Sicherheit der Verarbeitung nach Art. 32 DSGVO

CIRCLE2 GmbH
Sumpfweg 6

72070 Tübingen

Datenschutz-Organisation

Datenschutzberatung:	format8 GmbH
Adresse:	Handwerkerpark 3 72070 Tübingen
Telefon:	+49 (0) 7071 138870
Email:	kontakt@format8.de

Einleitung

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen trifft die CIRCLE2 GmbH geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

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

▪ Pseudonymisierung

Es werden folgende Maßnahmen eingesetzt:

- getrennte Speicherung von Zusatzinformationen zur Identifikation,
- Verwendung von (Personal-, Kunden- oder Teilnehmer-) Kennziffern statt Namen,
- Verschlüsselung von Zusatzinformationen zur Identifikation,
- Verwaltung und Dokumentation von differenzierten Berechtigungen auf die Zusatzinformationen zur Identifikation,
- Kopierschutz hinsichtlich Zusatzinformationen zur Identifikation,
- Vier-Augen-Prinzip für Identifikation,
- Anwenderkennwörter werden als Hashwert gespeichert,
- Personenbezogene Daten für die Auswertung zu statistischen Zwecken werden pseudonymisiert, bevor diese in einem Report bereitgestellt werden.

▪ Verschlüsselung

Es werden folgende Maßnahmen eingesetzt:

- Verschlüsselung von mobilen Endgeräten wie Laptops, Tablets, Smartphones,
- Verschlüsselung von mobilen Speichermedien (CD/DVD- ROM, USB-Stick, externen Festplatten),
- Verschlüsselung von Systemen/Anlagen und Dateien,
- Verschlüsselte Aufbewahrung von Passwörtern,
- E-Mail-Anhänge werden bei Bedarf verschlüsselt, die Passwörter werden auf gesondertem Weg mitgeteilt
- Gesichertes WLAN,
- Einsatz von Hypertext Transfer Protocol Secure-zertifikat (https) für Internetportal,
- Zusätzliche Verschlüsselung mittels Secure Socket Layer (SSL)/ Transport Layer Security (TLS),
- Es wird für SSL/TSL wenigstens eine 256-bit Verschlüsselung eingesetzt.

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

▪ Zutrittskontrolle

Es werden folgende Maßnahmen bei den Büros eingesetzt:

- Der Zutritt zum Gebäude und definierten Büroräumen ist über ein mechanisches Schlosssystem gesichert.
- Die Türen sind außer zum Betreten und Verlassen stets geschlossen und außerhalb der Geschäftszeiten fest abgesperrt.
- Es existieren keine Nebenzutrittsmöglichkeiten zu den Büroräumen
- Fenster sind außerhalb der Geschäftszeiten stets geschlossen
- Es existieren keine eigenen Server. Die Datenhaltung ist in das Rechenzentrum der Firma
  Hetzner Online GmbH
  Industriestr. 25, 91710 Gunzenhausen
  ausgelagert
- Der Zutritt für betriebsfremde Personen ist eingeschränkt.
- Zutrittsberechtigungen werden nur an Berechtigte ausgegeben und sofort eingezogen, wenn die Zugangsberechtigung erlischt.
- Beim Verlust eines Zutrittsmittels oder bei nicht erfolgter Rückgabe werden die betreffenden Schlösser getauscht.

▪ Zugangskontrolle

Die Zugangskontrolle zu DV-Systemen stellt sich wie folgt dar:

- PCs, Laptops der Fa. CIRCLE2 unterliegen ihrem Einflussbereich,
- Persönlicher und individueller User-Log-In bei Anmeldung am System bzw. Netzwerk,
- Autorisierungsprozess für Zugangsberechtigungen,
- Begrenzung der befugten Benutzer,
- Zwei-Faktor-Authentifizierung bei kritischen Systemen,
- Kennwortverfahren,
  (Vorgabe von Kennwortparametern hinsichtlich Komplexität und Aktualisierungsintervall),
- Elektronische Dokumentation von Passwörtern und Schutz dieser Dokumentation vor unbefugtem Zugriff,
- Automatische Sperrung der Clients nach gewissem Zeitablauf ohne Useraktivität
  (auch passwortgeschützter Bildschirmschoner oder automatische Pausenschaltung),
- Einsatz linux-basierter Hardwarefirewall,

- Bestimmungsgemäße Zugriffe von außen werden durch Virtual Private Network (VPN) abgesichert.

▪ Zugriffskontrolle

Berechtigungen innerhalb der DV-Systeme werden Richtlinien geregelt. Hierbei werden Standarduser definiert und gemäß den betrieblichen Erfordernissen für die Mitarbeiter verwendet. Die Vergabe von Sonderrechten erfolgt nur durch die Geschäftsleitung.

Darüber hinaus stellt sich die Zugriffskontrolle wie folgt dar:

- Es existieren Berechtigungskonzepte
- Die Zugriffsrechte werden differenziert vergeben:
    - Nach Dateien
    - Nach Anwendungsprogrammen und
    - Nach Betriebssystem
- Die Verarbeitungsberechtigungen werden differenziert vergeben nach
    - Leseberechtigungen
    - Änderungsberechtigungen
    - Löschberechtigungen
- Dokumente werden datenschutzgerecht mittels Schredder P4 vernichtet.

▪ Trennungskontrolle

Es werden folgende Maßnahmen eingesetzt:

- Trennung von Testdaten bei Softwareentwicklung und Echtdaten (wenn erforderlich)

3. Integrität, Weitergabekontrolle, Auftragskontrolle und Fernwartung (Art. 32 Abs. 1 lit. b DS-GVO)

▪ Weitergabekontrolle

Es werden folgende Maßnahmen eingesetzt:

- Die zur Datenverarbeitung eingesetzten Ausgabegeräte sind so angeordnet, dass unbefugte Dritte keinen Einblick nehmen bzw. Zugriff erhalten können,
- Sichtschutzfolien für mobile Datenverarbeitungssysteme, wenn der Einblick durch Dritte verhindert werden soll,
- Der E-Mail-Server unterstützt TLS,

- Protokollierung von Datenübertragung oder Datentransport,
- erfolgt eine Empfängerkontrolle vor Versand

▪ Eingabekontrolle und Protokollierung

Es werden folgende Maßnahmen eingesetzt:

- Über Zugriffsrechte geregelte Eingabekontrolle,
- Es werden Standard-Protokolle der IT-Systeme verwendet,
- Dokumenten Management System (DMS) mit Änderungshistorie,
- Sicherheits-/Protokollierungssoftware,
- Protokollierung von lesenden Zugriffen,
- Protokollierung des Kopierens, Veränderns oder Entfernens von Daten.

▪ Auftragskontrolle

Es werden folgende Maßnahmen eingesetzt:

- Dienstleister werden sorgfältig und nach Datenschutzgesichtspunkten ausgewählt,
- Weisungen werden protokolliert,
- Im Rahmen von Auftragsverarbeitung eingesetzte Dienstleister werden gemäß den Anforderungen der DSGVO vertraglich gebunden.

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

▪ Verfügbarkeitskontrolle und Zuverlässigkeit

Es werden folgende Maßnahmen eingesetzt:

- Hier greift hauptsächlich die Sicherheit des nach DIN 27001 zertifizierten Rechenzentrums,
- Gewährleistung der Datenspeicherung im gesicherten Netzwerk,
- Regelmäßige Aktualisierung der verwendeten Betriebssysteme und Software,
- Server, Desktops, Notebooks etc. werden mittels eines Virenscanners ständig überwacht,
- Einsatz von Spamfiltern,
- Ausreichende Kapazität von IT-Systeme und Anlagen,
- Resilienz und Fehler-Management,
- Dedizierte Notfallpläne existieren.

▪ Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Es werden folgende Maßnahmen eingesetzt:

- Sicherheitskonzept für Software- und IT-Anwendungen,
- Regelmäßige Datensicherung,
- Redundante, örtlich getrennte Datenaufbewahrung (Offsite Storage),
- Administrator-Passwörter werden sicher verwahrt.

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

▪ Datenschutz-Management

Die CIRCLE2 GmbH betreibt ein beschriebenes und organisiertes Datenschutz-Management-System

- Es ist ein externer Datenschutzbeauftragter dauerhaft bestellt,
- Die vorhandenen Dokumentationen der Datensicherheit und des Datenschutzes werden regelmäßig geprüft und ggf. aktualisiert,
- Es erfolgen interne Audits durch den externen DSB,
- Alle Mitarbeiter sind auf die Vertraulichkeit verpflichtet,
- Es finden regelmäßige Datenschutzschulungen statt,
- Es ist ein wirksamer P-D-C-A Zyklus etabliert.

▪ Umgang mit Betroffenenrechten und Datenschutzvorfällen

Folgende Maßnahmen wurden umgesetzt und werden regelmäßig überprüft:

- Zum Umgang mit Betroffenenrechten und der Behandlung von Datenschutzvorfällen sind Richtlinien und Prozesse formuliert und umgesetzt,
- Die Mitarbeiter sind informiert und geschult,
- Es existieren Richtlinien/Vorgaben zur Gewährleistung von technischen & organisatorischen Msaßnahmen zur Sicherheit der Verarbeitung.