

Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO – Brandwarnsystem (Safe Fire House) und Einbruchwarnsystem (EWS)

(Als PDF am linken oberen Seitenrand unter "Anhänge" zu finden)

zwischen

[Auftraggeber / Behörde / Kommune / Betreiber]

[Straße Hausnummer] · [PLZ Ort]

vertreten durch: [vertretungsberechtigte Person]

– nachfolgend „Verantwortlicher“ –

und

Dexa Solutions GmbH

Möhnestraße 2 · 59519 Möhnesee

Telefon: +49 2924 496 937-0 · E-Mail: info@dexa.gmbh

Registergericht Arnsberg, HRB 14749 · USt-IdNr. DE310146224

vertreten durch die Geschäftsführer Tim Behrendt und Florian Leipold

– nachfolgend „Auftragnehmer“ –

Präambel

Der Auftragnehmer erbringt für den Verantwortlichen Leistungen zu zwei eigenständigen Produkten: dem Brandwarnsystem „Safe Fire House“ und dem hiervon getrennten Einbruchwarnsystem „EWS“. Im Rahmen von Bereitstellung, Fernwartung, Monitoring und Alarmweiterleitung verarbeitet der Auftragnehmer in begrenztem Umfang personenbezogene Daten im Auftrag des Verantwortlichen. Dafür schließen die Parteien diesen Vertrag nach Art. 28 DSGVO. Die Einzelheiten regelt Anlage 1.

§ 1 Gegenstand und Dauer

(1) Gegenstand ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Verantwortlichen. Art, Zweck und Umfang der Verarbeitung, die Kategorien betroffener Personen sowie die Datenarten ergeben sich abschließend aus Anlage 1.

(2) Der Vertrag läuft für die Dauer des zugrunde liegenden Hauptvertrages und endet mit diesem. Der Verantwortliche kann ihn bei schwerwiegenden Datenschutzverstößen fristlos kündigen.

§ 2 Weisungsgebundenheit

(1) Der Auftragnehmer verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern er nicht durch Unionsrecht oder mitgliedstaatliches Recht zur Verarbeitung verpflichtet ist.

(2) Hält der Auftragnehmer eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich und darf die Ausführung bis zur Bestätigung aussetzen (Art. 28 Abs. 3 S. 3 DSGVO).

§ 3 Pflichten des Auftragnehmers

Der Auftragnehmer

- verpflichtet die mit der Verarbeitung befassten Personen zur Vertraulichkeit (Art. 28 Abs. 3 lit. b, Art. 29 DSGVO);

- setzt die in Anlage 2 vereinbarten technischen und organisatorischen Maßnahmen (Art. 32 DSGVO) um und hält sie aufrecht;
- unterstützt den Verantwortlichen bei Betroffenenanfragen sowie bei dessen Pflichten nach Art. 32 bis 36 DSGVO im Rahmen seiner Möglichkeiten;
- meldet ihm jede Verletzung des Schutzes personenbezogener Daten unverzüglich nach Kenntnis und unterstützt bei Art. 33, 34 DSGVO;
- führt ein Verzeichnis der im Auftrag durchgeführten Verarbeitungen (Art. 30 Abs. 2 DSGVO) und benennt einen Ansprechpartner für den Datenschutz [Datenschutzbeauftragter: Tim Behrendt].

§ 4 Unterauftragsverarbeiter

(1) Der Verantwortliche genehmigt die in Anlage 2 aufgeführten Unterauftragsverarbeiter. Beabsichtigte Änderungen teilt der Auftragnehmer vorab mit; der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund widersprechen (Art. 28 Abs. 2 DSGVO).

(2) Der Auftragnehmer verpflichtet jeden Unterauftragsverarbeiter auf dieselben Datenschutzpflichten (Art. 28 Abs. 4 DSGVO) und bleibt dem Verantwortlichen gegenüber verantwortlich.

(3) Vom Verantwortlichen selbst beauftragte Alarmierungs- und Leitstellenplattformen (beispielsweise DIVERA 24/7, GroupAlarm, Alamos, iSE Cobra 4) sind keine Unterauftragsverarbeiter des Auftragnehmers; insoweit ist der Verantwortliche selbst verantwortlich.

§ 5 Rechte der betroffenen Personen

(1) Der Auftragnehmer unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Erfüllung der Betroffenenrechte (Art. 12 bis 23 DSGVO).

(2) Wendet sich eine betroffene Person unmittelbar an den Auftragnehmer, leitet dieser das Anliegen unverzüglich an den Verantwortlichen weiter und beantwortet es nicht selbst, sofern er nicht angewiesen wurde.

§ 6 Kontrolle, Löschung und Drittlandübermittlung

(1) Der Auftragnehmer weist die Einhaltung seiner Pflichten nach und ermöglicht Überprüfungen mit angemessener Vorankündigung; geeignete Zertifikate, Testate oder Prüfberichte genügen (Art. 28 Abs. 3 lit. h DSGVO).

(2) Nach Vertragsende löscht oder gibt der Auftragnehmer die personenbezogenen Daten nach Wahl des Verantwortlichen zurück, vorbehaltlich gesetzlicher Aufbewahrungspflichten. Die Bilddaten des EWS werden ohnehin automatisiert spätestens nach 15 Minuten gelöscht.

(3) Eine Übermittlung in Drittländer erfolgt nur nach Art. 44 ff. DSGVO. Betroffen ist ausschließlich der CRM-Dienstleister Airtable, Inc. (USA), abgesichert über das EU-US Data Privacy Framework beziehungsweise EU-Standardvertragsklauseln. Die zentralen Server (BOS Data Broker, gui.dexa.gmbh) sowie ein etwaiges durch den Auftragnehmer bereitgestelltes VPN werden in Deutschland im Rechenzentrum der Centron GmbH, Bamberg, betrieben.

§ 7 Schlussbestimmungen

(1) Änderungen und Ergänzungen bedürfen der Textform. In datenschutzrechtlichen Fragen geht dieser Vertrag dem Hauptvertrag vor.

(2) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen unberührt. Es gilt deutsches Recht. Die Anlagen 1 und 2 sind Bestandteil dieses Vertrages.

Verantwortlicher (Auftraggeber)	Dexa Solutions GmbH (Auftragnehmer)
Ort, Datum:	Ort, Datum:
Unterschrift:	Unterschrift:

Anlage 1 – Beschreibung der Verarbeitung

Zweck

Bereitstellung, Fernwartung, Monitoring und Alarmweiterleitung der Produkte Safe Fire House (Brandwarnsystem) und EWS (Einbruchwarnsystem) sowie Verwaltung der zugehörigen Stamm- und Kontaktdaten.

Produkt 1 – Safe Fire House (Brandwarnsystem)

- Cloud-freies Brandwarnsystem. Verarbeitet ausschließlich technische Telemetrie (Geräte-/Funkadressen, RSSI, Batterie-, Verschmutzungs- und Funktionswerte, Fehlercodes). **Kein Personenbezug.**

Produkt 2 – EWS (Einbruchwarnsystem)

- Eigenständige, kamerabasierte Produktlinie mit KI-gestützter Personenerkennung.
- Im Ruhezustand (unscharf) sind die Kameras **physisch stromlos** (Datenschutz by Design) – es findet keine Verarbeitung statt.
- Nur im scharfgeschalteten Zustand: bei Auslösung (Eindringling oder Fehlalarm) Erzeugung eines Snapshots und gegebenenfalls eines kurzen Live-Streams; Übermittlung an die Alarmschnittstelle beziehungsweise an gui.dexa.gmbh.
- Keine dauerhafte Speicherung auf dem Server; der Snapshot wird automatisiert spätestens nach 15 Minuten gelöscht, der Abruf-Link ist danach nicht mehr erreichbar. Eine etwaige weitergehende Speicherung erfolgt nur beim angebundenen Alarmierungsdienst und liegt in dessen Verantwortung.

CRM (Stamm- und Kontaktdaten)

- Verwaltung von Standort-Stammdaten, Ansprechpartnern sowie Alarm-/Benachrichtigungsempfängern und Servicetickets im CRM-System (Airtable). Dies ist die **wesentliche Verarbeitung personenbezogener Daten** und erfolgt über einen Drittland-Dienstleister (USA); siehe Anlage 2.

Kategorien betroffener Personen

- Ansprechpartner und Verantwortliche des Auftraggebers;
- Empfänger von Alarm-, Service- und Warnmeldungen;
- Personen im Erfassungsbereich des scharfgeschalteten EWS (Eindringlinge sowie Personen aus Fehlalarmen, beispielsweise Mitarbeitende, Reinigungs- oder Einsatzkräfte).

Kategorien personenbezogener Daten und Löschfristen

Kontext	Datenarten	Löschfrist
CRM	Name, Funktion, Organisation, dienstliche E-Mail/Telefon, Standortzuordnung, Servicevorgänge	Vertragsdauer

Kontext	Datenarten	Löschfrist
EWS (scharf)	Bilddaten (Snapshot/kurzer Stream), Ereignisdaten (Zeitstempel, Kamera/Zone)	max. 15 Min
Safe Fire House	kein Personenbezug (technische Telemetrie)	–

Anlage 2 – Technische/organisatorische Maßnahmen und Unterauftragsverarbeiter

Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

- Zugriff ausschließlich durch namentlich befugte Administratoren; zentrale Verwaltung der Zugangsdaten; Mehr-Faktor-Authentifizierung.
- Fernwartung nur über verschlüsselten Tunnel mit MFA; ausschließlich verschlüsselte Verbindungen (TLS 1.3).
- Datenminimierung: EWS-Kameras im Ruhezustand stromlos; automatische Löschung der Bild-Snapshots ? 15 Min; keine dauerhafte Bildspeicherung.
- Mandanten- und Standorttrennung; Identifikation der Geräte über technische Adressen statt über Personen.
- Kontinuierliches Monitoring (Uptime/Watchdog), tägliche Selbsttests, Datensicherung der zentralen Systeme.
- Serverbetrieb in einem zertifizierten Rechenzentrum in Deutschland (Centron GmbH, Bamberg).

Genehmigte Unterauftragsverarbeiter

Unterauftragsverarbeiter	Leistung	Ort	Drittland-Grundlage
Centron GmbH	Rechenzentrum/Hosting (BOS Data Broker, gui.dexa.gmbh, gegebenenfalls VPN)	Bamberg, DE	entfällt (EU)
Dexa Systems GmbH	BOS Data Broker / Alarm-Schnittstellensoftware (konzernintern)	Möhnesee, DE	entfällt (EU)
Airtable, Inc.	CRM / Stamm- und Kontaktdaten, Service-Log	USA	EU-US DPF beziehungsweise EU-Standardvertragsklauseln

Hinweis: Vom Verantwortlichen selbst beauftragte Alarmierungs-/Leitstellenplattformen (beispielsweise DIVERA 24/7) sind keine Unterauftragsverarbeiter des Auftragnehmers (§ 4 Abs. 3).