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	EVG Betriebsgesellschaft mbH	Geschäftsführer	info@evgu.de
Klaus Radtke	EVG Betriebsgesellschaft mbH	Betriebsleiter	04151-896040 klaus.radtke@evgu.de

B) Datenschutzbeauftragte

Name	Organisationseinheit	Telefon / E-Mail
Leila Concetti	SVG Qualität und Transport-Beratungs-GmbH	0173 2367604 l.concetti@svg-koblenz.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
HERTER Service und Recycling GmbH	Ernst-Abbe-Straße 7 72770 Reutlingen	Herr Hafner	Transport

Sebil Handels GmbH	Bensheimer Str. 61 65428 Rüsselsheim	Herr Tahhan	Transport
Spedition Hennenkämper GmbH & Co. KG	Korzerter Straße 73 42349 Wuppertal	Herr Bergmann	Transport
Fahrlogistik Wächter GmbH	Augustinusstraße 9 b 50226 Frechen	Herr Ensel	Transport
Otto Dörner Entsorgung GmbH	Lederstraße 24 22525 Hamburg	Herr Spieshöfer	Aktenvernichtung

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
- Einfriedung (außen Abschirmung)
- Zutritt (Sicherheitsschloss)
- Personenkontrolle beim Empfang
- Protokollierung der Zutritte / Abgänge
- Tragepflicht von Besucher und -Berechtigungsausweisen
- Videoüberwachung des Hauseingangs
- Videoüberwachung gekennzeichnet
- Alarmanlage,
- Bewegungsmelder

Sicherung der Räume
- Zutritt (Sicherheitsschlösser)
- Schlüsselregelung (Schlüsselausgabe)
- Bewegungsmelder

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
- Sperren von externen Schnittstellen (USB etc.)
- Sperren von offenen Netzwerkverbindungen
- Einsatz von Anti-Viren Software
- Einsatz von Firewalls (Hard- und Software)
- LAN durch DMZ vom Internet separiert
- WPA2, NAT und integrierte Firewall für Router aktiv

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
- Passwortrichtlinie und Passwortwechsel sind Mitarbeitern bekannt
- Protokollierung der Zugriffe (Logfiles)

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

- Daten werden ausschließlich zum Zweck der Erhebung verarbeitet
- die Verarbeitung der Daten erfolgt ausschließlich zum vereinbarten Zweck
- Berechtigungskonzepte existieren
- Aufteilung in Mandanten oder logische Trennung von Datenbeständen

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.

- Verschlüsselungsverfahren existieren

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 von besonderen Kategorien erfolgt in anonymisierter Form
- Detaillierte Protokollierungs- und Protokollauswertungssysteme vorhanden
- Die Zurechenbarkeit und Verbindlichkeit sind gegeben
- Dokumentation der Empfänger von Daten
- Physische Löschung von Datenträgern vor Wiederverwendung
- Ordnungsgemäße Vernichtung von Datenträgern nach (DIN 66399)
- 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
- Einsatz von Logfiles

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.

- Datenschutzfreundliche Voreinstellungen
- Einsatz von IT-Incident Management bzw. IT-Störungsmanagement

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

- Sorgfältige Vertragsgestaltung (z.B. MA-Verpflichtung etc.)
- 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
- Einsatz von Management-Systemen & Zertifizierung (z.B. ISO-27001, ITSEC)

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

Schwarzenbek, Januar 2022

EVG Betriebsgesellschaft mbH
EVG Unternehmensgruppe
Buchenhofener Straße 35, 42329 Wuppertal
Tel.: +49 (0) 202 / 771 606 Fax: +49 (0) 202 / 772 559
E-Mail: info@evgu.de
www.evgu.de

EVG Unternehmensgruppe
Standort Schwarzenbek