004 Technische und organisatorische Massnahmen TOM

Allgemeinde Angaben

Datum der letzten Überprüfung:	
Informationen zum Standort von Datenverarbeitungsanlagen und Rechenzentren	Der Standort des Rechenzentrums (hauptsächlich Hosting und E-Mail-Server) liegt bei der Firma XXXX AG. Die Serverstandorte befinden sich in der Schweiz. Weitere Datenverarbeitungen finden in-House statt, ein eigenes Rechenzentrum wird allerdings nicht betrieben.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Zutrittskontrolle (Kein unbefugter Zutritt zu Datenverarbeitungsanlagen)

Konkrete Massnahme	Vorhanden	Kommentare
Zutrittskontrollsystem: Ausweisleser, Magnetkarte, Chipkarte	Ja	
Schlüssel / Schlüsselvergabe	Ja	
Türsicherung (elektrische Türöffner usw.)	Ja	
Gebäudesicherung (Zäune, Pforten)	Nein	
Werkschutz, Pförtner	Nein	
Überwachungseinrichtung: Alarmanlage, Video- / Fernsehmonitor	Ja	
Biometrisches Zugangssystem	Nein	
Alarmsicherung	Nein	
Tragepflicht von Ausweisen / Ausweissystem	Nein	
Schliesssystem	Nein	
Sonstige:	Nein	

Zugangskontrolle (Keine unbefugte Systembenutzung)

Konkrete Massnahme	Vorhanden	Kommentare
Kennwortverfahren (u.a. Sonderzeichen, Mindestlänge, regelmässiger Wechsel des Kennworts)	Ja	
Two-Factor Authentication	Nein	
Automatische Sperrung (z.B. Kennwort oder Pausenschaltung)	Nein	
Einrichtung eines Benutzerstammsatzes pro User	Ja	
Verschlüsselung von Datenträgern	Nein	
Software Firewall	Nein	
Hardware Firewall	Nein	

Einsatz von zentraler Administrations-Software für mobile Endgeräte (z.B. zum externen Sperren und Löschen von Daten)	Nein	
Gehäuseschutz	Nein	
Schutzmassnahmen zur Sicherung bei Nutzung von eigenen Geräten durch Mitarbeiter (z.B. Fernlöschung oder -sperrung)	Nein	
Anti-Viren Software	Nein	
Sonstige:	Nein	

Zugriffskontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems)

Konkrete Massnahme	**Vorhanden**	**Kommentare**
Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte (Profile, Rollen, Transaktionen und Objekte)	Nein	
Benutzerkennung mit Passwort	Nein	
Ausgabe von Zertifikaten zur Authentifizierung	Nein	
Sicherung von Schnittstellen (USB, Firewire usw.)	Nein	
Virenschutz / Firewall	Nein	
Einschränkung der Nutzung von mobilen Datenträgern / sonstigen Geräten	Nein	
Regelmässige Updates der Systeme	Nein	
Klassische Rollen (Auswertungen, Kenntnisnahme, Veränderung, Löschung)	Nein	
Protokollierung von Zugriffen in Logs	Nein	
Sonstige:	Nein	

Trennungskontrolle / Verwendungszweckkontrolle (Getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden)

Konkrete Massnahme	**Vorhanden**	**Kommentare**
"Interne Mandantenfähigkeit"	Nein	
Zweckbindung	Nein	
Separierung Datenbanken	Nein	
Separierung von Tables in Datenbanken	Nein	
Funktionstrennung / Produktion / Test & Sandboxing	Nein	
Sonstige:	Nein	

Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Konkrete Massnahme	**Vorhanden**	**Kommentare**
Umwandeln von Identifiaktionsmerkmalen in zufällige Zeichenfolgen (Z.B. Namen und Geburtsdaten)	Nein	
Identifizierung von Datensätzen mit IDs anstatt Klarnamen und anderen persönlichen Daten	Nein	
Keine Eingabemöglichkeiten von nicht psedonymen Daten (z.B. Angabe von Nicknames statt Klarnamen)	Nein	

Kontrolle der Bestimmbarkeit bei Kumulation von Datensätzen	Nein	
Automatische Pseudonymisierungsverfahren bei neuen Datensätzen	Nein	
Sonstige:	Nein	

Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

Weitergabekontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport)

Konkrete Massnahme	Vorhanden	Kommentare
Verschlüsselung / Tunnelverbindung	Nein	
Prüfung der Rechtmässigkeit der Weitergabe von Daten	Nein	
Regelungen zum datenschutzkonformen Vernichten von Datenträgern	Nein	
Verfahrensverzeichnis	Nein	
Elektronische Signatur	Nein	
Protokollierung	Nein	
Transportsicherung	Nein	
Sonstige:	Nein	

Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind)

Konkrete Massnahme	Vorhanden	Kommentare
Dokumentenmanagement, Dokumentenlenkung	Nein	
Protokollierungs- und Protokollauswertungssysteme	Nein	
Protokollierungs- und Protokollauswertungssysteme (3 Monate Revisionssicher)	Nein	
Plausibilitätskontrollen	Nein	
Sicherung von Protokolldaten gegen Verlust oder Veränderung	Nein	
Sonstige:	Nein	

Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust)

Konkrete Massnahme	Vorhanden	Kommentare
Backup-Strategie (offline)	Nein	
Backup-Strategie (online, z.B. Cloud)	Nein	
Unterbrechungsfreie Stromversorgung (USV)	Nein	
Getrennte Aufbewahrung	Nein	
Überspannungsschutz	Nein	
Schutz vor Diebstahl	Nein	
Virenschutz / Firewall	Nein	

Sonstige:	Nein	

Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO - die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen)

Konkrete Massnahme	Vorhanden	Kommentare
Notfallmanagement inkl. Notfallpläne	Nein	
Testen der Wiederherstellungssysteme	Nein	
Incident Management	Nein	
Sonstige:	Nein	

Technische und organisatorische Umsetzung des Rechts auf Löschung, "Recht auf Vergessenwerden" (Art. 17 DS-GVO)

Folgende Massnahmen wurden ergriffen:

Konkrete Massnahme	Vorhanden	Kommentare
Einfache Datenlöschung (ohne Überschreiben)	Nein	
Randomisiertes Überschreiben von Datensätzen	Nein	
Implementierung von Fernlöschung, z.B. auf mobilen Endgeräten	Nein	
Zerstörung von Datenträgern vor der Entsorgung	Nein	
Schreddern / mechanische Deformierung von Datensätzen auf Papier / DVD / CD oder sonstigen Datenträgern	Nein	
Entmagnetisierung von physischen Datenträgern (Festplatten / Datenbändern)	Nein	
Automatische Löschung von Datensätzen nach einem festgelegten Ablaufdatum	Nein	
Sorgfältige Auswahl von Entsorgungsdienstleistern	Nein	
Klassifikation der Daten in Schutzklassen	Nein	
Umsetzung der DIN-EN 15713 “Sichere Vernichtung von vertraulichen Unterlagen - Verfahrensregeln”	Nein	
Protokollierung von Löschvorgängen	Nein	
Sonstige:	Nein	

Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung

Konkrete Massnahme	Vorhanden	Kommentare
Datenschutz-Management	Nein	
Regelmässige Datenschutzschulungen	Nein	
Incident-Response-Management	Nein	
Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)	Nein	
Auftragskontrolle (BCR)	Nein	

Auftragskontrolle (AV)	Nein	
Eindeutige Vertragsgestaltung	Nein	
Vorabüberzeugungspflicht	Nein	
Nachkontrollen	Nein	
Sonstige:	Nein	

Gesamtevaluierung der Massnahmen

Die dokumentierten Massnahmen sind unter Berücksichtigung des aktuellen Standes der Technik, angemessener Implementierungs- und Wartungskosten, der Art, des Umfangs und der Zwecke der Verarbeitung, sowie unter Abwägung der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten der Betroffenen wie folgt geeignet, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten:	Sie sind geeignet.	ja