

# Anlage „Auftragsverarbeitung“ i.S.d. Art. 28 Abs. 3 Datenschutz-Grundverordnung im Rahmen der Beauftragung des Betriebs eines

## VIDEO GUARD

zwischen

dem Vertragspartner der Anmietung einer Video Guard Videoüberwachungslösung

- Auftraggeber -

und

International Security GmbH, Wehrden Ost 5, 26835 Hesel

- Auftragnehmer -

### Präambel

Diese Anlage konkretisiert die Verpflichtungen der Vertragsparteien zum Datenschutz, die sich aus der Beauftragung einer Videoüberwachung mit VIDEO GUARD und der entsprechenden Auftragsverarbeitung u. a. aus dem BDSG und der DS-GVO ergeben. Sie findet Anwendung auf alle Tätigkeiten, die mit dem Vertrag in Zusammenhang stehen und bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (»Daten«) des Auftraggebers verarbeiten.

### § 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

Der Auftragnehmer (AN) stellt seinen Kunden mobile Videoüberwachungslösungen zur Verfügung und betreibt diese (VIDEO GUARD). Diese mobilen Videoüberwachungssysteme überwachen den Zutritt auf die privaten Gelände des Kunden. Sollte es während der mit dem Kunden vereinbarten Überwachungszeit, d.h. generell außerhalb der Arbeitszeiten, zu einem Alarm kommen, so verifiziert der (AN) den Alarm und ergreift die vorher mit dem Kunden abgestimmten Maßnahmen. Dem Kunden kann je nach vorliegender Gefahr zuvor oder danach ein Videoclip des Alarms zur Verfügung gestellt werden. Die Videobilder werden in einem Ringspeicher gespeichert und nach individuell vereinbarter Speicherdauer automatisiert gelöscht bzw. überschrieben.

Aus der zu Grunde liegenden Beauftragung (im Folgenden: Vertrag) ergeben sich Gegenstand und Dauer des Auftrags sowie Umfang und Art der Datenerhebung, -verarbeitung oder -nutzung. Im Einzelnen sind insbesondere die folgenden Daten Bestandteil der Datenverarbeitung:

Art der Daten	Zweck der Datenerhebung, -verarbeitung oder -nutzung	Kreis der Betroffenen
<u>Identifikationsdaten:</u> Name Anschrift Telefonnummer Emailadresse Beruf/Firma Vertragsdaten Kundennummer	Sämtliche erhobenen und verarbeiteten Daten werden benötigt, um die beauftragte Videobe- und überwachung durchzuführen und gegenüber dem Kunden abzurechnen.	Insb. Mitarbeiter des Kunden und von diesem mitgeteilte externe Ansprechpartner.

<u>Abrechnungsdaten:</u> Bankverbindung Angebotsdaten Kontakthistorie  <u>Sicherheitsdaten:</u> Videoüberwachung		Insb. die Firmendaten des Kunden  Alle Besucher des überwachten Bereiches.
--	--	--

Die Laufzeit dieser Anlage richtet sich nach der Laufzeit des Vertrages, sofern sich aus den Bestimmungen dieser Anlage nicht darüberhinausgehende Verpflichtungen ergeben.

## § 2 Anwendungsbereich und Verantwortlichkeit

1. Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Dies umfasst Tätigkeiten, die im Vertrag und in der Leistungsbeschreibung konkretisiert sind. Der Auftraggeber ist im Rahmen dieses Vertrages für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich (»Verantwortlicher« im Sinne des Art. 4 Nr. 7 DS-GVO).
2. Die Weisungen werden anfänglich durch den Vertrag festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

## § 3 Pflichten des Auftragnehmers

1. Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten außer es liegt ein Ausnahmefall im Sinne des Artikel 28 Abs. 3 a) DS-GVO vor. Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde.
2. Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen der Datenschutz-Grundverordnung (Art. 32 DS-GVO) genügen. Der Auftragnehmer hat technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherstellen. Dem Auftraggeber sind diese technischen und organisatorischen Maßnahmen bekannt und er trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeitenden Daten ein angemessenes Schutzniveau bieten. Eine Änderung der getroffenen Sicherheitsmaßnahmen bleibt dem Auftragnehmer vorbehalten, wobei jedoch sichergestellt sein muss, dass das vertraglich vereinbarte Schutzniveau nicht unterschritten wird. Der Status Quo der Maßnahmen wird in Anlage 1 näher definiert.
3. Der Auftragnehmer unterstützt soweit vereinbart den Auftraggeber im Rahmen seiner Möglichkeiten bei der Erfüllung der Anfragen und Ansprüche betroffenen Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in Art. 33 bis 36 DS-GVO genannten Pflichten.
4. Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeiter und andere für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.
5. Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, jedoch aber innerhalb von 48h, wenn ihm Verletzungen des Schutzes personenbezogener Daten des Auftraggebers bekannt werden. Er trifft die

erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen der betroffenen Personen und spricht sich hierzu unverzüglich mit dem Auftraggeber ab. Die Mitteilung des Auftragnehmers an den Auftraggeber umfasst folgende Informationen (soweit dem Auftragnehmer bereits bekannt): (i) Datum und Uhrzeit des Vorfalls, (ii) eine Beschreibung des Vorfalls, (iii) die Namen, der von dem Vorfall betroffenen Personen, deren personenbezogene Daten möglicherweise Gegenstand des Vorfalls geworden sind, sowie eine Beschreibung der Kategorien betroffener personenbezogener Daten.

6. Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen ist Daniel Schirmer, Tel. 04950 80620, Datenschutz@international-security-group.de. Der Auftragnehmer gewährleistet ferner, seinen gesetzlichen Pflichten zur Bestellung eines Datenschutzbeauftragten nachzukommen.
7. Der Auftragnehmer gewährleistet, seinen Pflichten nach Art. 32 Abs. 1 lit. d) DS-GVO nachzukommen, ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung einzusetzen
8. Der Auftragnehmer berichtigt oder löscht die vertragsgegenständlichen Daten, wenn der Auftraggeber dies anweist und dies vom Weisungsrahmen umfasst ist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt der Auftragnehmer die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grund einer Einzelbeauftragung durch den Auftraggeber oder gibt diese Datenträger an den Auftraggeber zurück, sofern nicht im Vertrag bereits vereinbart. In besonderen, vom Auftraggeber zu bestimmenden Fällen, erfolgt eine Aufbewahrung bzw. Übergabe, Vergütung und Schutzmaßnahmen hierzu sind gesondert zu vereinbaren, sofern nicht im Vertrag bereits vereinbart.
9. Daten, Datenträger sowie sämtliche sonstige Materialien sind nach Auftragsende auf Verlangen des Auftraggebers entweder herauszugeben oder zu löschen. Entstehen zusätzliche Kosten durch abweichende Vorgaben bei der Herausgabe oder Löschung der Daten, so trägt diese der Auftraggeber

#### **§ 4 Pflichten des Auftraggebers**

1. Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.
2. Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen des Vertrages anfallende Datenschutzfragen.

#### **§ 5 Anfragen Betroffener**

1. Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer leitet den Antrag der betroffenen Person unverzüglich an den Auftraggeber weiter. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.
2. Wendet sich ein Betroffener mit Forderungen zur Berichtigung, Löschung oder Sperrung an den Auftragnehmer, wird der Auftragnehmer den Betroffenen an den Auftraggeber verweisen.

#### **§ 6 Nachweismöglichkeiten**

1. Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in diesem Vertrag niedergelegten Pflichten durch einen Selbstaudit nach. Alternativ bietet er dem Auftraggeber die Möglichkeit eines eigenen Audits durch einen zur standesrechtlichen Verschwiegenheit verpflichteten und geeigneten Auditor.
2. Sollten im Einzelfall Inspektionen durch den Auftraggeber oder einen von diesem beauftragten Prüfer erforderlich sein, werden diese zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf diese von der vorherigen Anmeldung mit angemessener Vorlaufzeit und von der Unterzeichnung einer Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen. Sollte der durch den Auftraggeber

beauftragte Prüfer in einem Wettbewerbsverhältnis zu dem Auftragnehmer stehen, hat der Auftragnehmer gegen diesen ein Einspruchsrecht.

Für die Unterstützung bei der Durchführung einer Inspektion darf der Auftragnehmer eine Vergütung verlangen, wenn dies im Vertrag vereinbart ist. Der Aufwand einer Inspektion ist für den Auftragnehmer grundsätzlich auf einen Tag pro Kalenderjahr begrenzt.

3. Sollte eine Datenschutzaufsichtsbehörde oder eine sonstige hoheitliche Aufsichtsbehörde des Auftraggebers eine Inspektion vornehmen, gilt grundsätzlich Absatz 2 entsprechend. Eine Unterzeichnung einer Verschwiegenheitsverpflichtung ist nicht erforderlich, wenn diese Aufsichtsbehörde einer berufsrechtlichen oder gesetzlichen Verschwiegenheit unterliegt, bei der ein Verstoß nach dem Strafgesetzbuch strafbewehrt ist.

## **§ 7 Subunternehmer**

1. Der Einsatz von Subunternehmern als weiteren Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.
2. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der im Vertrag vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.
3. Der Auftraggeber stimmt zu, dass der Auftragnehmer Subunternehmer hinzuzieht. Vor Hinzuziehung oder Ersetzung der Subunternehmer informiert der Auftragnehmer den Auftraggeber. Der Auftraggeber kann der Änderung – innerhalb einer angemessenen Frist – aus wichtigem Grund – gegenüber der vom Auftraggeber bezeichneten Stelle widersprechen. Erfolgt kein Widerspruch innerhalb der Frist gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.
4. Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus diesem Vertrag dem Subunternehmer zu übertragen.
5. Ein zustimmungspflichtiges Subunternehmerverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei externem Personal, Post- und Versanddienstleistungen oder Wartung. Der Auftragnehmer wird mit diesem Dritten im erforderlichen Umfang Vereinbarungen treffen, um einen angemessenen Datenschutz zu gewährleisten.

## **§ 8 Informationspflichten, Schriftformklausel, Rechtswahl**

1. Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als »Verantwortlicher« im Sinne der Datenschutz-Grundverordnung liegen.
2. Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile – einschließlich etwaiger Zusicherungen des Auftragnehmers – bedürfen einer schriftlichen Vereinbarung, die auch in einem elektronischen Format (Textform) erfolgen kann, und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.
3. Bei etwaigen Widersprüchen gehen Regelungen dieser Anlage zum Datenschutz den Regelungen des Vertrages vor. Sollten einzelne Teile dieser Anlage unwirksam sein, so berührt dies die Wirksamkeit der Anlage im Übrigen nicht.
4. Es gilt deutsches Recht.

## § 9 Haftung und Schadensersatz

1. Auftraggeber und Auftragnehmer haften gegenüber betroffener Personen entsprechend der in Art. 82 DS-GVO getroffenen Regelung

### Anlage 1:

## Technische und organisatorische Maßnahmen i.S.d. Art. 32 DS-GVO

### 1. Zutrittskontrolle

*Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.*

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Alarmanlage in der Immobilie Wehrden Ost 5, Hesel sowie im VIDEO GUARD Ultimate          | <input checked="" type="checkbox"/> Manuelles Schließsystem   |
| <input checked="" type="checkbox"/> Bewegungsmelder bei VIDEO GUARD ultimate und in der Immobilie Wehrden Ost 5, Hesel       | <input checked="" type="checkbox"/> Sicherheitsschlösser in der Immobilie Wehrden Ost 5, Hesel                  |
| <input checked="" type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.)  | <input checked="" type="checkbox"/> Tragepflicht von Berechtigungsausweisen, soweit Wachpersonal vom AG gebucht |
| <input checked="" type="checkbox"/> Protokollierung der Besucher soweit Wachpersonal vom AG gebucht                          | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal in Wehrden Ost 5, Hesel          |
| <input checked="" type="checkbox"/> Sorgfältige Auswahl von Wachpersonal am Einsatzort, soweit vom Auftraggeber (AG) gebucht | <input checked="" type="checkbox"/> Tragepflicht von Berechtigungsausweisen, soweit Wachpersonal vom AG gebucht |

### 2. Zugangskontrolle

*Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.*

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Zuordnung von Benutzerrechten  | <input checked="" type="checkbox"/> Erstellen von Benutzerprofilen   |
| <input checked="" type="checkbox"/> Passwortvergabe  | <input checked="" type="checkbox"/> Einsatz einer Firewall   |
| <input checked="" type="checkbox"/> Authentifikation mit Benutzername / Passwort   | <input checked="" type="checkbox"/> Zuordnung von Benutzerprofilen zu IT-Systemen                                      |
| <input checked="" type="checkbox"/> Gehäuseverriegelungen  | <input checked="" type="checkbox"/> Einsatz von VPN-Technologie  |
| <input checked="" type="checkbox"/> Sperren von externen Schnittstellen (USB etc.)   | <input checked="" type="checkbox"/> Einsatz von Anti-Viren-Software  |
| <input checked="" type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.)  | <input checked="" type="checkbox"/> Einsatz von Intrusion-Detection-Systemen beim VIDEO GUARD Professional, Ultra, One |
| <input checked="" type="checkbox"/> Sorgfältige Auswahl von Wachpersonal am Einsatzort, soweit vom Auftraggeber (AG) gebucht | <input checked="" type="checkbox"/> Tragepflicht von Berechtigungsausweisen, soweit Wachpersonal vom AG gebucht        |

## 2. Zugriffskontrolle

*Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.*

- |  |   |
|--|---|
| <input checked="" type="checkbox"/> Erstellen eines Berechtigungskonzepts  | <input checked="" type="checkbox"/> Verwaltung der Rechte durch Systemadministrator         |
| <input checked="" type="checkbox"/> Anzahl der Administratoren auf das „Notwendigste“ reduziert  | <input checked="" type="checkbox"/> Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel |
| <input checked="" type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | <input checked="" type="checkbox"/> Sichere Aufbewahrung von Datenträgern                   |
| <input checked="" type="checkbox"/> Verschlüsselung von Datenträgern   |   |

## 3. Weitergabekontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.*

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Einrichtungen von Standleitungen bzw. VPN-Tunneln  | <input checked="" type="checkbox"/> Beim physischen Transport: sichere Transportbehälter/-verpackungen           |
| <input checked="" type="checkbox"/> Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Transportfahrzeugen                     | <input checked="" type="checkbox"/> Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen |
| <input checked="" type="checkbox"/> Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschrufen |  |

## 4. Eingabekontrolle

*Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.*

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Protokollierung der Eingabe, Änderung und Löschung von Daten | <input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts |
|--|--|

Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)

Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind

## 5. Auftragskontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.*

Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)

Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags

schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG

Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis

Auftragnehmer hat Datenschutzbeauftragten bestellt (Art. §28 DSGVO)

## 6. Verfügbarkeitskontrolle

*Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.*

Unterbrechungsfreie Stromversorgung (USV)

Klimaanlage in Serverräumen

Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen

Schutzsteckdosenleisten in Serverräumen

Feuer- und Rauchmeldeanlagen

Feuerlöschgeräte in Serverräumen

Serverräume nicht unter sanitären Anlagen

Vorhalten eines Backup- & Recoverykonzeptes

Testen von Datenwiederherstellung

Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

## 7. Trennungsgebot

*Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.*

physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern

Logische Mandantentrennung (softwareseitig)

Erstellung eines Berechtigungskonzeptes

Trennung von Produktiv- und Testsystem

Festlegung von Datenbankrechten

