# Beschreibung der technischen und organisatorischen Massnahmen

## 1. Zweck und Anwendungsbereich

Dieses Dokument beschreibt die umgesetzten technischen und organisatorischen Massnahmen zum Informations- und Datenschutz. Es vermittelt einen Überblick über die umgesetzten technischen und organisatorischen Massnahmen und erfüllt die in der Datenschutz-Grundverordnung (DS- GVO) geforderten Dokumentations- und Nachweispflichten gem. Art. 24 Abs. 1 DS-GVO und die Anforderungen an die Rechenschaftspflicht gem. Art. 5 Abs. 2 DS-GVO.

## 2. Beschreibung der technischen und organisatorischen Massnahmen

### 2.1. Pseudonymisierung und Trennungskontrolle

#### 2.1.1. Pseudonymisierung

#### 2.1.2. Trennungskontrolle

Folgende Massnahmen wurden getroffen, um zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeiten zu können:

–

### 2.2. Verschlüsselung personenbezogener Daten

### 2.3. Gewährleistung der Vertraulichkeit

#### 2.3.1. Zutrittskontrolle

Folgende Massnahmen zur Zutrittskontrolle wurden getroffen, mit denen Unbefugten der physische Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden sowie zu den vertraulichen Akten und Datenträgern verwehrt wird:

☒ Sicherheitstüren (Brandschutz)

☒ Elektronisches Zutrittskontrollsystem mittels Chipkartenzugangssystem sowie separaten Türschlüsseln

☐ Sperrbereiche

☒ Das Gebäude ist durch Brandmelde-, Alarmanlage und Wachdienst gesichert. Der Wachdienst übernimmt die Überwachung des Gebäudes außerhalb der Geschäftszeiten.

☒ Ein zentraler Eingangsbereich mit Empfang ist vorhanden.

☐ Ein Zutritt von betriebsfremden Personen/Gästen/Besuchern und sonstigen Dritten zu den Geschäftsräumen ist nur mit Voranmeldung und in Begleitung einer zutrittsberechtigten Person möglich.

☐ Die Zutrittsberechtigungen sind im Zutrittsberechtigungssystem hinterlegt. Für die Vergabe und den Entzug sind die Vorgesetzten zuständig. Die Steuerung und deren Entzug erfolgt zentral auf Weisung der Vorgesetzten.

☐ Dokumentation und Verwaltung der Chipkarten- und Schlüsselvergabe

☐ …

#### 2.3.2. Zugangskontrolle

Folgende Sicherheitsmassnahmen zur Zugangskontrolle wurden getroffen, um Datenverarbeitungssysteme vor der Nutzung Unbefugter zu schützen:

☒ Alle Datenverarbeitungsanlagen sind zugangsgeschützt.

☒ Zur Anmeldung/Log-In gegenüber der Datenverarbeitungsanlage muss der Benutzer seiner Benutzerkennung (User-ID) und sein persönliches Passwort eingeben.

☒ Zusätzlicher System-Log-In für bestimmte Anwendungen.

☒ Firewall und Netz-Segmentierungen der internen Netzwerke als Abschottung gegen ungewollten Zugang und Zugriffe von außen.

☒ Viren Scanner und Virenschutz-Richtlinien.

☒ Scannen des ein- bzw. ausgehenden E-Mail- und Web-Verkehrs über verschiedene Schutzsysteme.

☒ Sicherung der FTP-Servers für die externe Datenübermittlung über einen Virenscanner.

☐ …

#### 2.3.3. Zugriffskontrolle

Folgende Massnahmen zur Zugriffskontrolle wurden getroffen, die zur Benutzung eines Datenverarbeitungssystems berechtigte Personen ausschliesslich auf Daten entsprechend ihrer Zugriffsberechtigung zugreifen lassen können, und dass personenbezogene Daten bei der Verarbeitung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

☐ Aufgabenbezogene Berechtigungsprofile durch Reglementierung oder Vergabe durch den Auftraggeber.

☒ Verwaltung von Berichtigungen – „Prinzip der minimalen Berechtigung". Jeder Beschäftigte erhält nur die Berechtigung, die für die Erfüllung seiner Tätigkeit minimal erforderlich ist.

☒ Differenzierte Berechtigungen.

☒ Vergabe und Entzug von Berechtigungen.

☒ Dokumentation von Berechtigungen.

☐ Protokollierung und Auswertung der Zugriffe.

☒ Verwaltung des Zugriffs auf den Terminalserver von Administratoren.

☒ Der Zugriff auf Datensicherungen (Backup, Bandsicherung, Transfer der Bandmedien) ist auf berechtigte Systemadministratoren beschränkt.

☒ Identifikation durch Passwörter, Einmal-Passwörter und Keys.

☐ Aufbewahrung ausgemusterter Festplatten in verschlossenen Behältnissen in einem abgeschlossenen Raum bis zur Entsorgung bzw. Vernichtung.

☒ Spezielle Regelungen zur Datenträgervernichtung.

☐ …

## 2.4. Gewährleistung der Integrität

#### 2.4.1. Weitergabekontrolle

Folgende Massnahmen zur Weitergabekontrolle wurden getroffen, die bei der elektronischen Übertragung oder beim Transport von personenbezogenen Daten oder ihrer Speicherung auf Datenträger eingesetzt werden, um unberechtigte Zugriffe, insbesondere zum Lesen, Kopieren, Verändern oder Entfernen dieser Daten zu verhindern, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

☒ Physikalischer Versand von Daten im Rahmen des mit dem Auftraggeber vereinbarten Verfahren nur auf Anweisung des Auftraggebers und an autorisierte Personen sowie ggf. verschlüsselt nach Vorgaben des Auftraggebers oder nach dem aktuellen Stand der Technik.

☒ Protokollierung der Verbindung.

☒ E-Mails mit vertraulichen Inhalten werden verschlüsselt.

☒ Gesichertes WLAN.

☒ Gäste WLAN.

☒ SSL-Verschlüsselung nach dem aktuellen Stand der Technik.

☒ Zugriff auf Restore Funktionen nur durch Beschäftigte. Transport der Sicherungsbänder in einem gesicherten Behältnis und Lagerung in Tresor.

☐ Datenlöschungen werden nur nach schriftlicher Beauftragung durch den Auftraggeber oder auf der Grundlage der vertraglichen Vereinbarungen datenschutzkonform durchgeführt.

☒ Löschung von Daten nach Auftragsende wird mit dem Auftraggeber individuell vereinbart, soweit im Rahmen der vertraglichen Vereinbarungen überhaupt personenbezogene Daten vorhanden sind.

☐ Verschlüsselung der Festplatten von mobilen Endgeräten.

☐ …

2.4.2. Eingabekontrolle

Folgende Massnahmen zur Eingabekontrolle wurden getroffen, durch die festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssystemen eingegeben, verändert oder entfernt worden sind:

☐ Im Regelfall keine Eingabe, Veränderung oder Entfernung von personenbezogenen Daten in Datenverarbeitungssystemen des Auftraggebers.

☐ Manuelle Änderungen an Kundendaten erfolgen nur im Rahmen der vertraglichen Vereinbarungen und/oder nach ausdrücklicher, schriftlicher (auch per Textform, E-Mail zulässig) Beauftragung durch den Kunden.

☒ Zur Anmeldung/Log-In gegenüber der Datenverarbeitungsanlage muss der Benutzer seiner Benutzerkennung (User-ID) und sein persönliches Passwort eingeben.

☒ Zugriffsrechte.

☒ Systemseitige Protokollierungen der An- und Abmeldevorgänge.

☐ ...

2.4.3. Auftragskontrolle

Folgende Massnahmen zur Auftragskontrolle wurden getroffen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

☒ Wach-, Reinigungs-, Entsorgungs- und Transportpersonal und andere weitere Dienstleister, deren Leistung nicht den konkreten Auftrag als Unterauftragnehmer, sondern indirekt eine Hilfstätigkeit betrifft, werden sorgfältig ausgewählt.

☒ Zur Gewährleistung des Schutzes und der Sicherheit werden auch bei fremd vergebenen Nebenleistungen angemessene vertragliche Vereinbarungen getroffen sowie Kontrollmaßnahmen ergriffen.

☐ Bestimmung von Ansprechpartnern und Projektverantwortlichen für den konkreten Auftrag.

☐ Bei Auftragsverarbeitung schriftlicher Vertrag gemäß Art. 28 Abs. 3 DS-GVO.

☐ Keine Beauftragung von Unterauftragnehmern ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Auftraggebers. Abschluss von Verträgen über Auftragsverarbeitung nach Art. 28 Abs. 4 DS-GVO im Falle einer Beauftragung eines Unterauftragnehmers.

☐ …

## 2.5. Gewährleistung der Verfügbarkeit

Folgende Massnahmen sind getroffen worden, die gewährleisten, dass Daten nicht zufällig verloren gehen oder zerstört werden:

☒ Unterbrechungsfreie Stromversorgung (USV) inkl. Batterieversorgung sowie Netzersatzanlage.

☒ Feuerlöschgeräte im oder unmittelbar vor dem Serverraum.

☒ Einhaltung der einschlägigen Brandschutzvorschriften.

☐ Brandfrühtest- und Feuermeldeanlage.

☐ Der Serverraum ist an die zentrale Brandfrühtest- und Feuermeldeanlage angeschlossen.

☐ Besonderer Wassereintrittsschutz für Serverraum.

☒ Vollständig redundante Auslegung der aktiven Komponenten wie z.B. Klimaanlage, USV, usw.

☒ Permanente und redundante Überwachung der Betriebsparameter zur frühzeitigen Erkennung von Störungen.

☒ Überwachung der Temperatur im Serverraum.

☐ Überwachung der Feuchtigkeit im Serverraum.

☒ Wartungsverträge für die Infrastruktureinrichtungen.

☒ Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, SPAM-Filter) mit automatisierten Standardroutinen für regelmäßige Aktualisierung (z.B. Virenscanner), sofern technisch umsetzbar.

☒ Einsatz von Storage Systemen mit Redundanz (RAID).

☐ ...

## 2.6. Gewährleistung der Belastbarkeit der Systeme

☒ Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Belastbarkeit der Datenverarbeitungssysteme werden eingesetzt.

☒ Regelmäßige Überprüfung der Redundanzen.

☒ Kontrollen des Datenschutzbeauftragten.

☐ ...

## 2.7. Verfahren zur Wiederherstellung der Verfügbarkeit personenbezogener Daten nach einem physischen oder technischen Zwischenfall

Folgende Massnahmen wurden getroffen, die gewährleisten, dass personenbezogene Daten nicht zufällig verloren gehen oder zerstört werden:

☒ Kundenindividuelle Backup- & Recovery Konzepte.

☒ Sicherungskopien werden nach dem Generationenprinzip in geeigneten zeitlichen Abständen erstellt.

☒ Der Datenbestand wird wenigstens einmal täglich inkrementell, wenigstens einmal wöchentlich vollständig auf externe Speichermedien gesichert.

☒ Mehrfache getrennte Aufbewahrung der Datensicherungsbänder.

☐ Die jeweils letzte vollständige Sicherungskopie wird unmittelbar nach ihrer Erstellung an einem sicheren Ort im gleichen Gebäudekomplex untergebracht und regelmäßig betriebsextern in einem Bankschließfach sicher verwahrt.

☒ Backup-Verzeichnisse werden geführt bzw. es existiert eine Backup-Verzeichnisstruktur.

☐ Wiederanlauf- und Notfallpläne nach ISO/IEC 27001:2013 und Geprüftes Rechenzentrum hochverfügbar Stufe 3 tekPlus im Falle eines Rechenzentrumsausfalls oder Ausfalls kritischer Komponenten.

☐ Um das Backupsystem im Notfall wiederherzustellen, wird regelmäßig ein Disaster Recovery Image der CommServe Konfiguration generiert.

☐ ...

## 2.8. Verfahren regelmässiger Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen

☐ Die vorhandenen Dokumentationen der Datensicherheit werden regelmäßig auf Aktualität geprüft.

☐ Sicherheitsvorfälle werden dokumentiert und ausgewertet.

☐ Es werden Tests zur Simulation von Sicherheitsvorfällen durchgeführt und Ergebnisse dokumentiert, z. B. Katastrophenfalltests.

☐ Es erfolgen interne Audits durch den betrieblichen Datenschutzbeauftragten und/oder die IT.

☐ Es erfolgen externe Audits, insbesondere im Rahmen der Re-Zertifizierung.

☒ Ein betrieblicher Datenschutzbeauftragter wurde benannt bzw. bestellt.

☒ Verpflichtung aller Beschäftigten auf die Einhaltung der datenschutzrechtlichen Anforderungen nach der DS-GVO, des Sozialgeheimnisses gemäß § 35 SGB I-neu, des Fernmeldegeheimnisses gemäß § 88 TKG und Belehrung auf die sogenannten „Hackerparagraphen“ (§§ 202a ff, § 263a StGB).

☒ Unterrichtung und Verpflichtung der Beschäftigten über Vertraulichkeits- und Sorgfaltspflichten im Zusammenhang mit der Bearbeitung von Daten, Projekten und im Umgang mit Informationstechnik.

☒ Fremdpersonal ist ebenfalls auf Vertraulichkeit verpflichtet.

☒ Schulungen der Beschäftigten.

☒ Regelmäßig stattfindende Nachschulungen.

☐ ...

### 2.9. Informationssicherheitsmanagement

Folgende Prüfungen und Zertifizierungen zur Informationssicherheit wurde durchgeführt:

-

## 3. Weitere Massnahmen

### 3.1. Massnahmenbereich Personal

3.1.1. Einarbeitung neuer Beschäftigter

ja

3.1.2. Regelmässige Informationen

Ja, durch Geschäftsführer persönlich

3.1.3. Verfahren beim Ausscheiden von Beschäftigten

Ja

### 3.2. Massnahmenbereich Gebäude

3.2.1. Brandschutz

Ja, gemäss Kopas und Suva

3.2.2. Allgemeine Sicherungsmassnahmen

Ja, gemäss Kopas und Suva