Technische und organisatorische Massnahmen

IQ Solutions GmbH
Kirchstrasse 24
3097 Liebefeld

TOMs IQS, Version 1.0 (07.07.2025)

IQ Solutions GmbH
Kirchstrasse 24
3097 Liebefeld
T 031 398 41 51
F 031 398 41 52
info@iqsolutions.ch
www.iqsolutions.ch

IQ solutions

Inhalt

1. Vertraulichkeit

1.1. Zutrittskontrolle: Der Auftragnehmer gewährleistet, dass kein unbefugter, physischer Zutritt zu Datenbearbeitungsanlagen erfolgt.

Die Zutrittskontrolle zum Rechenzentrum und zu den Räumlichkeiten des Auftragnehmers bzw. dessen genehmigte Unterauftragnehmer, in welchen die Daten des Auftraggebers gespeichert bzw. bearbeitet oder Zugangsdaten zu den denselben gespeichert werden, gestaltet sich wie folgt:

Rechenzentrum (NTS Workspace, Colobern Nord, Tier IV)

- Zutrittskontrollsystem über [biometrische Kontrolle];
- Schlüsselvergabe nur an beschränkten Personenkreis mit Schlüsselliste;
- Türsicherung (Schlüssel, elektrischer Türöffner und Biometrische Kontrolle);

Die NTS als Rechenzentrumprovider hat keinerlei Zugriff auf die Systeme oder Personendaten in den Colocations und untersteht dem strengen Fernmeldegeheimnis.

Büroräumlichkeiten (Liebefeld)

- Überwachungseinrichtung durch Alarmanlage und Aufschaltung auf Sicherheitsdienst;
- Ausserhalb der Arbeitszeiten: Überprüfung des Gebäudes durch Sicherheitsdienst (1 Durchgang nachts);
- Zugangstüre ständig geschlossen, Zutritt zu den Unternehmensräumen nur nach Öffnen eines Mitarbeiters;
- Türsicherung Zugang Serverraum (Büro) nur für eingeschränkte Personenkreis mit Schlüssel.

1.2. Zugangskontrolle: Der Auftragnehmer stellt sicher, dass keine unbefugte Systembenutzung erfolgt. Dafür ergreift er folgende Massnahmen:

- Kennwortverfahren (u.a. Komplexitätsanforderungen, Mindestlänge, regelmässiger Wechsel des Kennworts mit Historienverwaltung);
- Automatische Sperrung des Logins bei mehrfache Fehleingabe des Kennworts;
- Zwei-Faktor Authentifizierung;
- Nach Möglichkeit Durchsetzung von persönlichen User-Accounts. Ausnahmen nur nach explizitem Kundenwunsch (mit Hinweis an Kunden). (keine geteilten Logins);
- Passwortschutz und Verschlüsselung der integrierten Datenträger bei Arbeitsstationen und Notebooks;
- Verwendung von zeitgesteuerter Bildschirmsperre mit Passwortschutz;
- Protokollierung der Nutzung von sensiblen Anwendungen (z.B. Passwortmanager, Remote Desktop Management, etc.) ;
- bei Bedarf verschlüsseltes WLAN für den internen Gebrauch, zusätzlich entkoppeltes für Gäste-WLAN;
- Firewall-Konzept;
- Regelmässige Sicherung wichtiger Daten auf ext. Datenträger

Ausserdem werden die Sicherheit des Rechenzentrums (Tier IV) sowie die Räumlichkeiten des Auftragnehmers regelmässig intern überprüft.

1.3. Zugriffskontrolle: Der Auftragnehmer stellt sicher, dass kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen von den bearbeiteten personenbezogenen Daten innerhalb des Systems erfolgt. Der Auftragnehmer ergreift die folgenden Massnahmen:

- Festlegung und Kontrolle der Zugriffsbefugnisse differenziert nach Daten, Programmen und Zugriffsarten (Berechtigungskonzept);
- Auswertungen über Zugriffe bei Bedarf oder Verdachtsfälle;
- Sichere Verwaltung und Verwahrung (Serverraum) von Datenträgern/-bestände;
- Verschlüsselung / Tunnelverbindung (VPN = Virtual Private Network) für eingeschränkten Mitarbeiterkreis;
- Vernichtung sensibler Unterlagen oder Datenträger durch Entsorgungs-Fachbetrieb, Menge und Abholung wird protokolliert;
- Verbot der Verwendung privater Datenträger oder Eingabegeräte (s. ICT Nutzungsrichtlinien für Mitarbeitende).

2. Integrität

2.1. Weitergabekontrolle: Der Auftragnehmer stellt sicher, dass personenbezogene Daten bei einer elektronischen Übertragung oder einem Transport nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Dafür ergreift er folgende Massnahmen:

- Es werden keine Datenträger mit Personendaten versendet oder empfangen;
- Transportsicherung bei Versand mit Nachweiskontrolle (Post-Quittung);
- Datenvernichtung entsprechend datenschutzrechtlichen Vorgaben;
- Aufbewahrung von zu vernichtenden Datenträgern in gesichertem Bereich (Serverraum);
- Verschlüsselung aller ausgehenden E-Mails, wo zumutbar.
- Regelmässige Erneuern unserer Infrastruktur (Clients / Server / Infrastruktur)
- Alle von uns eingesetzten Produkte sind korrekt lizenziert.

2.2. Eingabekontrolle: Der Auftragnehmer kontrolliert regelmässig, ob und von wem personenbezogene Daten in Datenbearbeitungssysteme eingegeben, verändert oder entfernt worden sind.: Auswertungen über Zugriffe bei Bedarf oder Verdachtsfälle

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle: Der Auftragnehmer stellt sicher, dass personenbezogene Daten gegen zufällige oder mutwillige Zerstörung bzw. Verlust geschützt sind. Der Auftragnehmer ergreift die folgenden Massnahmen:

- Definiertes Backup-Verfahren;
- Zeitnahes Einspielen der notwendigen Sicherheitsupdates;
- Ständige Aktualisierung des Virenschutzes;
- Verfügbarkeitsgewährleistung durch redundante Speichersysteme;
- Unterbrechungsfreie Stromversorgung;
- Gesicherter und klimatisierter Serverraum;
- Räumlich- und medium getrennte Aufbewahrung;
- Virenschutz / Firewall;
- Rauchmeldeanlage;
- CO2-Feuerlöscher;
- Notfallplan.

Der Auftragnehmer sorgt für eine rasche Wiederherstellbarkeit der Systeme und der Daten des Auftraggebers.

4. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

4.1. Der Auftragnehmer ist für ein angemessenes Datenschutz-Management und ein Incident-Response-Management besorgt.

4.2. Der Auftragnehmer setzt datenschutzfreundliche Voreinstellungen um, damit möglichst wenig personenbezogene Daten bearbeitet werden.