Sicherheit der Verarbeitung nach Art. 32 DSGVO

bei

CETOS Services AG
Econopark Pankstraße
Pankstraße 8, Haus Q
13127 Berlin

Datenschutz-Organisation

Datenschutzbeauftragter:	harrand consulting gmbh
Ansprechpartner zum Datenschutz:	Sebastian Harrand
Stellv. Ansprechpartner zum Datenschutz:	Lars-Holger Krause
Adresse:	Karl-Liebknecht-Str. 28b 16348 Wandlitz
Telefon:	+49 30 92 10 80 24 100
E-Mail:	datenschutz@cetos.com

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 treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Mitarbeiterverpflichtung -schulung zum Datenschutz (Artt. 5 Abs. 1 lit. f. und 28 Abs.3 lit. b DSGVO)

- **Zutrittskontrolle**

Maßnahmen, die unbefugten Personen den Zutritt zu IT-Systemen und Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, sowie zu vertraulichen Akten und Datenträgern physisch verwehren:

Beschreibung des Zutrittskontrollsystems:
- kontrollierte Schlüsselvergabe
- Türsicherung

- **Zugangskontrolle**

Maßnahmen, die verhindern, dass Unbefugte datenschutzrechtlich geschützte Daten verarbeiten oder nutzen können.
Beschreibung des Zugangskontrollsystems:

- Kennwortverfahren, d.h. persönlicher und individueller User Log-In bei Anmeldung am System (u.a. Sonderzeichen, Mindestlänge, regelmäßiger Wechsel des Kennwortes)
- Einrichtung eines Benutzerstammsatzes pro User
- Begrenzung der Zahl der berechtigten Mitarbeiter
- Abkapselung von sensiblen Systemen durch getrennte Netzbereiche
- Authentifizierungsverfahren
- Protokollierung der Anmeldeversuche und Abbruch des Anmeldevorgangs nach festgelegter Zahl von erfolgloser Zahl von Versuchen
- Einrichten von regelmäßigen aktualisierten Antiviren- und Spywarefiltern
- Firewall

- **Zugriffskontrolle**

Maßnahmen, die gewährleisten, dass die zur Benutzung der Datenverarbeitungsverfahren Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können, so dass Daten bei der Verarbeitung, Nutzung und Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Beschreibung des Zugriffskontrollsystems:

- Berechtigungskonzepte (Profile, Rollen, etc.) und deren Dokumentation
- Auswertung/Protokollierungen
- Archivierungskonzept
- Protokollierung von Zugriffen und Missbrauchsversuchen

- **Trennungskontrolle**

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden und so von anderen Daten und Systemen getrennt sind, dass eine ungeplante Verwendung dieser Daten zu anderen Zwecken ausgeschlossen ist.

Beschreibung des Trennungskontrollvorgangs:

- Berechtigungskonzepte
- Softwareseitige Kundentrennung
- Trennung von Test- und Produktivsystemen

- **Pseudonymisierung**

Maßnahmen, die den unmittelbaren Personenbezug während der Verarbeitung in einer Weise reduzieren, dass nur mit Hinzuziehung zusätzlicher Informationen eine Zuordnung zu einer spezifischen betroffenen Person möglich ist. Die Zusatzinformationen sind dabei durch geeignete technische und organisatorische Maßnahmen von dem Pseudonym getrennt aufzubewahren.

Beschreibung der Pseudonymisierung:

- Kürzung von Datensätzen um identifizierte Merkmale (z.B. Entfernen von IP-Adressen)
- Löschung von identifizierenden Merkmalen vor Übermittlung
- Ausschluss der (Re-)Identifizierung von Merkmalen durch Berechtigungen
- Trennung von Produktiv- und Testsystemen
- Logische Mandantentrennung (softwareseitig)
- Erstellung eines Berechtigungskonzepts zwecks Mandantentrennung
- Versehen der Datensätze mit Zweckattributen/Datenfeldern

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Maßnahmen, die gewährleisten, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden:

Beschreibung der Datenintegrität:

- Einspielen neuer Releases und Patches mit Release-/Patchmanagement
- Funktionstest bei Installation und Releases/Patches durch IT-Abteilung
- Logging

- **Weitergabekontrolle**

Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport, z.B.: Verschlüsselung (SSL, TSL), Virtual Private Networks (VPN), elektronische Signatur.

Beschreibung der Weitergabekontrolle:

- Einrichtung von VPN-Tunneln
- Verschlüsselung von Anhängen
- Dokumentation der Empfänger von Daten und der Zeitspannender geplanten Überlassung bzw. vereinbarter Löschfristen
  - Wird gemäß den Regelungen in den Auftragsverarbeitungsvereinbarungen (AVV) nach Art. 28 DSGVO behandelt.
- Weitergabe von Daten in anonymisierter oder pseudonymisierter Form

- **Eingabekontrolle**

Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind, z.B.: Protokollierung, Dokumentenmanagement.

- Protokollierung der Eingabe und Änderungen
- Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

- **Verfügbarkeitskontrolle**

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

Beschreibung des Verfügbarkeitskontrollsystems:

- Internes und externes Datensicherungsverfahren
- Spiegeln von Festplatten
- Unterbrechungsfreie Stromversorgung (USV)
- Klimaanlage in Serverräumen
- Notfallpläne
- Feuerlöscher
- keine wasserführenden Leitungen über oder neben Serverräumen

- Softwareüberwachung auf den Servern mit Alarmmeldungssystem
- Schutzsteckdosenleisten

- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)**

Maßnahmen, die die Fähigkeit sicherstellen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

Beschreibung der Maßnahmen zur raschen Widerherstellbarkeit:

- Datensicherungsverfahren
- regelmäßige Tests der Datenwiederherstellung
- Notfallpläne

- **Zuverlässigkeit**

Maßnahmen, die gewährleisten, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden:

Beschreibung der Maßnahmen zur Zuverlässigkeit:

- Automatisches Monitoring mit E-Mail-Benachrichtigung
- Notfallpläne mit Verantwortlichkeiten
- IT-Notdienst 24/7
- regelmäßige Tests der Datenwiederherstellung

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

- **Datenschutz-Management**

CETOS Services AG betreibt ein beschriebenes und organisiertes Datenschutz Management System. Dieses Datenschutz-Management-System berücksichtigt den kontinuierlichen Verbesserungsprozess in Anlehnung an die „High-Level-Structure“ der ISO-Normen.

- **Incident-Response-Management**

Zum Umgang und der Behandlung von Datenschutzvorfällen hat CETOS Services AG Richtlinien formuliert und umgesetzt. Die Mitarbeiter von CETOS Services AG sind informiert und geschult.

- **Auftragskontrolle**

Keine Auftragsdatenverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers, z.B.: Eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

- Auswahl des Auftragsnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)