Technische und organisatorische Massnahmen

1. Vertraulichkeit

(1) Zutrittskontrolle: Predata AG gewährleistet, dass kein unbefugter Zutritt zu Datenbearbeitungsanlagen erfolgt.

Die Zutrittskontrolle zum **Rechenzentrum** von Predata AG bzw. dessen genehmigte Unterauftragnehmer, in welchen die Daten des Auftraggebers gespeichert bzw. bearbeitet oder Zugangsdaten zu denselben gespeichert werden, gestaltet sich wie folgt:

- Zutrittskontrollsystem über [biometrische Kontrolle];
- Schlüsselvergabe nur an beschränkten Personenkreis mit Schlüsselliste;
- Türsicherung (elektrischer Türöffner und biometrische Kontrolle);
- Überwachungseinrichtung durch Alarmanlage und Aufschaltung auf Sicherheitsdienst;
- Zugangstür ständig geschlossen, Zutritt zu den Unternehmensräumen nur nach Klingeln und Öffnen eines Mitarbeiters;

Die Zutrittskontrolle zu den **Räumlichkeiten** von Predata AG bzw. dessen genehmigte Unterauftragnehmer, in welchen die Daten des Auftraggebers gespeichert bzw. bearbeitet oder Zugangsdaten zu denselben gespeichert werden, gestaltet sich wie folgt:

- Schlüsselvergabe nur an beschränkten Personenkreis mit Schlüsselliste;
- Türsicherung (elektrische Türschliessung ausserhalb der Arbeitszeiten);

(2) Zugangskontrolle: Predata AG stellt sicher, dass keine unbefugte Systembenutzung erfolgt. Dafür ergreift sie folgende Massnahmen:

- Kennwortverfahren (u.a. Komplexitätsanforderungen, Mindestlänge 10 Zeichen);
- Zwei oder Multi-Faktor Authentifizierung von ausserhalb der Räumlichkeiten von Predata AG (z.B. Homeoffice);
- Einrichtung eines Benutzerstammsatzes pro User;
- Verwendung von zeitgesteuerter Bildschirmsperre mit Passwortschutz (Betriebsvereinbarung);

- bei Bedarf verschlüsseltes WLAN für den internen Gebrauch, zusätzlich entkoppeltes für Gäste in DMZ;

- Ausgefeiltes Firewall-Konzept;

(3) Zugriffskontrolle: Predata AG stellt sicher, dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen von den bearbeiteten personenbezogenen Daten innerhalb des Systems erfolgt. Predata AG ergreift die folgenden Massnahmen:

- Festlegung und Kontrolle der Zugriffsbefugnisse differenziert nach Daten, Programmen und Zugriffsarten (Berechtigungskonzept);

- Zeitnahes Einspielen der notwendigen Sicherheitsupdates;

- Ständige Aktualisierung des Virenschutzes;

- Sichere Verwaltung und Verwahrung von Datenträgern/-beständen;

- Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network) für eingeschränkten Mitarbeiterkreis;

- Gesicherter Zugriff über Proxy;

- Vernichtung sensibler Unterlagen oder Datenträger durch Entsorgungs-Fachbetrieb, Nachweis über Vernichtung durch Datenvernichtungsprotokoll;

- Verbot der Verwendung privater Datenträger (Betriebsvereinbarung).

(4) Trennungskontrolle: Predata AG stellt sicher, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt bearbeitetet werden. Predata AG ist für die Umsetzung der folgenden Massnahmen besorgt:

- „Mandantenfähigkeit“ der verwendeten Software;

- Trennung der Datensätze durch Speicherung in physikalisch getrennten Datenbanken;

(5) Pseudonymisierung: Die Bearbeitung personenbezogener Daten erfolgt in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Massnahmen unterliegen. Predata AG ist bemüht, Pseudonymisierungsverfahren, wo möglich und zumutbar, umzusetzen.

2. Integrität

(1) Weitergabekontrolle: Predata AG stellt sicher, dass personenbezogene Daten bei einer elektronischen Übertragung oder einem Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Dafür ergreift sie folgende Massnahmen:

- Datenvernichtung entsprechend datenschutzrechtlicher Vorgaben;
- Aufbewahrung in gesichertem Bereich;
- Archivierung aller ausgehenden E-Mails;

(2) Eingabekontrolle: Predata AG kontrolliert regelmässig, ob und von wem personenbezogene Daten in Datenbearbeitungssysteme eingegeben, verändert oder entfernt worden sind. Dafür ergreift sie folgende Massnahmen:

- Protokollierung im Ticketsystem.

3. Verfügbarkeit und Belastbarkeit

(1) Verfügbarkeitskontrolle: Predata AG stellt sicher, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung bzw. Verlust geschützt sind. Predata AG ergreift die folgenden Massnahmen:

- Definiertes Backup-Verfahren;
- Verfügbarkeitsgewährleistung durch redundante Speichersysteme;
- Unterbrechungsfreie Stromversorgung;
- Gesicherter und klimatisierter Serverraum (redundant);
- Räumlich- und mediumgetrennte Aufbewahrung;
- Virenschutz / Firewall;
- Rauchmeldeanlage;
- CO2-Feuerlöscher;
- Notfallplan;

(2) Predata AG sorgt für eine rasche Wiederherstellbarkeit der Systeme und der Daten des Auftraggebers.

4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

(1) Predata AG ist für ein angemessenes Datenschutz-Management und ein Incident-Response-Management besorgt.

(2) Predata AG setzt datenschutzfreundliche Voreinstellungen um, damit möglichst wenig personenbezogene Daten bearbeitet werden.

(3) Auftragskontrolle: Es erfolgt keine Auftrags- bzw. Unterauftragsdatenbearbeitung ohne entsprechende Weisung des Auftraggebers. Predata AG setzt insbesondere die folgenden Massnahmen um:

- Verpflichtung der Mitarbeiter sowie von beauftragten Unternehmen (Dienstleistungsunternehmen, Steuerberater, Wirtschaftsprüfer, Sicherheitsunternehmen und weitere) zum Datenschutz und zur Geheimhaltung;

- Dokumentierte Rückgabe der ggf. überlassenen Datenträger und Löschung von Restdaten;