT-Systemen
- Einsatz von VPN-Technologie
- Einsatz von SSL-Verschlüsselung und Zertifikaten
- Sperren von externen Schnittstellen (USB etc.)
- Sperren von offenen Netzwerkverbindungen
- Einsatz von Anti-Viren Software
- Einsatz von Firewalls (Hard- und Software)

c) Zugriffskontrolle
Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungs-systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unter-liegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Zugriffsberechtigungskonzept (Rechteverwaltung) vorhanden
- Zugriffsebene Dateisystemberechtigungen
- Festlegung der personellen Zuständigkeiten (Need-to-know-Prinzip)
- Regelmäßige Kontrolle der Gültigkeit der zugewiesenen Berechtigungen
- Verwaltung der Rechte durch Systemadministrator
- Protokollierung der Zugriffe (Logfiles)
- Verschlüsselung von Ordnern / Dateien
- Verschlüsselung von Datenträgern

d) Trennungskontrolle
Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können:

- die Verarbeitung der Daten erfolgt ausschließlich zum vereinbarten Zweck

e) Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)
Die Verarbeitung personenbezogener 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 möglich und sinnvoll, sind Verschlüsselungstechniken nach „Stand der Technik" einzusetzen. Dies gilt für die Übertragungswege ebenso wie für Speichermedien.

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

f) Weitergabekontrolle
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.

- Weitergabe per SFTP-Servers
- Detaillierte Protokollierungs- und Protokollauswertungssysteme vorhanden
- Dokumentation der Empfänger von Daten
- Ordnungsgemäße Vernichtung von Datenträgern
- Protokollierung der Vernichtung
- Benutzung sicherer Transportbehälter (Versiegelung)
- Übergabe erfolgt gegen Quittung

Ergänzungen:
Es erfolgt keine Datenübermittlung in ein „Drittland".

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

Über die Werkzeuge der Nutzerverwaltung und der damit verbundenen Rechteverwaltung muss nachvollziehbar sein, wer Neueingaben, Änderungen oder das Löschen personenbezogener und vertraulicher Informationen veranlasst hat.

- Gibt es einen Dateiverantwortlichen (Owner)
- Vergabe von Rechten zur Eingabe/Änderung/Löschung von Daten (Berechtigungskonzept)
- Protokollierung und Nachvollziehbarkeit der Eingabe, Änderung und Löschung von Daten

3.0 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)
Maßnahmen, welche dazu fähig sind, die **Verfügbarkeit und Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

h) Verfügbarkeitskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- Backupkonzept ist vorhanden (z.B. Großvater-Vater-Sohn Prinzip)

- Sichere Aufbewahrung von Datenträgern ist gewährleistet
- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- IT-Brandnorm, Feuer - EN-1047-2
- Schutzsteckdosenleisten in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschgeräte in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Serverräumen
- Backup- und Recoverykonzept ist vorhanden
- Notfallplan ist vorhanden
- Einsatz eines IT-Incident Management bzw. IT-Störungsmanagement
- Virenschutz
- Regelmäßige Software-Updates
- Regelmäßige Schwachstellenanalyse zu Hard- und Software

i) Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)
Maßnahmen, die befähigen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen

Siehe 3.0 lit. h

4.0 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

- Einsatz von IT-Incident Management bzw. IT-Störungsmanagement
- Durchführung von Sensibilisierungsmaßnahmen

j) Auftragskontrolle
Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Die Unterauftragnehmer wurden sorgfältig ausgewählt
- Regelmäßige Kontrolle der Vertragsausführung von Auftragsverarbeitern

k) Weitere organisatorische Maßnahmen zur Einhaltung des Datenschutzes

- Organisationsanweisung und Verhaltensregeln
- IT – Richtlinien (Regeln z.B. Clean Desk Policy etc.)
- Schulung der beteiligten Mitarbeiter und Wahrung des Datengeheimnisses

Das Intervall der Wiedervorlage zur Überprüfung der Sicherheit der Verarbeitung gemäß Art. 32 DS-GVO beträgt sechs Monate.

Wuppertal, Januar 2024

EVG Betriebsgesellschaft mbH
EVG Unternehmensgruppe
Hauptsitz:
Buchenhofener Straße 35, 42329 Wuppertal
Tel.: +49 202 / 89798970
E-Mail: kontakt@evgu.de
www.evgu.de

EVG Betriebsgesellschaft mbH
Standort Wuppertal