Hinweise zum Datenschutz nach DSGVO

- Lieferanten und deren Mitarbeiter -

Als Verantwortlicher im Sinne der DSGVO nehmen wir den Schutz personenbezogener Daten ernst und verarbeiten diese nach den gesetzlichen Bestimmungen.

1. Verantwortlicher im Sinne des Datenschutzes

Verantwortlicher ist die Gesellschaft, mit welcher der Lieferantenvertrag geschlossen ist.

- Aareon AG, Isaac-Fulda-Allee 6, 55124 Mainz, E-Mail: info@aareon.com
- Aareon Deutschland GmbH, Isaac-Fulda-Allee 6, 55124 Mainz, E-Mail: info@aareon.com
- Aareon RELion GmbH (ehem. mse Gesellschaften, Isaac-Fulda-Allee 6, 55124 Mainz, E-Mail: RELion.Vertrieb@aareon.com
- Calcon Deutschland GmbH, Beethovenplatz 4, 80336 München, E-Mail: info@calcon.de
- phi-Consulting GmbH, Lise-Meitner-Allee 2, 44801 Bochum, E-Mail: info@phi-consulting.de

2. Kontakt mit dem Datenschutzbeauftragten

- der beiden Aareon-Gesellschaften per E-Mail: datenschutzbeauftragter@aareon.com
- der Aareon RELion GmbH (ehem. mse-Gesellschaften) per E-Mail: d.klapproth@ains-a.de
- der Calcon Deutschland GmbH per E-Mail: t.ewald@capcad.de
- der phi-Consulting GmbH per E-Mail: datenschutzbeauftragter@phi-consulting.de

3. Zweck und Rechtsgrundlage

Durchführung des Lieferantenverhältnisses und Vertragserfüllung nach Art. 6 Abs. 1 b) DSGVO.

4. Daten und Kategorien von Daten

Lieferanten und „Third Parties" (soweit es natürliche Personen sind)	Abrechnungs- und Zahlungsdaten
	Adresse
	Bankverbindung
	Bonitätsdaten
	Daten die im Rahmen einer Vertragspartnerprüfung erhoben werden.
	Fotos
	Geburtsdatum
	Ggf. Daten zur Identifizierung wirtschaftlich Berechtigter gem. Geldwäschegesetz
	Im Rahmen einer Due Diligence-Prüfung zur Verfügung gestellte Daten
	Kommunikationsdaten (E-Mail-Daten, gewählte Rufnummern)
	Kontaktdaten (Telefon, Fax, E-Mail)
	Meldung der auf Projekte/Schulungen geleisteten Zeiten
	Name + Namenzusätze (Herr/Frau, akademischer Titel)
	Personalisierte Arbeitsergebnisse in diversen Tools (Ticketsystem, Wikis, Entwicklungssysteme, Projektmanagement-Tools)
	Skills

	Terminverwaltung (Kalenderdaten)
	Vertragsdaten (Inhalt des Vertrags und Daten zur Vertragsabwicklung)
	Vertragsnummer, Lieferanten-Nr.
Mitarbeiter/Beschäftigte von Lieferanten und „Third Parties“	Adresse
	Angaben zu bisherigen Kontakten
	Daten die im Rahmen einer Vertragspartnerprüfung erhoben werden
	Fotos
	Geburtsdatum
	Im Rahmen einer Due Diligence-Prüfung zur Verfügung gestellte Daten
	Inhalte (Ausschreibungsunterlagen, Prospekte, Präsentationen, Schriftverkehr)
	Kommunikationsdaten (E-Mail-Daten, gewählte Rufnummern)
	Kontaktdaten (Telefon, Fax, E-Mail)
	Meldung der auf Projekte/Schulungen geleisteten Zeiten
	Name + Namenzusätze (Herr/Frau, akademischer Titel)
	Personalisierte Arbeitsergebnisse in diversen Tools (Ticketsystem, Wikis, Entwicklungssysteme, Projektmanagement-Tools)
	Skills
	Terminverwaltung (Kalenderdaten)

5. Empfänger bzw. Kategorien von Empfängern

Relevante Mitarbeiter beteiligter Abteilungen und verbundener Unternehmen, Auftragsverarbeiter. Aareon nutzt intern Microsoft®-Office-Anwendungen (z.B. Word®, Outlook®) und im Zentraleinkauf Systeme von Coupa® mit Kofax® für Bestellungen und Rechnungen sowie SAP® für Bezahlung, bei denen Support mit der möglichen Einsicht in Daten von außerhalb der EU/des EWR (USA, weltweit) erfolgen kann. Support von SAP kann aus der EU/EWR und der Schweiz erfolgen, die als sicheres Drittland mit Angemessenheitsbeschluss der EU-Kommission gilt. Im Übrigen gelten für Microsoft®, Coupa® und Kofax® EU Standardvertragsklauseln. Für Microsoft-Support sind die EU-Standardvertragsklauseln im Microsoft Trust Center einsehbar.

Aareon ist verpflichtet, an der Terrorismusbekämpfung mitzuwirken und führt einen Datenabgleich mit EU/US-Anti-Terrorlisten durch (Sanction Screening). Der Abgleich erfolgt über den Dienstleister/Lieferanten, nicht über dessen Mitarbeiter. Dafür nutzt Aareon das System AEB, für das bei Bedarf Support von außerhalb der EU/des EWR (UK, Singapore) erfolgen kann. UK gilt als sicheres Drittland gemäß Angemessenheitsbeschluss der EU-Kommission, für den Support aus Singapore gelten EU-Standardvertragsklauseln. Bei einem internationalen Datentransfer nach bzw. Zugriff von außerhalb der EU bestehen besondere Risiken für personenbezogene Daten (z. B. Zugriff durch ausländische Geheimdienste).

6. Speicherdauer

Die Daten zur Vertragserfüllung bzw. des Sanction Screening werden unter Beachtung der gesetzlichen Aufbewahrungsfristen bis 10 Jahre nach Beendigung des Lieferantenverhältnisses bzw. der Vornahme des Sanction Screening gespeichert. Nicht mehr benötigte Daten werden gelöscht.

7. Betroffenenrechte

Betroffene haben das Recht auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit und Beschwerde bei einer Aufsichtsbehörde.

Stand 28.09.2021