# TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN (TOM)

DURCH DIE LIBERA AG (Stand 01.09.2023)

## 1. Verwendete Datenelemente

1.1 Der Kunde überlässt LIBERA im Rahmen der Verträge in seinem eigenen Ermessen und in seinem Auftrag Personendaten und/oder geheimnisgebundene Daten zur Bearbeitung.

1.2 Es gilt dabei zwischen Personendaten und besonders schützenswerten Personendaten zu unterscheiden.

Mit **«Personendaten»** sind Daten gemeint, die sich auf eine bestimmte oder bestimmbare Person beziehen, d. h. die Rückschlüsse auf deren Identität zulassen.

**«Besonders schützenswerte Personendaten»** sind Kategorien von Personendaten, die besonders heikel sind, weshalb deren Bearbeitung besonderen Anforderungen unterstehen kann. Als besonders schützenswerte Personendaten gelten z. B. Gesundheitsdaten und Daten über strafrechtliche oder verwaltungsrechtliche Sanktionen sowie über die soziale Hilfe.

1.3 Unsere Datenbearbeitungen können insbesondere folgende Personen betreffen:

- Potentielle Kunden, Kunden, Geschäftspartner – welche natürliche Personen sind
- versicherte Personen, die der Vorsorgelösung des Kunden angehören
- Drittpersonen, die mit denjenigen Personen, die der Vorsorgelösung des Kunden angehören, rechtlich verbunden sind

Es kann sich dabei insbesondere um folgende Arten von Personendaten handeln:

- Stammdaten (Vorname, Nachname, Geburtsdatum, Alter, Geschlecht, Nationalität etc.)
- Finanzdaten (Lohn, Altersguthaben, etc.)
- Gesundheitsdaten
- Angaben zur sozialen Hilfe oder straf- und verwaltungsrechtlichen Sanktionen
- Kommunikationsdaten (Telefon, E-Mail etc.)

1.4 Bei geheimnisgebundenen Daten kann es sich beispielsweise um Daten, die dem Berufsgeheimnis, dem Bankgeheimnis, dem Amtsgeheimnis, der Verschwiegenheitspflicht gemäss Sozialversicherungsrecht unterliegen, handeln.

1.5 Wurden die Daten durch den Kunden verschlüsselt und sind sie für LIBERA daher nicht einsehbar, handelt es sich nicht um eine Auftragsdatenbearbeitung durch LIBERA. Damit ist die Vereinbarung über die Auftragsdatenbearbeitung auf diese Daten nicht anwendbar.

1.6 Die Beurteilung, ob die nachfolgend beschriebenen technischen und organisatorischen Massnahmen zum Schutz der LIBERA zur Bearbeitung anvertrauten Daten (namentlich bei besonders schützenswerten Personendaten oder geheimnisgebundenen Daten) angemessen sind, obliegt ausschliesslich dem Kunden.

## 2. Technische und organisatorische Massnahmen

2.1 Die folgenden Kapitel beschreiben die von LIBERA getroffenen Massnahmen in Bezug auf den Schutz von Personendaten im Rahmen der Auftragsdatenbearbeitung. Die nachstehend aufgeführten Massnahmen sind generisch zu verstehen. Die nachfolgenden Massnahmen gelten für die Fälle, in welchen LIBERA selbst die relevanten Daten verarbeitet. Findet die Datenbearbeitung durch von LIBERA beauftragte Dritte statt, sorgt LIBERA mittels geeigneter vertraglicher Vereinbarungen dafür, dass die Dritten vergleichbare Massnahmen einhalten.

2.2 Zutrittskontrolle – Massnahmen, die geeignet sind, Unbefugten den Zutritt zu den Datenverarbeitungsanlagen, mit denen personenbezogenen Daten verarbeitet oder genutzt werden, zu verwehren:

- Manuelles Schliess-System
- Sicherheitsschlösser
- Schlüsselregelung (Schliessplan)
- Sorgfältige Auswahl von Reinigungspersonal
- Auswahl von Mitarbeitenden unter Sorgfaltspflichtspunkten (insbesondere berufliche Fähigkeiten und Integrität)

2.3 Zugangskontrolle – Massnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Zuordnung von Benutzerrechten
- Erstellen von Benutzerprofilen
- Passwortvergabe
- Authentifikation mit Benutzername/Passwort
- Protokollierung des Zugangs (der Benutzer)
- Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität (passwortgeschützter Bildschirmschoner)
- Einsatz von VPN-Technologie
- Einsatz einer Zwei-Faktor Authentifizierung
- Planmässige Schulungen zur Sensibilisierung von Mitarbeitenden
- Verschlüsselung von Datenträgern in Laptops
- Einsatz von Anti-Viren-Software
- Einsatz einer Hardware-Firewall
- Einsatz einer Software-Firewall
- Regelmässiges Patchen der Infrastruktur
- Regelmässiges Security Testing der Infrastruktur
- Regelmässige Überprüfung der Security Awareness von Mitarbeitenden

2.4 Zugriffskontrolle – Massnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigte 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:

- Berechtigungskonzept
- Verwaltung der Rechte durch Systemadministrator
- Anzahl der Administratoren auf das Notwendigste reduziert
- Passwortrichtlinie (Passwortlänge, Passwortwechsel)
- Physische und nicht reversible Löschung von Datenträgern vor Wiederverwendung
- Ordnungsgemässe Vernichtung von Datenträgern
- Einsatz von Aktenvernichtern durch Dienstleister mit DIN-66399 Zertifizierung

2.5 Trennungskontrolle – Massnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können. Die Verarbeitung erfolgt nur für den Zweck, für den sie erhoben worden ist:

- Trennung von Produktiv- und Testumgebung
- Physikalische Trennung (Systeme / Datenbanken / Datenträger)
- Steuerung über Berechtigungskonzept
- Festlegung von Datenbankrechten
- Segmentierung des Netzwerkes

2.6 Weitergabekontrolle – Massnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und, dass überprüft und festgestellt werden kann, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Einrichtungen von VPN-Tunneln
- Einsatz einer Zwei-Faktor Authentifizierung
- Weitergabe von Daten in verschlüsselter Form (M365 Mail Verschlüsselung)
- Verschlüsselung von Datenträgern in Laptops
- Verschlüsselung von externen Datenträgern

2.7 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:

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten (Berechtigungskonzept)
- Servermonitoring mit Logging und Event-Detection
- Protokollierung aller Manipulationen von Daten im Verwaltungssystem

2.8 Auftragskontrolle (Outsourcing an Dritte) – Massnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftragsgebers verarbeitet werden können. Unter diesen Punkt fällt neben der Datenverarbeitung im Auftrag auch die Durchführung von Wartung und Systembetreuungsarbeiten sowohl vor Ort als auch per Fernwartung.

Die LIBERA ist zum Beizug von Unter-Auftragsdatenbearbeitern berechtigt, sofern diese mindestens die gleichen technischen und organisatorischen Massnahmen einhalten. Die für die Auftragsabwicklung verwendete IT-Services werden von verschiedenen Dienstleistern betreut. Mit allen Dienstleistern, die möglicherweise Einsicht in Personendaten haben könnten, hat Libera vertragliche Vereinbarungen getroffen.

Die LIBERA tritt insbesondere die folgenden Massnahmen, um Auftragskontrolle zu gewährleisten:

- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (speziell in Bezug auf Datenschutz und Datensicherheit)
- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung
- Schriftliche Weisungen an den Auftragnehmer
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis
- Kontrollrechte gegenüber dem Auftragnehmer
- Gleiche Regelungen gelten auch auf Subunternehmer des Auftragnehmers

2.9 Verfügbarkeitskontrolle – Massnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Unterbrechungsfreie Stromversorgung (USV)
- Abgesicherter Zutritt zum Server
- Klimaanlage in Serverräumen
- Brandmelder mit Alarmauslösung
- Keine Wasserleitungen in oder über den Serverräumen
- Erstellen eines Backup- & Recoverykonzepts
- Testen von Datenwiederherstellung
- Erstellen eines Notfallplans
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort in der Schweiz mit ISO-Zertifizierung
- Incident-Response-Management mit festgelegten Bearbeitungszeiten