Technische und organisatorische Massnahmen (TOM)

1 Vertraulichkeit

1.1 Zutrittskontrolle

Die Predata AG stellt sicher, dass kein unbefugter Zutritt zu Datenverarbeitungsanlagen erfolgt. Die Zutrittskontrolle zu den Rechenzentren der Predata AG oder ihrer autorisierten Unterauftragnehmer, in denen die Daten des Auftraggebers gespeichert oder verarbeitet werden, erfolgt durch folgende Massnahmen:

- Zutrittskontrollsystem mittels biometrischer Kontrolle
- Schlüsselvergabe an einen beschränkten Personenkreis, dokumentiert durch eine Schlüsselliste
- Türsicherung durch elektrische Türöffner und biometrische Kontrolle
- Überwachung durch Alarmanlagen mit Aufschaltung auf einen Sicherheitsdienst
- Zugangstüren sind ständig geschlossen; Zutritt zu den Unternehmensräumen erfolgt nur nach Klingeln und Freigabe durch Mitarbeitende

Die Zutrittskontrolle zu den weiteren Räumlichkeiten der Predata AG bzw. deren Unterauftragnehmer erfolgt durch:

- Schlüsselvergabe an einen beschränkten Personenkreis, dokumentiert durch eine Schlüsselliste
- Elektronische Türschliessungen ausserhalb der Arbeitszeiten

1.2 Zugangskontrolle

Um unbefugte Systemzugriffe zu verhindern, ergreift die Predata AG folgende Massnahmen:

- Passwortverfahren mit Komplexitätsanforderungen und einer Mindestlänge von 10 Zeichen
- Zwei- oder Multi-Faktor-Authentifizierung für Zugriffe ausserhalb der Geschäftsräume (z.B. Homeoffice)
- Einrichtung individueller Benutzerstammsätze
- Zeitgesteuerte Bildschirmsperren mit Passwortschutz gemäss Betriebsvereinbarung
- Verschlüsseltes WLAN für den internen Gebrauch; entkoppeltes WLAN für Gäste in einer DMZ
- Firewall-Konzept zum Schutz vor unbefugten Zugriffen

1.3 Zugriffskontrolle

Um unbefugtes Lesen, Kopieren, Verändern oder Entfernen personenbezogener Daten zu verhindern, setzt die Predata AG folgende Massnahmen um:

- Berechtigungskonzept zur differenzierten Kontrolle der Zugriffsbefugnisse nach Daten, Programmen und Zugriffsarten
- Zeitnahe Installation von sicherheitsrelevanten Updates
- Regelmässige Aktualisierung des Virenschutzes
- Sichere Verwaltung und Aufbewahrung von Datenträgern
- Verschlüsselte VPN-Verbindungen für einen eingeschränkten Mitarbeiterkreis
- Gesicherter Zugriff über Proxy-Server
- Fachgerechte Vernichtung sensibler Unterlagen durch zertifizierte Entsorgungsunternehmen mit Nachweisprotokoll
- Verbot der Verwendung privater Datenträger gemäss Betriebsvereinbarung

1.4 Trennungskontrolle

Die Predata AG stellt sicher, dass personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden. Zu den Massnahmen zählen:

- Mandantenfähigkeit der verwendeten Software
- Physische Trennung der Datensätze in separaten Datenbanken

1.5 Pseudonymisierung

Personenbezogene Daten werden, soweit möglich und zumutbar, pseudonymisiert verarbeitet. Eine Zuordnung zu einer bestimmten Person ist ohne Hinzuziehung zusätzlicher Informationen nicht möglich. Diese zusätzlichen Informationen werden separat gespeichert und durch angemessene technische und organisatorische Massnahmen geschützt.

2 Integrität

2.1 Weitergabekontrolle

Um unbefugtes Lesen, Kopieren, Verändern oder Entfernen personenbezogener Daten während der Übertragung oder beim Transport zu verhindern, setzt die Predata AG folgende Massnahmen ein:

- Datenvernichtung gemäss datenschutzrechtlicher Vorgaben
- Sichere Aufbewahrung in überwachten Bereichen
- Archivierung aller ausgehenden E-Mails

2.2 Eingabekontrolle

Die Predata AG kontrolliert, ob und von wem personenbezogene Daten in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt werden. Dies erfolgt durch:

- Protokollierung im Ticketsystem

3 Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Zum Schutz personenbezogener Daten vor zufälliger oder vorsätzlicher Zerstörung bzw. Verlust ergreift die Predata AG folgende Massnahmen:

- Regelmässige und gesicherte Backups
- Redundante Speichersysteme zur Gewährleistung der Verfügbarkeit
- Unterbrechungsfreie Stromversorgung (USV)
- Gesicherte, klimatisierte und redundante Serverräume
- Räumlich und mediengetrennte Aufbewahrung von Backups
- Virenschutz und Firewall-Systeme
- Rauchmelder und CO_2-Feuerlöscher
- Notfallplan zur schnellen Wiederherstellung

3.2 Wiederherstellbarkeit

Die Predata AG gewährleistet eine rasche Wiederherstellung der Systeme und der Daten des Auftraggebers im Falle eines Ausfalls oder eines Vorfalls.

4 Regelmässige Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Management und Incident Response

Die Predata AG verfügt über ein angemessenes Datenschutz-Management und ein Incident-Response-Management.

4.2 Datenschutzfreundliche Voreinstellungen

Es werden datenschutzfreundliche Voreinstellungen umgesetzt, um die Verarbeitung personenbezogener Daten auf das notwendige Minimum zu reduzieren.

4.3 Auftragskontrolle

Es erfolgt keine Auftrags- oder Unterauftragsdatenverarbeitung ohne entsprechende Weisung des Auftraggebers. Zu den Massnahmen zählen:

- Verpflichtung der Mitarbeitenden sowie beauftragter Unternehmen zur Geheimhaltung und zum Datenschutz
- Dokumentierte Rückgabe und fachgerechte Löschung von Datenträgern nach Projektende