



## Technische und organisatorische Maßnahmen i.S.d. Artikel 32 DSGVO

### 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                               | <input type="checkbox"/> Absicherung von Gebäudeschächten                      |
| <input checked="" type="checkbox"/> Automatisches Zugangskontrollsystem       | <input checked="" type="checkbox"/> Chipkarten-/Transponder-Schließsystem      |
| <input checked="" type="checkbox"/> Schließsystem mit Codesperre              | <input checked="" type="checkbox"/> Manuelles Schließsystem                    |
| <input type="checkbox"/> Biometrische Zugangssperren                          | <input type="checkbox"/> Videoüberwachung der Zugänge                          |
| <input checked="" type="checkbox"/> Lichtschranken / Bewegungsmelder          | <input checked="" type="checkbox"/> Sicherheitsschlösser                       |
| <input checked="" type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input checked="" type="checkbox"/> Personenkontrolle beim Pförtner / Empfang  |
| <input type="checkbox"/> Protokollierung der Besucher                         | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input type="checkbox"/> Sorgfältige Auswahl von Wachpersonal                 | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen               |

### 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 type="checkbox"/> Authentifikation mit biometrischen Verfahren  |
| <input checked="" type="checkbox"/> Authentifikation mit Benutzername / Passwort | <input checked="" type="checkbox"/> Zuordnung von Benutzerprofilen zu IT-Systemen  |
| <input type="checkbox"/> Gehäuseverriegelungen                                   | <input checked="" type="checkbox"/> Einsatz von VPN-Technologie  |
| <input type="checkbox"/> Sperren von externen Schnittstellen (USB etc.)          | <input checked="" type="checkbox"/> Sicherheitsschlösser   |
| <input type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.)               | <input checked="" type="checkbox"/> Personenkontrolle beim Pförtner / Empfang  |
| <input type="checkbox"/> Protokollierung der Besucher                            | <input checked="" type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal   |
| <input type="checkbox"/> Sorgfältige Auswahl von Wachpersonal                    | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen   |
| <input type="checkbox"/> Einsatz von Intrusion-Detection-Systemen                | <input checked="" type="checkbox"/> Verschlüsselung von mobilen Datenträgern   |
| <input type="checkbox"/> Verschlüsselung von Smartphone-Inhalten                 | <input type="checkbox"/> Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) |
| <input checked="" type="checkbox"/> Einsatz von Anti-Viren-Software              | <input type="checkbox"/> Verschlüsselung von Datenträgern in Laptops / Notebooks   |
| <input type="checkbox"/> Einsatz einer Hardware-Firewall                         | <input checked="" type="checkbox"/> Einsatz einer Software-Firewall  |



### 3. 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"/> physische Löschung von Datenträgern vor Wiederverwendung   | <input checked="" type="checkbox"/> ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) |
| <input type="checkbox"/> Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)                          | <input checked="" type="checkbox"/> Protokollierung der Vernichtung                         |
| <input checked="" type="checkbox"/> Verschlüsselung von Datenträgern   |   |

### 4. 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 type="checkbox"/> Weitergabe von Daten in anonymisierter oder pseudonymisierter Form            |
| <input type="checkbox"/> E-Mail-Verschlüsselung   | <input type="checkbox"/> Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen  |
| <input type="checkbox"/> Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschrufen | <input checked="" type="checkbox"/> Beim physischen Transport: sichere Transportbehälter/-verpackungen |
| <input checked="" type="checkbox"/> Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen                  |  |

### 5. 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"/> Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. |
| <input checked="" type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) | <input type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind   |
| <input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts                    |   |



## 6. Auftragskontrolle

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

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)              | <input type="checkbox"/> vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen |
| <input checked="" type="checkbox"/> schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG | <input checked="" type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)   |
| <input type="checkbox"/> Auftragnehmer hat Datenschutzbeauftragten bestellt  | <input checked="" type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags                |
| <input type="checkbox"/> Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart  | <input checked="" type="checkbox"/> laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten                       |
| <input type="checkbox"/> Vertragsstrafen bei Verstößen   |  |

## 7. Verfügbarkeitskontrolle

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

- |  |  |
|--|--|
| <input checked="" type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV)                              | <input checked="" type="checkbox"/> Klimaanlage in Serverräumen                |
| <input checked="" type="checkbox"/> Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | <input checked="" type="checkbox"/> Schutzsteckdosenleisten in Serverräumen    |
| <input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen   | <input checked="" type="checkbox"/> Feuerlöschgeräte in Serverräumen           |
| <input checked="" type="checkbox"/> Alarmmeldung bei unberechtigten Zutritten zu Serverräumen              | <input checked="" type="checkbox"/> Erstellen eines Backup- & Recoverykonzepts |
| <input checked="" type="checkbox"/> Testen von Datenwiederherstellung                                      | <input checked="" type="checkbox"/> Erstellen eines Notfallplans               |
| <input checked="" type="checkbox"/> Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort   | <input checked="" type="checkbox"/> Serverräume nicht unter sanitären Anlagen  |
| <input checked="" type="checkbox"/> In Hochwassergebieten: Serverräume über der Wassergrenze               |  |

## 8. Trennungsgebot

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

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern | <input checked="" type="checkbox"/> Logische Mandantentrennung (softwareseitig)   |
| <input checked="" type="checkbox"/> Erstellung eines Berechtigungskonzepts  | <input checked="" type="checkbox"/> Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden  |
| <input checked="" type="checkbox"/> Versehen der Datensätze mit Zweckattributen/Datenfeldern                      | <input type="checkbox"/> Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System |
| <input checked="" type="checkbox"/> Festlegung von Datenbankrechten   | <input checked="" type="checkbox"/> Trennung von Produktiv- und Testsystem  |



04.05.2018

Datum

Elke Niemann

Andre Freese

Verantwortlicher für die Erstellung (in Druckbuchstaben)

*E. Niemann*

*A. Freese*

Unterschrift des Verantwortlichen