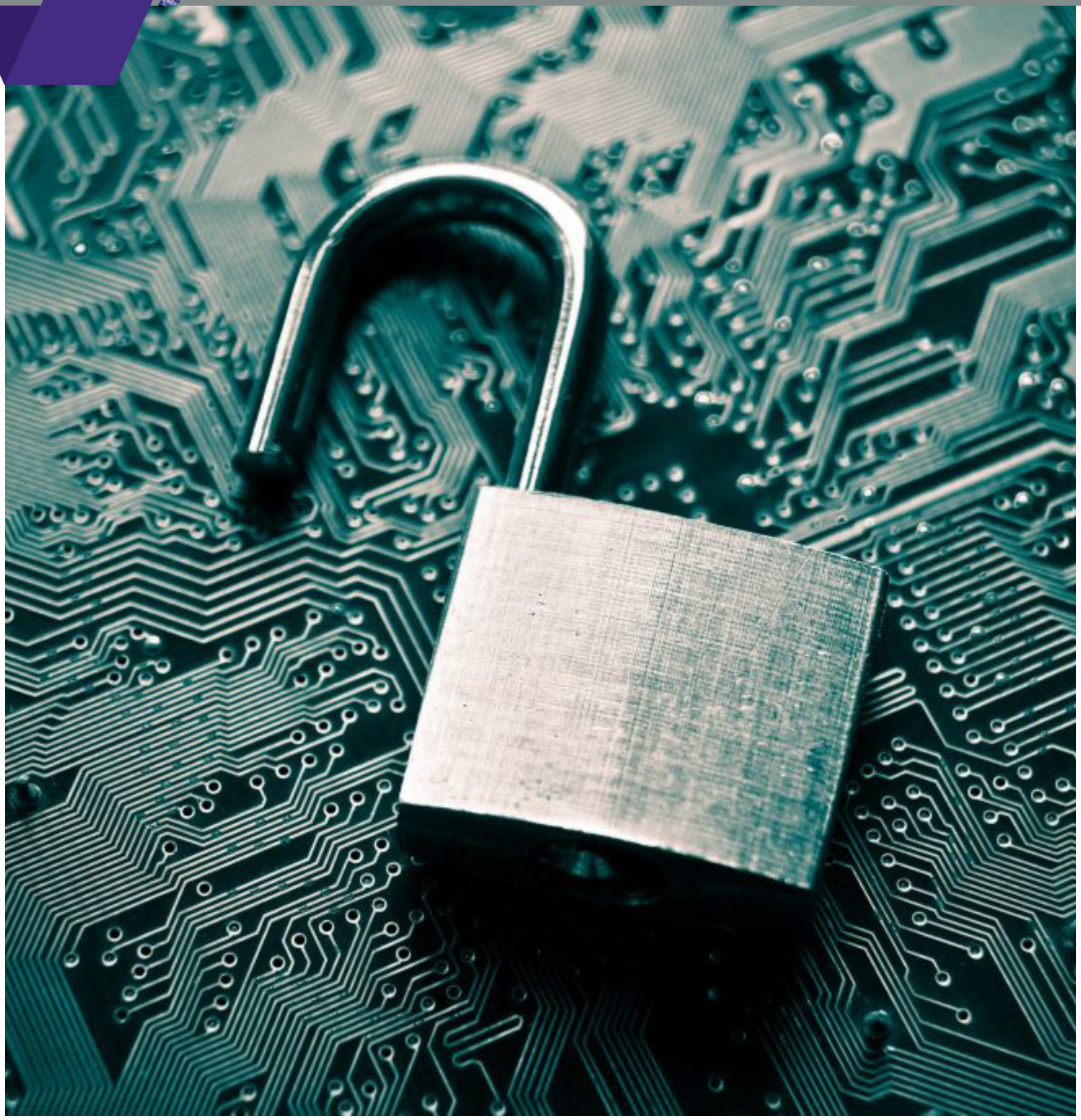
E.C.S.
ELEKTRONIK COMPUTER SERVICE

TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN

Anlage TOM — Datensicherheit — Art. 32 DSGVO — Version 2.0 — 2019



1. Vertraulichkeit

1.1 Zutrittskontrolle

Übersicht aller getroffenen Maßnahmen – Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

Technische Maßnahmen	
› Alarmanlage + professionelle Management Software	✓
› Automatisches Zugangskontrollsystem	✓
› Chipkarten / Transpondersysteme	✓
› Sicherheitsschlösser	✓
› elektronisches Schließsystem	✓
› Absicherung der Gebäudeschächte	✓
› Türen mit Knauf Außenseite	✓
› Klingelanlage mit Kamera	✓
› Videoüberwachung der Eingänge und Gebäude	✓

Organisatorische Maßnahmen	
› Zugang mit Schlüsselregelung	✓
› aktives Zugangs- und Berechtigungskonzept	✓
› Zutritt ins Gebäude nur nach Anmeldung	✓
› Besucher nur in Begleitung durch Mitarbeiter	✓
› Sorgfalt bei Auswahl Lieferanten und Partner	✓
› keine automatische Türöffnung - alle Zugänge sind verschlossen	✓

1.2 Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.

Technische Maßnahmen	
› Login mit Benutzername + Passwort	✓
› Anti-Viren-Software Server	✓
› Anti-Virus-Software Clients	✓
› Anti-Virus-Software mobile Geräte	✓
› Firewall	✓
› Verschlüsselung von Datenträgern	✓
› Sperre externer Schnittstellen (USB)*	✓
› Automatische Desktopsperre	✓
› Verschlüsselung von Notebooks / Tablet	✓

Organisatorische Maßnahmen	
› Verwalten von Benutzerberechtigungen	✓
› Erstellen von Benutzerprofilen	✓
› Zentrale Passwortverwaltung	✓
› Anwendung Richtlinien:	✓
– „Sicheres Passwort“	✓
– „Löschen / Vernichten“	✓
– „Clean desk“	✓
– Allg. Datenschutz/Sicherheit/Vertraulichkeit	✓
– Anleitung „Manuelle Desktopsperre“	✓

** ist jederzeit umsetzbar - jedoch als IT-Dienstleister für die Auftragsbearbeitung notwendig. IT-Service und Lösungen...*

1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten 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. Die Zugriffskontrolle kann unter anderem gewährleistet werden durch geeignete Berechtigungskonzepte, die eine differenzierte Steuerung des Zugriffs auf Daten ermöglichen. Dabei gilt, sowohl eine Differenzierung auf den Inhalt der Daten vorzunehmen als auch auf die möglichen Zugriffsfunktionen auf die Daten. Weiterhin sind geeignete Kontrollmechanismen und Verantwortlichkeiten zu definieren, um die Vergabe und den Entzug der Berechtigungen zu dokumentieren und auf einem aktuellen Stand zu halten (z.B. bei Einstellung, Wechsel des Arbeitsplatzes, Beendigung des Arbeitsverhältnisses). Besondere Aufmerksamkeit ist immer auch auf die Rolle und Möglichkeiten der Administratoren zu richten.

Technische Maßnahmen	
› Aktenschredder	✓
› Externe Aktenvernichtung (DIN 66399)	✓
› Externe Datenvernichtung mit Zertifikatsnachweis	✓
› Physische Löschung von Datenträgern	✓
› Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	✓

Organisatorische Maßnahmen	
› Einsatz Berechtigungs- und Benutzerkonzept	✓
› Minimale Anzahl an Administratoren	✓
› Verwaltung Benutzerrechte durch Administratoren	✓
› Datenschutztresor (Daten und Zugänge)	✓
› Notfallprotokoll und Gebäuderichtlinien lt. Qualitätsmanagement	✓

1.4 Trennungskontrolle

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Dieses kann beispielsweise durch logische und physikalische Trennung der Daten gewährleistet werden.

Technische Maßnahmen	
› Trennung von Produktiv- und Testumgebung	✓
› Physikalische Trennung (Systeme /Datenbanken / Datenträger)	✓
› Mandanten - und Clientfähigkeit relevanter Anwendungen	✓

Organisatorische Maßnahmen	
› Steuerung über Berechtigungskonzept	✓
› Prüfung Benutzerkonten	✓
› Festlegung von Datenbankrechten	✓
› Datensätze sind mit Zweckattributen versehen	✓
› Sorgfaltsverpflichtung der Mitarbeiter	✓

1.5 Pseudonymisierung

Die Verarbeitung personenbezogener Daten 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 entsprechenden technichen und organisatorischen Maßnahmen unterliegen;

Technische Maßnahmen	
› Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt)	✓

Organisatorische Maßnahmen	
› Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren	✓

2. Integrität

2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

Technische Maßnahmen	
› Email-Verschlüsselung (TLS) bevorzugt	✓
› Einsatz von VPN, Firewall und SSL	✓
› Protokollierung der Zugriffe und Abrufe	✓
› Sichere Transportbehälter	✓
› Bereitstellung über verschlüsselte Verbindungen wie sftp, https	✓

Organisatorische Maßnahmen	
› Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen	✓
› Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen	✓
› Weitergabe in anonymisierter oder pseudonymisierter Form	✓
› Sorgfalt bei Auswahl von Transport-Personal	✓
› Persönliche Übergabe mit Protokoll	✓

2.2 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. Eingabekontrolle wird durch Protokollierungen erreicht, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) stattfinden können.

Technische Maßnahmen	
› Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	✓
› Manuelle oder automatisierte Kontrolle der Protokolle	✓

Organisatorische Maßnahmen	
› Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können	✓
› Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzer	✓
› Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	✓
› Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden	
› Klare Zuständigkeiten für Löschungen	✓

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Technische Maßnahmen	
› Feuer- und Rauchmeldeanlagen - Feuerlöscher	✓
› unterbrechungsfreie Stromversorgung	✓
› Serverraumüberwachung Temperatur und Feuchtigkeit	✓
› Serverraum klimatisiert	✓
› Schutzsteckdosenleisten Serverraum	✓
› Datenschutztresor mit Quelldichtung	✓
› RAID System / Festplattenspiegelung	✓
› Videoüberwachung Serverraum	✓
› Zugangskontrolle / Alarmmeldung	✓

Organisatorische Maßnahmen	
› Backup & Recovery-Konzept	✓
› Kontrolle des Sicherungsvorgangs	✓
› Regelmäßige Tests zur Datenwiederherherstellung und Protokollierung der Ergebnisse	✓
› Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums	✓
› Keine sanitären Anschlüsse im oder oberhalb des Serverraums	✓
› Getrennte Partitionen für Betriebssysteme und Daten	✓
› Existenz eines Notfallplans	✓

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Datenschutz-Maßnahmen

Maßnahmen, die gewährleisten, dass der Datenschutz eingehalten wird.

Technische Maßnahmen	
› Software-Lösungen für Datenschutz-Management im Einsatz	✓
› Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung	✓
› Sicherheitszertifizierung nach ISO 27001 in Vorbereitung - Sicherheitskonzept	✓
› Eine Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	✓

Organisatorische Maßnahmen	
› Interner QM-Mitarbeiter	✓
› externer Datenschutzbeauftragter Giovanni Blasi Phone: +49 711 3808877 Mobile: +49 170 22 26 351 Mail: Datenschutz@giovanni-blasi.com	✓
› Mitarbeiter Schulungen und auf Vertraulichkeit/ Datengeheimnis verpflichtet	✓
› Regelmäßige Sensibilisierung der Mitarbeiter	✓
› externer Informationssicherheitsbaauftragter (Kontakt siehe Datenschutzbeauftragter)	✓

4.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen.

Technische Maßnahmen	
› Einsatz Firewall / automatisierte Aktualisierung	✓
› Einsatz Spamfilter / automatisierte Aktualisierung	✓
› Einsatz Virenscanner / automatisierte Aktualisierung	✓

Organisatorische Maßnahmen	
› Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen	✓
› Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen	✓
› Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem	✓
› Formaler Prozess und Verantwortlichkeiten zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen	✓