

# ANLAGE 2 ZUM VERTRAG ZUR AUFTRAGSVERARBEITUNG

## SCHUTZMAßNAHMEN DES AUFTRAGNEHMERS (TECHNISCH-ORGANISATORISCHE MAßNAHMEN)

### 1. Beschreibung der Pseudonymisierung

- Verwendung von Kennziffern       Trennung Kontaktdaten       Trennung Stammdaten
- Sonstiges: Der Nutzer wählt einen Alias bei der Registrierung, welcher stellvertretend für diesen in jeglicher öffentlichen Anzeige verwendet wird. Diesen kann der Nutzer jederzeit über das Accountportal bearbeiten.

### 2. Beschreibung der Verschlüsselung

- Symmetrische Verschlüsselung       Asymmetrische Verschlüsselung
- Sonstiges: Die Übertragung personenbezogener Daten ist durch die Nutzung von SSL geschützt.
- Daten wie Passwörter werden immer mit der Verschlüsselung SHA265 kodiert, welches eine Dekodierung nicht ermöglicht.

### 3. Maßnahmen zur Gewährleistung der Vertraulichkeit

#### 3.1 Beschreibung der Zutrittskontrolle

- Alarmanlage       Besucherprotokolle       Bewegungsmelder       Biometrie
- Chipkarten       Empfang       Pförtner       Schließanlage
- Schließsystem (PIN)       Schlüsselverwaltung       Videoüberwachung       Zutrittsbereiche
- Sonstiges: Der Zugang zur Serverhardware ist durch den Betreiber geregelt.

Lokale Datenspeicher wie Laptops (Biometrie) oder Datenspeicher (Passwort) unterliegen Zutrittskontrollen

#### 3.2 Beschreibung der Zugangskontrolle

- Benutzer + Passwort       Benutzerberechtigung       Firewall       MDM
- Sorgfältige Personalauswahl       Sperre extern. Schnittstelle       Verschlüsselung Datenträger       Chipkarten

- Sonstiges: Zugang zur Datenanzeigen und Datenspeichern verfügen über eine Authentifizierung mit Benutzer+Passwort

Die Datenspeicher selbst sind nicht direkt über das Internet erreichbar.

Lokale Datenspeicher wie Laptops (Biometrie) oder Datenspeicher (Passwort) unterliegen Zugangskontrollen

### 3.3 Beschreibung der Zugriffskontrolle

- |  |   |   |  |
|--|---|---|--|
| <input type="checkbox"/> Berechtigungskonzept  | <input type="checkbox"/> Datenlöschung        | <input type="checkbox"/> Aktenvernichtung                 | <input type="checkbox"/> Passwortrichtlinien             |
| <input type="checkbox"/> Protokollierung der Systemnutzung   | <input type="checkbox"/> Sichere Aufbewahrung | <input type="checkbox"/> Verschlüsselung von Datenträgern | <input type="checkbox"/> Verschlüsselung von Smartphones |
| <input checked="" type="checkbox"/> Sonstiges: <u>Speicherorte wie Laptops (Biometrie) und Festplatten (Passwort) unterliegen Zugriffskontrollen</u> |   |   |  |

### 3.4 Beschreibung der Weitergabekontrolle

- |  |  |  |  |
|--|--|--|--|
| <input type="checkbox"/> E-Mail-Verschlüsselung  | <input type="checkbox"/> Sichere Transportbehälter | <input type="checkbox"/> SSL/TLS Verschlüsselung       | <input type="checkbox"/> VPN-Tunnel        |
| <input type="checkbox"/> Passwortabfrage   | <input type="checkbox"/> Firewall                  | <input type="checkbox"/> Arbeitsanweisungen/Schulungen | <input type="checkbox"/> Protokollierungen |
| <input checked="" type="checkbox"/> Sonstiges: <u>Es besteht keine Weitergabe vertraulicher Daten.</u> |  |  |  |

### 3.5 Beschreibung des Trennungskontrolle

- |   |   |  |   |
|---|---|--|---|
| <input type="checkbox"/> Logische Mandantentrennung | <input type="checkbox"/> Physikalische Trennung der Daten | <input checked="" type="checkbox"/> Produktiv- und Testsysteme | <input type="checkbox"/> Schulung der Mitarbeiter |
| <input type="checkbox"/> Sonstiges: _____           |   |  |   |

## 4. Maßnahmen zur Gewährleistung der Integrität

### 4.1 Beschreibung der Eingabekontrolle

- |   |  |   |   |
|---|--|---|---|
| <input type="checkbox"/> Protokollierung der Eingaben   | <input type="checkbox"/> Speicherung Log-Files für längeren Zeitraum | <input type="checkbox"/> Schulung Mitarbeiter | <input type="checkbox"/> Regelmäßige Auswertung Log-Files |
| <input checked="" type="checkbox"/> Sonstiges: <u>Die Änderung Personenbezogener Daten erfolgen nur über das Accountportal nach vorheriger Authentifizierung.</u> |  |   |   |
| <u>Zugriff auf die Änderung Personenbezogener Daten direkt in der Datenbank hat nur der Admin.</u>  |  |   |   |

## 4.2 Beschreibung sonstiger TOM

- Personalisierte Benutzernamen       Protokollierung       Zugriffsrechte

- Sonstiges: Das Zugriffsrecht auf die Datenbanksektion der Personenbezogenen Daten hat nur der Admin.
- 
- 

## 5. Maßnahmen zur Verfügbarkeit

- Antivirensoftware       Auslagerung der Datensicherung       Backup- und Recovery-konzept       Brandmeldeanlagen
- Feuerlöschgeräte       IT-Notfallplan       Klimaanlage       Redundante Datenerhaltung
- Temperaturüberwachung       Unterbrechungsfreie Stromversorgung       Sicherungskopien       Verhaltensanweisungen; Schulungen

- Sonstiges: \_\_\_\_\_
- 
- 

## 6. Maßnahmen zur Gewährleistung der Belastbarkeit

- Speicherkapazitäten       Zugriffskapazitäten       Leitungskapazitäten

- Sonstiges: Durchführung von Belastungstests
- 
- 

## 7. Beschreibung der raschen Wiederherstellbarkeit nach physischem oder technischen Zwischenfall

- Datenwiederherstellung       Notfallpläne       Redundante Datenerhaltung       Cloud-Lösung
- Doppelte IT-Infrastruktur       Schatten-Rechenzentrum

- Sonstiges: \_\_\_\_\_
- 
-

## 8. Weitere Maßnahmen zum Datenschutz

### 8.1 Beschreibung des Managementsystems zum Datenschutz (Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung)

- |   |   |   |  |
|---|---|---|--|
| <input type="checkbox"/> Audits                           | <input type="checkbox"/> Incident-Response-System         | <input type="checkbox"/> Managementsystem Datenschutz | <input type="checkbox"/> Managementsystem Informationssicherheit |
| <input checked="" type="checkbox"/> Schwachstellenanalyse | <input type="checkbox"/> Softwareseitige Voreinstellungen | <input type="checkbox"/> Softwaregestützte Tools      | <input type="checkbox"/> 24/7 Monitoring                         |

Sonstiges: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

### 8.2 Beschreibung der Auftragskontrolle

- |                                 |  |                                     |   |
|---------------------------------|--|-------------------------------------|---|
| <input type="checkbox"/> Audits | <input type="checkbox"/> Laufende Überprüfungen; Kontrollbesuche | <input type="checkbox"/> Schulungen | <input type="checkbox"/> Verpflichtungen auf das Datengeheimnis |
|---------------------------------|--|-------------------------------------|---|

Sonstiges: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

### 8.3 Sonstige Bemerkungen zu den Maßnahmenbeschreibungen

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## 9. Schriftliche Anlagen gemäß obenstehender Angaben

- |   |  |  |  |
|---|--|--|--|
| <input type="checkbox"/> Verhaltensregeln | <input type="checkbox"/> Risikoanalyse | <input type="checkbox"/> Allgemeine Datensicherheitsbeschreibung | <input type="checkbox"/> Umfassendes Datensicherheitskonzept |
|---|--|--|--|

Wiederanlaufkonzept

Zertifikat

Zertifizierungsstelle:

Sonstiges: \_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_