

Hinweise zum Datenschutz nach DSGVO

- Kunden und deren Mitarbeitende -

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 für eine Vertragserfüllung und weitere Geschäftsanbahnung ist die Aareon-Gesellschaft, mit welcher der Kundenvertrag geschlossen ist. Die Gesellschaften der Aareon Group sind auch gemeinsame Verantwortliche für Marketingmaßnahmen (z. B. Einladung zu Events, Umfragen) und konzerninterne Verkaufsberichterstattung (sales reporting).

- Aareon Group GmbH (ehem. Aareon AG), Isaac-Fulda-Allee 8, 55124 Mainz, E-Mail: info@aareon.com
- Aareon Deutschland GmbH, Isaac-Fulda-Allee 8, 55124 Mainz, E-Mail: info@aareon.com (inkl. ehem. Aareon RELion GmbH, GAP GmbH, Haus Perfekt GmbH, Immo Software GmbH, Locoia GmbH, UTS GmbH))
- CalCon Deutschland GmbH, Beethovenplatz 4, 80336 München, E-Mail: info@calcon.de
- First Financial Software GmbH, Isaac-Fulda-Allee 8, 55124 Mainz, E-Mail: info@first-financial.biz
- wohnungshelden GmbH, Beethovenplatz 4, 80336 München, E-Mail: info@wohnungshelden.de

Die gemeinsamen Verantwortlichen haben eine Vereinbarung geschlossen, wonach die Kontaktdaten von der Aareon Group GmbH für Marketingmaßnahmen (z. B. Einladung zu Events, Umfragen) und konzerninterne Verkaufsberichterstattung (sales reporting) genutzt werden. Die Aareon Group GmbH bildet die Hauptniederlassung für die Bestimmung der federführenden Aufsichtsbehörde.

2. Kontakt mit dem Datenschutzbeauftragten

- der genannten Gesellschaften per E-Mail: datenschutzbeauftragter@aareon.com

3. Zweck und Rechtsgrundlage

Durchführung des Kundenvertrags und Vertragserfüllung nach Art. 6 Abs. 1 b) DSGVO. Weitere Geschäftsanbahnung sowie Marketing mit Einwilligung nach Art. 6 Abs. 1 a) und/oder berechtigtem Interesse nach Art. 6 Abs. 1 f) DSGVO für Geschäftsanbahnung sowie Marketing. Betroffene Personen können jederzeit eine Einwilligung (z. B. Newsletter) widerrufen oder Geschäftsanbahnung und Marketing widersprechen.

4. Daten und Kategorien von Daten

Kunden (soweit es natürliche Personen sind)	Abrechnungs- und Zahlungsdaten
	Adresse
	Bankverbindung
	Betreuungsinformationen, inkl. Kundenentwicklung und bisherige Kontakte
	Bonitätsdaten

	Daten zum Opt-in oder Opt-out zu Marketingmaßnahmen (Erklärtes Einverständnis zu werblichen Benachrichtigungen und sonst. Werbemaßnahmen, Anmeldung Newsletter, Werbewidersprüche)
	Fotos
	Geburtsdatum
	Kontaktdaten (Telefon, Fax, E-Mail)
	Kundennummer
	Name + Namenszusätze (Herr/Frau, akademischer Titel)
	Produkt- bzw. Vertragsinteresse (für Upselling)
	Sonstige Daten, die zur Identifizierung nach Geldwäschegesetz ggf. erforderlich sind
	Vertragsdaten
	Videos (aufgenommen bei Veranstaltungen)
Mitarbeitende/Beschäftigte von Kunden	Adresse (idR Geschäftsadresse)
	Daten zum Opt-in oder Opt-out zu Marketingmaßnahmen (Erklärtes Einverständnis zu werblichen Benachrichtigungen und sonst. Werbemaßnahmen, Anmeldung Newsletter, Werbewidersprüche)
	Fotos
	Geburtsdatum
	Inhalte (Teilnahme an Workshops und Schulungen, inhaltliche Stellungnahmen (z. B. Fehlermeldungen, Abnahmen, Weisungen, Konkretisierungen)
	Kontaktdaten (Telefon, Fax, E-Mail)
	Name + Namenszusätze (Herr/Frau, akademischer Titel)
	Videos (aufgenommen bei Veranstaltungen)

5. Empfänger bzw. Kategorien von Empfängern

Empfänger bzw. Kategorien von Empfängern sind relevante Mitarbeitende beteiligter Abteilungen und verbundener Unternehmen sowie Auftragsverarbeitende. Aareon nutzt für Interessenten- und Kundendaten Cloud Dienste von Hubspot® sowie Salesforce® und intern Microsoft®-Office-Anwendungen (z. B. Word®, Outlook®), Jira von Atlassian sowie Zendesk® (als Ticket System), bei denen eine Speicherung in der EU erfolgt, aber eine mögliche Einsicht in Daten von außerhalb der EU/des EWR erfolgen kann. Für Hubspot®, Microsoft®, Salesforce® und Zendesk® gelten EU-US Privacy Framework und EU-Standardvertragsklauseln. Bei Salesforce® und Zendesk® gelten zudem Binding Corporate Rules und für Jira von Atlassian die EU-Standardvertragsklauseln, die auf der jeweiligen Webseite der Unternehmen abrufbar sind.

Bei einer Kundenlösung mit SAP® und Blue Eagle gilt: Für Individualkunden erfolgt der SAP-Support mit weltweitem Support der SAP-Support-Organisation. Die Subunternehmen mit EU-Standardvertragsklauseln können vom Kunden im SAP-Support-Portal eingesehen werden. Individualkunden können den „EU Access“ im SAP-Support-Portal aktivieren. Für ASP- und Hosting-Kunden aktiviert Aareon den EU Access, bei dem SAP-Support nur aus EU/EWR und der Schweiz mit Angemessenheitsbeschluss der EU-Kommission erfolgt. In Einzelfällen kann eine weltweite Bearbeitung innerhalb der SAP-Support-Organisation mit Zustimmung des Kunden erfolgen, wofür die EU-Standardvertragsklauseln gelten.

Bei einer Kundenlösung mit Microsoft® Office 365 gilt: Bei einem Hosting in der Microsoft Azure Cloud oder Microsoft Support kann eine mögliche Einsicht in Daten von außerhalb der EU/des EWR erfolgen.

Dafür gelten über den Microsoft-Kundenvertrag EU-US Privacy Framework und EU-Standardvertragsklauseln, die im Microsoft Trust Center einsehbar sind.

Aareon setzt TeamViewer zum IT-Support für Fernwartungen bei Kunden ein. TeamViewer nutzt auch Subunternehmer außerhalb der EU/EWR, wofür Standardvertragsklauseln und Binding Corporate Rules gelten.

Aareon ist verpflichtet, an der Terrorismusbekämpfung mitzuwirken und führt einen Datenabgleich mit EU-/US-Anti-Terrorlisten durch (Sanction Screening). Der Abgleich erfolgt über den Kunden, nicht über dessen Mitarbeitende. 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

Daten zur Vertragserfüllung bzw. des Sanction Screening werden unter Beachtung der gesetzlichen Aufbewahrungsfristen bis zu 10 Jahre nach Beendigung des Kundenverhältnisses bzw. der Vornahme des Sanction Screening gespeichert. Nicht mehr benötigte Daten werden gelöscht. Daten auf Basis einer Einwilligung werden bis Widerruf gespeichert. Daten auf Basis eines berechtigten Interesses werden so lange gespeichert, wie das berechtigte Interesse besteht, bis Widerspruch oder bei Leads (z. B. Download Whitepaper) nach 2 Jahren Inaktivität und bei Kontakt (z. B. Vertragsverhandlung) längstens bis 7 Jahre nach dem letzten Kontakt des Unternehmens bzw. des Betroffenen.

7. Betroffenenrechte

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

Stand 16.09.2025