

# Anlage B: Technische und organisatorische Maßnahmen zum Datenschutz

gemäß Art. 28 Abs. 3 lit. c, 32 DSGVO i.V.m. Art. 5 Abs. 1, Abs. 2 DSGVO

## 1. Vertraulichkeit

### 1.1 Zutrittskontrolle

Unbefugten ist der Zutritt zu den vom Auftragnehmer zwecks Erbringung der ihm übertragenen Leistungen genutzten technischen Einrichtungen zu verwehren.

#### Beim Auftragnehmer umgesetzte Maßnahmen:

##### Zutrittskontrolle

- Dokumentation der Vergabe von Schüsseln
- Rückgabe von Schüsseln nach Austritt von Mitarbeitern
- Verwendung sicherer Türen und Fenster

### 1.2 Zugangskontrolle

Es ist zu verhindern, dass die zur Erbringung der in der beschriebenen IT-Dienstleistung notwendigen Einrichtungen (Hardware, Betriebssysteme, Software) von Unbefugten genutzt werden können.

#### Beim Auftragnehmer umgesetzte Maßnahmen:

##### Zugangskontrolle

- Anwendung von Maßnahmen zur Verschlüsselung von lokalen Daten (z. B. Festplatten, Server)
- Automatisches Sperren von PCs/Macs nach 15 Minuten
- Verwendung personalisierter Logins im Unternehmensnetzwerk
- Verwendung sicherer und individueller Passwörter
- Zwei-Faktor-Authentifizierung

### 1.3 Zugriffskontrolle

Es ist sicherzustellen, 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 oder verändert werden können.

#### Beim Auftragnehmer umgesetzte Maßnahmen:

##### Zugriffskontrolle

- Dokumentation eingerichteter Zugänge für Mitarbeiter
- Benutzer- und Rollenkonzepten für interne Systeme
- Sperrung von Zugängen nach Austritt von Mitarbeitern
- Zentrale Verwaltung von Benutzerzugängen und -rechten

### 1.4 Weitergabekontrolle

Es muss dafür gesorgt werden, 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 welchen Stellen die Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

#### Beim Auftragnehmer umgesetzte Maßnahmen:

##### Weitergabekontrolle

- Nutzung SSL-verschlüsselter Übertragungswege im Internet
- Sicherung von Dokumenten beim Versand auf dem Postweg (z. B. undurchsichtige Versandhüllen)
- Verschlüsselter Versand von E-Mails (S/MIME, PGP)
- Verwendung von VPN-Systemen zum Login in das Firmennetzwerk

### 1.5 Trennungskontrolle

Es ist sicherzustellen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

#### Beim Auftragnehmer umgesetzte Maßnahmen:

##### Trennungskontrolle

- Zugriffsberechtigungen für interne Systeme
- Trennung von internem WLAN und Gäste-WLAN
- Trennung von Live- und Entwicklungssystemen
- Verbot der Nutzung von privaten Endgeräten im Firmennetzwerk

### 1.6 Pseudonymisierung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

#### Beim Auftragnehmer umgesetzte Maßnahmen:

##### Pseudonymisierung

- Trennung von Kontaktdaten und weiteren nutzerbezogenen Daten
- Trennung von Kundenstammdaten und Auftragsdaten

### 1.7 Verschlüsselung

Die Verarbeitung personenbezogener Daten soll in einer Weise erfolgen, die eine unbeabsichtigte oder unrechtmäßige oder unbefugte Offenlegung dieser verhindert. Hierzu dienen dem Stand der Technik entsprechende und als sicher geltende Verschlüsselungsmechanismen.

#### Durch den Auftragnehmer umgesetzte Maßnahmen:

##### Verschlüsselung

- Verwendung verschlüsselter Übertragungswege für den Datenaustausch
- Verwendung von Maßnahmen zur verschlüsselten Datenspeicherung
- Verwendung von SSL-Zertifikaten für Hostingumgebungen

## 2. Integrität

### 2.1 Eingabekontrolle

Es muss nachträglich geprüft und festgestellt werden können, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

## Beim Auftragnehmer umgesetzte Maßnahmen:

### Eingabekontrolle

- Benutzer- und Rollenkonzepten für interne Systeme
- Individueller Zugänge für interne Systeme
- Protokollierung von Zugriffen im Firmennetzwerk
- Verwendung personalisierter Logins im Unternehmensnetzwerk

## 2.2 Weitergabekontrolle

Die Maßnahmen zur Weitergabekontrolle gem. 1.4 dienen auch der Sicherstellung der Integrität.

## 3. Verfügbarkeit und Belastbarkeit

### 3.1 Verfügbarkeitskontrolle

Es ist dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

## Beim Auftragnehmer umgesetzte Maßnahmen:

### Verfügbarkeitskontrolle

- Durchführung von Code-Reviews in der Entwicklung
- Erstellung von Code-Dokumentationen in der Entwicklung
- Klimatisierung von Räumen mit kritischer IT-Infrastruktur
- Nutzung von Testverfahren (z. B. Unittests) in der Entwicklung
- Nutzung einer Versionskontrolle (z. B. Gitlab) in der Entwicklung
- Regelmäßige Aktualisierung der Virendefinitionen
- Regelmäßige Durchführung von Datensicherungen
- Regelmäßige Durchführung von Updates
- Regelmäßige Überprüfung der erstellten Datensicherungen
- Verwendung einer Firewall
- Verwendung eines Virens scanners
- Verwendung von RAID-Systemen (z. B. für lokale File- und Entwicklungsserver)

## 3.2 Rasche Wiederherstellbarkeit

Es müssen Maßnahmen getroffen werden, um Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

## Durch den Auftragnehmer umgesetzte Maßnahmen:

### Rasche Wiederherstellbarkeit

- Dokumentation und Test von Datenwiederherstellungen
- Nutzung einer Versionskontrolle (z. B. Git) in der Entwicklung

## 4. Weitere Maßnahmenbereiche

### 4.1 Datenschutz-Managementsystem

Es muss ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung des Datenschutzes und der Wirksamkeit der festgelegten technischen und organisatorischen Maßnahmen implementiert sein.

## Beim Auftragnehmer umgesetzte Maßnahmen:

### Datenschutz-Managementsystem

- Dokumentation von datenschutzrelevanten Zwischenfällen
- Durchführung von Penetrationstests
- Durchführung von Security-Audits durch externe Sachverständige
- Löschen nicht mehr benötigter Daten (z. B. veraltete Daten, Testumgebungen)

- Sichere Entsorgung defekter/nicht mehr benötigter Hardware
- Sichere Entsorgung von Dokumenten (z. B. Aktenvernichter)
- Zuteilung von datenschutzrelevanten Verantwortungsbereichen

## 4.2 Auftragskontrolle

Es muss dafür gesorgt werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

## Beim Auftragnehmer umgesetzte Maßnahmen:

### Auftragskontrolle

- Abschluss von AV-Verträgen mit Dienstleistern, Partnern und Kunden
- Auswahl geeigneter Dienstleister und Partner unter Datenschutzaspekten
- Beauftragung zertifizierter Dienstleister (z. B. TÜV-zertifiziertes Hosting)
- Benennung eines Datenschutzbeauftragten
- Beratung/Aufklärung der Kunden zum Thema Datenschutz
- Durchführung von stichprobenartigen Überprüfungen bei Dienstleistern
- Kommunikation von Verhaltensrichtlinien zum Thema Datenschutz an alle Mitarbeiter
- Regelmäßige Unterweisung und Fortbildung der Mitarbeiter zum Thema Datenschutz