

Vertrag zur Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

Stand: 02.10.2026

zwischen

Auftragnehmer / Auftragsverarbeiter

SOS Security GmbH
Mitteldorfstr. 13
37083 Göttingen
vertreten durch den Geschäftsführer Tuncay Demiriz
E-Mail: info@sos-security.eu

Auftraggeber / Verantwortlicher

Firma / Name: _____
Anschrift: _____
PLZ / Ort: _____
Vertreten durch: _____
E-Mail: _____

gemeinsam nachfolgend „Vertragsparteien“ genannt

Dieser Vertrag ergänzt den jeweiligen Hauptvertrag über Wartung, Service, Installation, Fernzugriff, Leitstellen- oder sonstige sicherheitstechnische Leistungen. Soweit personenbezogene Daten im Auftrag verarbeitet werden, gehen die datenschutzrechtlichen Bestimmungen dieses Vertrags bei Widersprüchen den Regelungen des Hauptvertrags vor.

§ 1 Gegenstand, Anwendungsbereich und Dauer

- (1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Zusammenhang mit sicherheitstechnischen Leistungen. Hierzu können insbesondere Wartung, Inspektion, Störungsbeseitigung, Konfiguration, Fernwartung, technische Unterstützung, Alarmbearbeitung, Leitstellenaufschaltung sowie die Administration von Videoüberwachungs-, Einbruchmelde-, Zutrittskontroll- und sonstigen Gefahrenmeldesystemen gehören.
- (2) Eine Auftragsverarbeitung liegt nur insoweit vor, wie der Auftragnehmer personenbezogene Daten ausschließlich für die Zwecke und nach den dokumentierten Weisungen des Auftraggebers verarbeitet. Tätigkeiten, bei denen der Auftragnehmer eigene Zwecke und Mittel bestimmt, sind nicht Gegenstand dieses Vertrags.
- (3) Die Verarbeitung beginnt mit Aufnahme der auftragsbezogenen Verarbeitung und dauert für die Laufzeit des Hauptvertrags bzw. bis zur vollständigen Rückgabe oder Löschung der im Auftrag verarbeiteten personenbezogenen Daten, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.
- (4) Gegenstand, Art, Zweck, Datenkategorien und betroffene Personengruppen sind in Anlage 1 konkretisiert. Anlage 1 ist Bestandteil dieses Vertrags.

§ 2 Verantwortlichkeit des Auftraggebers

- (1) Der Auftraggeber bleibt Verantwortlicher im Sinne der DSGVO und ist insbesondere für die Rechtmäßigkeit der Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten, die Wahrung der Betroffenenrechte sowie die Erfüllung der Informationspflichten verantwortlich.
- (2) Bei Videoüberwachungs-, Zutrittskontroll- und Gefahrenmeldesystemen legt der Auftraggeber insbesondere Zweck, Rechtsgrundlage, Erfassungsbereiche, Berechtigungskonzepte, Speicher- bzw. Löschrufen und die zulässigen Auswertungen fest. Der Auftragnehmer setzt diese Vorgaben nur im Rahmen des technisch Machbaren und der dokumentierten Weisungen um.
- (3) Der Auftraggeber stellt sicher, dass dem Auftragnehmer keine Daten oder Zugriffe zur Verfügung gestellt werden, deren Verarbeitung gegen geltendes Datenschutzrecht verstößt. Er informiert den Auftragnehmer über besondere Schutzbedarfe, gesetzliche Geheimhaltungspflichten oder sonstige projektspezifische Anforderungen.

§ 3 Weisungen

- (1) Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, sofern er nicht durch Unionsrecht oder das Recht eines Mitgliedstaats zu einer Verarbeitung

verpflichtet ist. In diesem Fall informiert der Auftragnehmer den Auftraggeber vor der Verarbeitung über die entsprechende Rechtspflicht, soweit dies rechtlich zulässig ist.

(2) Weisungen können in Textform, über vereinbarte Ticketsysteme oder in dringenden Fällen mündlich erteilt werden. Mündliche Weisungen sind vom Auftraggeber zeitnah in Textform zu bestätigen. Weisungsberechtigte und Weisungsempfänger werden in Anlage 2 benannt.

(3) Hält der Auftragnehmer eine Weisung für datenschutzrechtswidrig, informiert er den Auftraggeber unverzüglich. Der Auftragnehmer darf die betreffende Verarbeitung bis zur Bestätigung, Änderung oder Rücknahme der Weisung aussetzen, soweit dies zur Vermeidung eines Datenschutzverstoßes erforderlich ist.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer verarbeitet personenbezogene Daten nur im vereinbarten Umfang und nicht für eigene Zwecke. Eine Nutzung zu Werbe-, Profiling- oder sonstigen sachfremden Zwecken ist ausgeschlossen.

(2) Der Auftragnehmer stellt sicher, dass alle zur Verarbeitung befugten Personen auf Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Zugriffsberechtigungen werden nach dem Need-to-know- und Least-Privilege-Prinzip vergeben.

(3) Der Auftragnehmer führt, soweit gesetzlich erforderlich, ein Verzeichnis der Kategorien von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DSGVO und arbeitet mit der zuständigen Datenschutzaufsichtsbehörde zusammen.

(4) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er feststellt, dass eine Verarbeitung oder eine Weisung des Auftraggebers gegen anwendbares Datenschutzrecht verstößt.

(5) Der Auftragnehmer darf auf Kundensysteme, Bilddaten, Ereignisspeicher oder Benutzerinformationen nur zugreifen, soweit dies zur Ausführung der beauftragten Leistung erforderlich ist. Lokale Kopien, Screenshots oder Exporte werden nur erstellt, wenn sie für Fehleranalyse, Nachweis oder Dokumentation erforderlich sind und werden anschließend nach Wegfall des Zwecks gelöscht bzw. sicher verwahrt, sofern gesetzliche Aufbewahrungspflichten bestehen.

§ 5 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer trifft unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie Art, Umfang, Umständen und Zwecken der Verarbeitung geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO. Die zum Zeitpunkt des Vertragsschlusses vorgesehenen Maßnahmen sind in Anlage 3 beschrieben.

(2) Der Auftragnehmer darf die Maßnahmen im Zuge technischer und organisatorischer Weiterentwicklung anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

(3) Bei Systemen im Verantwortungsbereich des Auftraggebers hängt das technisch erreichbare Schutzniveau teilweise von den eingesetzten Produkten, Firmwareständen, Netzwerkbedingungen und Herstellerfunktionen ab. Der Auftragnehmer weist auf erkennbare erhebliche Sicherheitsrisiken hin; die Entscheidung über Austausch, Update, Segmentierung oder sonstige Maßnahmen am Kundensystem trifft der Auftraggeber, soweit nicht ausdrücklich anders beauftragt.

§ 6 Unterstützung des Auftraggebers

(1) Der Auftragnehmer unterstützt den Auftraggeber unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Erfüllung der Pflichten aus Art. 12 bis 22 DSGVO, insbesondere bei Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch.

(2) Erhält der Auftragnehmer ein Ersuchen einer betroffenen Person, das sich auf die Auftragsverarbeitung bezieht, leitet er dieses unverzüglich an den Auftraggeber weiter und beantwortet es nicht eigenständig, es sei denn, der Auftraggeber weist ihn hierzu an.

(3) Der Auftragnehmer unterstützt den Auftraggeber, soweit erforderlich, bei der Sicherheit der Verarbeitung, der Meldung von Datenschutzverletzungen, der Benachrichtigung betroffener Personen, Datenschutz-Folgenabschätzungen und einer etwa erforderlichen vorherigen Konsultation der Aufsichtsbehörde gemäß Art. 32 bis 36 DSGVO.

(4) Soweit außergewöhnliche Unterstützungsleistungen nicht im Hauptvertrag enthalten sind und nicht durch eine Pflichtverletzung des Auftragnehmers verursacht wurden, können die Parteien vor Durchführung eine angemessene Vergütung des Zusatzaufwands vereinbaren.

§ 7 Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, sobald ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Daten des Auftraggebers betrifft. Die Meldung erfolgt so rechtzeitig, dass der Auftraggeber seine Pflichten nach Art. 33 und 34 DSGVO erfüllen kann.

(2) Die Meldung enthält, soweit zum Zeitpunkt der Meldung bekannt:

- eine Beschreibung der Art der Datenschutzverletzung sowie, soweit möglich, Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze;
- Name und Kontaktdaten einer Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung;
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung und zur Minderung möglicher nachteiliger Auswirkungen.

(3) Sind Informationen noch nicht vollständig verfügbar, werden sie ohne unangemessene Verzögerung schrittweise nachgereicht. Der Auftragnehmer dokumentiert relevante Sicherheitsvorfälle und die ergriffenen Maßnahmen.

§ 8 Unterauftragsverarbeiter

(1) Der Auftraggeber erteilt dem Auftragnehmer eine allgemeine schriftliche Genehmigung zum Einsatz der in Anlage 4 aufgeführten Unterauftragsverarbeiter. Eine tatsächliche Datenübermittlung erfolgt nur, soweit die jeweilige Teilleistung für den konkreten Auftrag genutzt wird.

(2) Beabsichtigt der Auftragnehmer die Hinzuziehung eines weiteren oder den Austausch eines bestehenden Unterauftragsverarbeiters, informiert er den Auftraggeber grundsätzlich vor Beginn der Verarbeitung in Textform. Der Auftraggeber kann aus sachlich begründeten datenschutzrechtlichen Gründen innerhalb einer angemessenen Frist widersprechen. Können die Parteien den Widerspruch nicht ausräumen, ist der Auftragnehmer berechtigt, die betroffene Teilleistung auszusetzen oder eine alternative technische Lösung anzubieten.

(3) Der Auftragnehmer verpflichtet Unterauftragsverarbeiter vertraglich mindestens zu den Datenschutzpflichten, die für deren jeweilige Verarbeitung aus diesem Vertrag gelten. Der Auftragnehmer bleibt gegenüber dem Auftraggeber für die Erfüllung der Pflichten des Unterauftragsverarbeiters verantwortlich.

(4) Dienstleister ohne Zugriff auf personenbezogene Daten des Auftraggebers oder reine Nebenleistungen ohne auftragsbezogene Datenverarbeitung gelten nicht als Unterauftragsverarbeiter im Sinne dieser Klausel.

§ 9 Drittlandübermittlungen

(1) Eine Verarbeitung personenbezogener Daten außerhalb des Europäischen Wirtschaftsraums erfolgt nur, wenn die Voraussetzungen des Kapitels V DSGVO erfüllt sind. Der Auftragnehmer stellt bei einer solchen Übermittlung insbesondere sicher, dass ein Angemessenheitsbeschluss, geeignete Garantien oder eine andere zulässige Rechtsgrundlage vorliegt.

(2) Soweit ein genehmigter Unterauftragsverarbeiter Daten in einem Drittland verarbeitet oder von dort aus auf Daten zugreifen kann, werden die hierfür vorgesehenen Garantien in Anlage 4 oder in der jeweiligen Anbieter-Dokumentation benannt.

§ 10 Nachweise und Kontrollrechte

(1) Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Pflichten aus Art. 28 DSGVO nachzuweisen. Nachweise können insbesondere durch TOM-Dokumentationen, Prüfberichte, Zertifikate, Protokolle oder vergleichbare Unterlagen erbracht werden.

(2) Der Auftraggeber ist berechtigt, die Einhaltung dieses Vertrags selbst oder durch einen zur Vertraulichkeit verpflichteten Prüfer zu kontrollieren. Kontrollen sollen vorrangig dokumentenbasiert oder remote erfolgen. Vor-Ort-Kontrollen werden mit angemessener Vorankündigung und während der üblichen Geschäftszeiten durchgeführt, soweit nicht ein Datenschutzvorfall, eine behördliche Anordnung oder ein vergleichbarer wichtiger Grund eine kurzfristige Prüfung erfordert.

(3) Prüfungen dürfen den Geschäftsbetrieb, die Sicherheit anderer Kunden und gesetzliche Geheimhaltungspflichten nicht unverhältnismäßig beeinträchtigen. Der Auftragnehmer kann zum Schutz vertraulicher Informationen angemessene Begleit- und Sicherheitsmaßnahmen verlangen.

§ 11 Rückgabe und Löschung

- (1) Nach Ende der Auftragsverarbeitung löscht oder gibt der Auftragnehmer nach Wahl des Auftraggebers alle im Auftrag verarbeiteten personenbezogenen Daten und vorhandenen Kopien zurück, soweit keine gesetzliche Pflicht zur weiteren Speicherung besteht.
- (2) Daten in technisch erforderlichen Sicherungskopien werden im Rahmen des regulären Backup-Lebenszyklus gelöscht und bis dahin gesperrt bzw. ausschließlich für Wiederherstellungszwecke verarbeitet. Gesetzlich aufzubewahrende Unterlagen werden nach Ablauf der jeweiligen Frist gelöscht.
- (3) Auf Wunsch bestätigt der Auftragnehmer dem Auftraggeber die vertragsgemäße Löschung in Textform, soweit eine solche Bestätigung technisch und organisatorisch möglich ist.

§ 12 Vertraulichkeit und Geschäftsgeheimnisse

- (1) Beide Vertragsparteien behandeln alle im Zusammenhang mit diesem Vertrag erlangten vertraulichen Informationen, Geschäftsgeheimnisse, Sicherheitskonzepte, Zugangsdaten, Netzwerk- und Anlageninformationen vertraulich. Diese Pflicht gilt über die Beendigung des Vertrags hinaus.
- (2) Zugangsdaten, Schlüssel, Passwörter, Tokens und vergleichbare Authentisierungsinformationen dürfen nur den für die Leistungserbringung erforderlichen Personen zugänglich gemacht und nicht unverschlüsselt oder ungeschützt weitergegeben werden.

§ 13 Haftung

Für die Haftung der Vertragsparteien gelten die gesetzlichen Regelungen, insbesondere Art. 82 DSGVO, sowie ergänzend die Haftungsregelungen des Hauptvertrags, soweit diese zwingendes Datenschutzrecht nicht einschränken.

§ 14 Laufzeit und Beendigung

- (1) Dieser Vertrag tritt mit Unterzeichnung bzw. mit Beginn der Auftragsverarbeitung in Kraft und gilt für die Dauer der auftragsbezogenen Verarbeitung personenbezogener Daten.
- (2) Bei schwerwiegenden oder wiederholten Verstößen gegen diesen Vertrag oder anwendbares Datenschutzrecht kann die jeweils andere Vertragspartei die betroffene Verarbeitung aussetzen und nach erfolgloser angemessener Abhilfefrist den Hauptvertrag aus wichtigem Grund kündigen, soweit die Fortsetzung der Verarbeitung unzumutbar ist.

§ 15 Schlussbestimmungen

- (1) Änderungen und Ergänzungen dieses Vertrags einschließlich seiner Anlagen bedürfen mindestens der Textform, soweit nicht zwingendes Recht eine strengere Form verlangt.
- (2) Sollten einzelne Bestimmungen unwirksam oder undurchführbar sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. Die unwirksame Regelung ist durch eine wirksame Regelung zu ersetzen, die dem datenschutzrechtlichen Zweck möglichst nahekommt.
- (3) Im Übrigen gelten die Bestimmungen des Hauptvertrags. Bei Widersprüchen zu datenschutzrechtlichen Pflichten hat dieser Vertrag für die Auftragsverarbeitung Vorrang.

Unterschriften

Mit ihrer Unterzeichnung bestätigen die Vertragsparteien die Vereinbarung dieses Vertrags einschließlich der Anlagen 1 bis 4. Die Anlagen sind Bestandteil des Vertrags.

Ort, Datum Auftraggeber

Ort, Datum Auftragnehmer

Unterschrift Auftraggeber

Unterschrift Auftragnehmer

Name / Funktion

SOS Security GmbH / Geschäftsführung

Anlage 1 - Beschreibung der Verarbeitung

Diese Anlage beschreibt die typischen Verarbeitungen im Rahmen der sicherheitstechnischen Leistungen. Der konkrete Leistungsumfang ergibt sich aus dem Hauptvertrag, Angebot, Auftrag oder Service-/Wartungsvertrag.

1. Gegenstand und Zweck der Verarbeitung

- Wartung, Inspektion, Prüfung, Störungsbeseitigung und Konfiguration sicherheitstechnischer Anlagen;
- Fernwartung und technischer Support, einschließlich zeitlich begrenzter Einsicht in Anlagenzustände, Ereignisspeicher oder Bilddaten;
- Administration von Benutzer-, Berechtigungs- und Zutrittsdaten nach Weisung des Auftraggebers;
- Alarmbearbeitung, Alarmweiterleitung und Leitstellenaufschaltung, soweit beauftragt;
- Dokumentation von Störungen, Servicearbeiten und Sicherheitsereignissen, soweit hierfür personenbezogene Daten erforderlich sind;
- Migration, Austausch oder Inbetriebnahme von Systemen, soweit dabei personenbezogene Daten aus Bestandsanlagen übernommen oder geprüft werden.

2. Betroffene Systeme / Datenquellen

- Videoüberwachungs- und Videoaufzeichnungssysteme;
- Einbruchmelde- und Überfallmeldeanlagen;
- Zutrittskontroll- und Türmanagementsysteme;
- Gefahrenmelde-, Brandmelde- oder sonstige sicherheitstechnische Systeme, soweit diese personenbezogene Benutzer-, Ereignis- oder Kontaktdaten enthalten;
- Leitstellen-/Alarmübertragungssysteme und projektbezogene Hersteller- oder Cloudportale, sofern vom Auftraggeber freigegeben.

3. Kategorien personenbezogener Daten

- Bild- und Videodaten einschließlich Zeitstempel und Kamerabezug;
- Zutritts- und Berechtigungsdaten, z. B. Name, Benutzer-/Kartenummer, Transponder-ID, Zutrittszeit und Zutrittsereignis;
- Scharf-/Unscharfschaltungs-, Alarm-, Störungs- und Ereignisdaten einschließlich Benutzerkennungen;
- Kontakt- und Kommunikationsdaten von Ansprechpartnern, Interventionspersonen und Systemnutzern;
- Protokoll- und technische Metadaten, z. B. Benutzerkennungen, IP-Adressen, Gerätekennungen, Zeitpunkte und Logeinträge;
- Objekt- und Standortbezug, soweit dieser einer natürlichen Person zugeordnet werden kann.

Besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO sind grundsätzlich nicht gezielt Gegenstand der beauftragten Verarbeitung. Soweit solche Merkmale in Bildaufnahmen lediglich beiläufig sichtbar sein können, erfolgt keine Auswertung zu Art.-9-Merkmalen. Biometrische Identifizierung oder Verifikation ist nur bei gesonderter schriftlicher Vereinbarung zulässig.

4. Kategorien betroffener Personen

- Beschäftigte des Auftraggebers;
- Kunden, Besucher, Lieferanten, Dienstleister und sonstige Zutrittsberechtigte;
- Passanten oder sonstige Personen, soweit sie zulässigerweise von Kameras erfasst werden;
- Ansprechpartner, Systemadministratoren, Interventionspersonen und sonstige Nutzer der Sicherheitssysteme;
- Beschäftigte von Auftragnehmern oder Unterauftragnehmern, soweit sie in Protokollen oder Bilddaten erfasst werden.

5. Art der Verarbeitung

Je nach Auftrag insbesondere Erheben bzw. Einsehen, Auslesen, Abfragen, Ordnen, Strukturieren, Konfigurieren, Speichern, Übermitteln, Abgleichen, Einschränken, Exportieren zu Dokumentationszwecken sowie Löschen personenbezogener Daten. Eine dauerhafte eigene Speicherung durch den Auftragnehmer erfolgt nur, soweit sie für die beauftragte Leistung, Nachweisführung oder gesetzliche Pflichten erforderlich ist.

6. Dauer / Löschkonzept

Die Verarbeitung erfolgt für die Dauer der jeweiligen Service-, Wartungs-, Projekt- oder Leitstellenleistung. Temporär angefertigte Diagnose- oder Dokumentationskopien werden nach Wegfall des Zwecks gelöscht. Daten auf Systemen des Auftraggebers werden entsprechend dessen Weisungen und den dort eingestellten Speicher- bzw. Löschfristen verarbeitet.

Anlage 2 - Weisungsberechtigte und Ansprechpartner

A. Auftraggeber / Verantwortlicher

Weisungsberechtigte Person 1 (Name, Funktion, E-Mail, Telefon):

Weisungsberechtigte Person 2 (Name, Funktion, E-Mail, Telefon):

Datenschutzkontakt / Datenschutzbeauftragter, falls vorhanden:

B. SOS Security GmbH / Auftragnehmer

Weisungsempfänger / zentrale Anlaufstelle:

SOS Security GmbH
Mitteldorfstr. 13, 37083 Göttingen
E-Mail: info@sos-security.eu
Telefon: 0551 389 32 93

Weitere projektbezogene Ansprechpartner können im Auftrag, Wartungsvertrag, Ticketsystem oder in sonstiger Textform benannt werden.

C. Form von Weisungen

Weisungen sollen vorzugsweise per E-Mail, Ticketsystem, Serviceauftrag oder in anderer nachvollziehbarer Textform erteilt werden. Bei dringenden Störungen sind telefonische Weisungen zulässig; sie sollen anschließend dokumentiert werden.

Anlage 3 - Technische und organisatorische Maßnahmen (TOM)

Die folgenden Maßnahmen beschreiben das organisatorische und technische Schutzniveau im Verantwortungsbereich der SOS Security GmbH. Sie gelten soweit auftragsbezogen anwendbar. Bei Kundensystemen können einzelne technische Funktionen vom eingesetzten Produkt, Hersteller, Firmwarestand oder Kundennetz abhängen.

1. Organisation, Verantwortlichkeiten und Vertraulichkeit

- Verpflichtung von Beschäftigten und eingesetzten Personen auf Vertraulichkeit und Datenschutz;
- klare Zuständigkeiten für Benutzerkonten, Zugriffsrechte, Fernzugriffe und Sicherheitsvorfälle;
- regelmäßige Sensibilisierung zu Phishing, Zugangsdaten, sicherem Umgang mit Kundendaten und Fernwartung;
- Dokumentation wesentlicher Verarbeitungs- und Sicherheitsprozesse.

2. Zutrittskontrolle

- Schutz von Geschäfts- und Technikräumen gegen unbefugten Zutritt;
- Schlüssel-/Zutrittsberechtigungen nur für berechtigte Personen und Rücknahme bei Wegfall der Berechtigung;
- Besucher werden, soweit erforderlich, begleitet oder organisatorisch kontrolliert.

3. Zugangskontrolle / Authentisierung

- personalisierte Benutzerkonten, soweit technisch möglich;
- Passwortrichtlinien und sichere Speicherung von Zugangsdaten;
- Multifaktor-Authentisierung für administrative, Cloud- und Remote-Zugänge, soweit technisch verfügbar und angemessen;
- Sperrung oder Entzug von Zugängen bei Austritt, Rollenwechsel oder Wegfall des Bedarfs;
- automatische bzw. organisatorische Bildschirmsperren auf Arbeitsgeräten.

4. Zugriffskontrolle und Berechtigungsmanagement

- Zugriffsrechte nach Need-to-know und Least-Privilege;
- Trennung administrativer und normaler Benutzerrechte, soweit technisch möglich;
- Zugriff auf Kundenanlagen und Kundendaten nur für beauftragte Mitarbeitende bzw. projektbezogen eingesetzte Personen;
- regelmäßige Überprüfung kritischer Berechtigungen.

5. Fernzugriff und Übertragung

- Fernzugriffe erfolgen nur aufgrund eines Auftrags, Wartungsvertrags oder einer Weisung des Auftraggebers;
- Nutzung verschlüsselter Transportwege (z. B. TLS/HTTPS/VPN oder herstellerseitig abgesicherte Verbindungen), soweit technisch verfügbar;
- keine ungeschützte Weitergabe von Passwörtern, Schlüsseln oder Tokens;
- Sitzungen werden nach Abschluss beendet; dauerhaft hinterlegte Zugänge werden auf das erforderliche Maß beschränkt;
- bei erkennbar unsicheren Alt- oder Kundensystemen wird der Auftraggeber auf wesentliche Risiken hingewiesen.

6. Trennungsgebot / Mandantentrennung

- organisatorische Trennung von Kundenprojekten, Zugängen und Dokumentationen;
- Vermeidung gemeinsamer Sammelkonten, soweit technisch möglich;
- Kundendaten werden nicht mit Daten anderer Kunden zu sachfremden Zwecken zusammengeführt.

7. Protokollierung und Nachvollziehbarkeit

- Dokumentation wesentlicher Service- und Fernwartungsvorgänge, soweit erforderlich;
- Nutzung vorhandener Systemprotokolle für administrative Zugriffe und Änderungen, soweit die jeweilige Technik dies unterstützt;
- Schutz von Protokollen gegen unbefugte Veränderung, soweit im Verantwortungsbereich des Auftragnehmers.

8. Verfügbarkeit, Sicherung und Wiederherstellung

- regelmäßige Datensicherungen betrieblicher Systeme nach einem angemessenen Sicherungskonzept;
- Schutz von Sicherungen vor unbefugtem Zugriff;
- Wiederherstellungsverfahren für betriebliche Daten und Konfigurationen, soweit anwendbar;
- angemessener Schutz gegen Strom-, Hardware- oder Systemausfälle im eigenen Verantwortungsbereich.

9. Integrität, Endgeräteschutz und Patchmanagement

- aktuelle Schutzmechanismen gegen Schadsoftware auf betrieblichen Endgeräten, soweit technisch angemessen;
- zeitnahe Einspielung sicherheitsrelevanter Updates für unterstützte Betriebssysteme und Anwendungen;
- Einsatz unterstützter Software- und Firmwarestände, soweit im eigenen Einflussbereich; bei veralteten Kundensystemen Risikohinweis an den Auftraggeber;
- Beschränkung der Installation nicht freigegebener Software auf betrieblichen Systemen.

10. Mobile Geräte und Datenträger

- Schutz mobiler Geräte durch Gerätesperre und, soweit technisch möglich, Verschlüsselung;
- Minimierung lokaler Speicherung personenbezogener Kundendaten;
- sichere Verwahrung, Rückgabe und Löschung nicht mehr benötigter Datenträger und Arbeitskopien.

11. Löschung und Entsorgung

- Löschung temporärer Diagnose-, Export- und Dokumentationsdaten nach Wegfall des Zwecks;
- sichere Löschung bzw. Vernichtung von Datenträgern und Papierunterlagen entsprechend dem Schutzbedarf;
- Berücksichtigung gesetzlicher Aufbewahrungsfristen; während der Aufbewahrung Einschränkung auf den erforderlichen Zugriff.

12. Sicherheitsvorfälle und Wirksamkeitskontrolle

- definierter Meldeweg für Datenschutz- und IT-Sicherheitsvorfälle;
- unverzügliche Eskalation relevanter Vorfälle an den Auftraggeber;
- regelmäßige Überprüfung und bei Bedarf Anpassung der Schutzmaßnahmen;
- Auswertung wesentlicher Störungen und Sicherheitsvorfälle zur Vermeidung von Wiederholungen.

Anlage 4 - Genehmigte Unterauftragsverarbeiter

Der Auftraggeber genehmigt die nachfolgend aufgeführten Unterauftragsverarbeiter im Rahmen von § 8. Eine tatsächliche Übermittlung erfolgt nur, soweit die jeweilige Teilleistung für den konkreten Auftrag genutzt wird. Änderungen erfolgen nach dem Informations- und Widerspruchsverfahren gemäß § 8 Abs. 2.

Unternehmen / Anschrift	Teilleistung	Daten / Zugriff	Ort der Verarbeitung	Hinweise
Microsoft Ireland Operations Limited One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Irland	Microsoft 365 / Exchange Online für geschäftliche E-Mail- und Dokumentenkommunikation	Kommunikations-, Kontakt-, Projekt- und ggf. Anhangsdaten, soweit im Rahmen des Auftrags übermittelt	EU/EWR; ggf. begrenzte Drittlandverarbeitung nach Microsoft DPA und anwendbaren Garantien	nur soweit auftragsbezogene Daten über Microsoft 365 verarbeitet werden
All Service Sicherheitsdienste GmbH Karl-von-Drais-Str. 16-18 60435 Frankfurt am Main	Notruf- und Serviceleitstellen-/Alarmbearbeitungsleistungen	Alarm-, Objekt-, Kontakt-, Interventions- und ggf. Video-/Ereignisdaten je nach Beauftragung	Deutschland	nur bei beauftragter Leitstellenleistung
Weitere projektbezogene Hersteller-/Cloudanbieter	z. B. Herstellerportal, Cloudzugang, Fernwartung oder projektspezifischer Dienst	nur die für die konkrete Funktion erforderlichen Daten	wird vor Einsatz mitgeteilt	Einsatz nur nach Information gemäß § 8; Drittlandvorgaben gemäß § 9