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
Sebastian Kretzer	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 können als Subunternehmen des Auftragnehmers zum Einsatz kommen.			
Firma	Anschrift / Land	Ansprechpartner	Beschreibung der Aufgaben

documentus GmbH Mecklenburg-Vorpommern	Neue Straße 37 18317 Saal	Frau Rusch Frau Lange	Vernichtung von Akten 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:

- Zutrittssicherung an allen Zutrittsmöglichkeiten zum Sicherheitsbereich
- Verzeichnis zur Verwaltung und Vergabe der individuellen Zutrittsberechtigungen zum Sicherheitsbereich
- Einbruchmeldeanlage gegen unbefugten Zutritt zum Sicherheitsbereich
- Zutrittsschleusen in den Sicherheitsbereich für Personen
- Zufahrtsschleusen oder gesicherte Andockschleusen für LKW an den Zufahrten/Zugängen in den Sicherheitsbereich
- Optische oder akustische Meldung an den örtlichen Sicherheitsbeauftragten, wenn Zugänge zum Sicherheitsbereich über eine bestimmte Zeit hinaus offen sind
- Zutritt von Mitarbeitern in den Sicherheitsbereich nur mit zutrittsberechtigtem ID-Chip/Schlüssel
- Zutritt betriebsfremder Personen nur nach vorheriger Identifikation über z.B. Personalausweis
- Zutritt betriebsfremder Personen in den Sicherheitsbereich nur nach Unterzeichnung einer Belehrung-/Verpflichtungserklärung
- Zutritt betriebsfremder Personen in den Sicherheitsbereich nur in ständiger Begleitung eines zutrittsberechtigten Mitarbeiters
- Dokumentation der Zutritte betriebsfremder Personen in den Sicherheitsbereich anhand einer Besucherliste/eines Besucherverzeichnisses
- Dokumentation aller Zutritte zum Sicherheitsbereich mittels Videoüberwachung

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

- Vergabe individueller Zutrittsberechtigungen zum Sicherheitsbereich für Mitarbeiter
- Zutritt betriebsfremder Personen nur nach vorheriger Identifikation über z.B. Personalausweis
- Dokumentation der Zutritte zum Sicherheitsbereich mittels Videoüberwachung
- Dokumentation der Aktivitäten im Sicherheitsbereich mittels Videoüberwachung
- Verbot von Foto- und Filmaufnahmen im Sicherheitsbereich

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:

- Verpflichtung aller Mitarbeiter auf alle einschlägigen und relevanten Gesetze
- Verwaltung und Dokumentation der Vergabe von Schlüsseln, ID-Chips und Schließberechtigungen an Betriebsangehörige
- Sorgfältige Auswahl und fortlaufende Kontrolle der Mitarbeiter (u.a. Vorlage polizeilicher Führungszeugnisse)
- Transport von zu vernichtenden Akten und Datenträgern grundsätzlich in ge- und verschlossenen Sicherheitsbehältern
- Dokumentation abgeholter und angelieferter Sicherheitsbehälter anhand von Lieferscheinen (in digitaler Form oder Papierform)

- Überwachung und Dokumentation der LKW-Positionen anhand GPS-Verfolgung
- Durchführung interner Audits und externer Revisionen

d) Maßnahmen zur Sicherstellung der Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- Transport von zu vernichtenden Akten und Datenträgern grundsätzlich in ge- und verschlossenen Sicherheitsbehältern oder in speziellen Sicherheitspresswagen/-LKW
- Transport von Sicherheitsbehältern ausschließlich in geschlossenen Fahrzeugen mit festem Aufbau
- Dokumentation abgeholter und angelieferter Sicherheitsbehälter anhand von Lieferscheinen (in digitaler Form oder Papierform)
- Überwachung und Dokumentation der LKW-Positionen anhand GPS-Verfolgung
- Arbeitsanweisungen gemäß dem Qualitätsmanagementsystem zur Sicherstellung der Integrität
- regelmäßige Schulung aller Mitarbeiter auf die in ihrem Arbeitsbereich wichtigen, datenschutzrelevanten Aspekte bei der Auftragsdurchführung
- Sicherheitskontrollstreifen zur Dokumentation der vollständigen Entleerung der Sicherheitsbehälter im Sicherheitsbereich

e) Maßnahmen zur Sicherstellung und Wiederherstellung von Verfügbarkeit

- Einbruchmeldeanlage im Sicherheitsbereich
- Notfallplanung zur Prävention und Bewältigung von Notfällen

f) Maßnahmen zur Sicherstellung der Belastbarkeit
Maßnahmen, welche dazu fähig sind, die **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen.

- Notfallplanung zur Prävention und Bewältigung von Notfällen
- redundante Anlagentechnik innerhalb der Gruppe

h) Maßnahmen zur Gewährleistung der Wirksamkeitskontrolle

- Verfahren für regelmäßige Kontrollen/Audits
- Definition von Prozessen und Arbeitsanweisungen zur Sicherstellung der vertraglich vereinbarten Leistungen
- Durchführung interner Audits und externer Revisionen

i) Weisungskontrolle bzw. Auftragskontrolle

- Vertrag zur Auftragsdatenverarbeitung gem. Art. 28 DS-GVO mit den gesetzlich geforderten Regelungen
- Verwendung von Papier-/und oder digitalem Lieferschein mit Angabe von Art und Menge abgeholter, geleerter oder angelieferter Sicherheitsbehälter, sowie Angabe von Datum, Lieferanschrift, Name des Mitarbeiters und Name des Kunden
- Unterschrift des Kunden auf dem Lieferschein (in digitaler Form oder in Papierform)
- Erstellung eines Vernichtungsprotokolls gemäß DIN SPEC 66399-3
- Überwachung und Dokumentation der LKW-Positionen anhand GPS-Verfolgung
- Verpflichtung aller Mitarbeiter auf alle einschlägigen und relevanten Gesetze
- Bestimmung von Ansprechpartnern und/oder verantwortlichen Mitarbeitern

Saal, Juni 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 Saal