**Chancental Works GmbH**
Zinggenstrasse 15
CH-9434 Au/SG
Schweiz

# Technische und organisatorische Massnahmen (TOM) i.S.d. Art. 32 DSGVO

## Inhaltsverzeichnis

# 1 Vorbemerkung

Alle personenbezogenen Daten der Chancental Works GmbH werden ausschliesslich in Fremdrechenzentren gespeichert und verarbeitet.

Die nachfolgenden Ausführungen beziehen sich auf die genutzten Systemumgebungen.

Die Chancental Works GmbH verfügt über keinen eigenen Serverraum.

Drittpersonen oder auch Personal der Chancental Works GmbH haben zu der genutzten Infrastruktur keinen Zutritt.

# 2 Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

## 2.1 Zutrittskontrolle

Massnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

| **Technische Massnahmen** | **Organisatorische Massnahmen** |
|---|---|
| ☒ Alarmanlage | ☒Schlüsselregelung / Liste |
| ☒ Automatisches Zugangskontrollsystem | ☒ Empfang / Rezeption / Pförtner |
| ☒ Biometrische Zugangssperren | ☒ Besucherbuch / Protokoll der Besucher |
| ☒ Chipkarten / Transpondersysteme | ☒ Mitarbeiter- / Besucherausweise |
| ☒ Manuelles Schliesssystem | ☒ Besucher in Begleitung durch Mitarbeiter |
| ☒ Türen mit Knauf Aussenseite | ☒ Sorgfalt bei Auswahl des Wachpersonals |
| ☒Klingelanlage mit Kamera | ☒ Sorgfalt bei Auswahl Reinigungsdienste |
| ☒ Videoüberwachung der Eingänge | |

## 2.2 Zugangskontrolle

Massnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

| **Technische Massnahmen** | **Organisatorische Massnahmen** |
|---|---|
| ☒ Login mit Benutzername + Starkes Passwort | ☒ Verwalten von Benutzerberechtigungen |
| ☒ Anti-Viren-Software Server | ☒ Erstellen von Benutzerprofilen |
| ☒ Anti-Virus-Software Clients | ☒ Zentrale Passwortvergabe |
| ☒ Anti-Virus-Software mobile Geräte | ☒ Richtlinie „Sicheres Passwort“ |
| ☒ Firewall | ☒ Richtlinie „Löschen / Vernichten“ |
| ☒ Intrusion Detection Systeme | ☒ Richtlinie „Clean desk“ |
| ☒ Einsatz VPN bei Remote-Zugriffen | ☒ Allg. Richtlinie Datenschutz und / oder Sicherheit |
| ☒ Verschlüsselung von Datenträgern | |
| ☒ Verschlüsselung Smartphones | |
| ☒ Automatische Desktopsperre | |
| ☒ Verschlüsselung von Notebooks / Tablet | |
| ☒ Intrusion Prävention Systeme | |
| ☒ Zwei-Faktor-Authentifizierung im RZ-Betrieb und bei kritischen Systemen | |

## 2.3 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.

| **Technische Massnahmen** | **Organisatorische Massnahmen** |
|---|---|
| ☒ Aktenschredder (mind. Stufe 3, cross cut) | ☒ Einsatz Berechtigungskonzepte |
| ☒ Physische Löschung von Datenträgern Sicherheitsstufe H-4 (DIN 66399) | ☒ Minimale Anzahl an Administratoren |
| ☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten | ☒ Verwaltung Benutzerrechte durch Administratoren |
| ☒ Zugriffe auf Systeme mittels SSH | ☒ Anwendung kryptografischer Verfahren nach aktuellem Stand der Technik |
| ☒ TLS-Verschlüsselung | |

## 2.4 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** | **Organisatorische Massnahmen** |
|---|---|
| ☒ Trennung von Produktiv- und Test-umgebung | ☒ Steuerung über Berechtigungskonzept |
| ☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger) | ☒ Festlegung von Datenbankrechten |
| ☒ Mandantenfähigkeit relevanter Anwendungen | ☒ Definierte Anforderungen für Entwicklungsumgebungen |
| ☒ VLAN-Segmentierung von Netzwerken | |
| ☒ Kundensysteme logisch getrennt | |
| ☒ Staging von Entwicklungs-, Test und Produktivumgebung | |

## 2.5 Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

| Technische Massnahmen | Organisatorische Massnahmen |
|---|---|
| ☒ Im Falle der Pseudonymisierung: Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System (mögl. verschlüsselt) | ☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren |

# 3 Integrität (Art. 32 Abs. 1 lit. b DSGVO)

## 3.1 Weitergabekontrolle

Massnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder bzw. Eingabe 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 | Organisatorische Massnahmen |
|---|---|
| ☒ Email-Verschlüsselung | ☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen |
| ☒ Einsatz von VPN | ☒ Übersicht regelmässiger Abruf- und Übermittlungsvorgängen |
| ☒ Protokollierung der Zugriffe und Abrufe | ☒ Umsetzung des Need-to-know Prinzips |
| ☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https<br>– Secure Cloudstores | |

## 3.2 Eingabekontrolle

Massnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder bzw. Eingabe 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** | **Organisatorische Massnahmen** |
|---|---|
| ☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten | ☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können |
| ☒ Manuelle oder automatisierte Kontrolle der Protokolle | ☒ Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch Individuelle Benutzernamen (nicht Benutzergruppen) |
| | ☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts |
| | ☒ Klare Zuständigkeiten für Löschungen |

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

## 4.1 Verfügbarkeitskontrolle

Massnahmen, die gewährleisten, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (USV, Klimaanlagen, Brandschutz, Datensicherungen, sichere Aufbewahrung von Datenträgern, Virenschutz, Raidsysteme, Plattenspiegelungen etc.).

| **Technische Massnahmen** | **Organisatorische Massnahmen** |
|---|---|
| ☒ Feuer- und Rauchmeldeanlagen | ☒ Backup & Recovery-Konzept (ausformuliert) |
| ☒ Feuerlöscher Serverraum | ☒ Kontrolle des Sicherungsvorgangs |
| ☒ Serverraumüberwachung Temperatur und Feuchtigkeit | ☒ Regelmässige Tests zur Datenwiederher-Herstellung und Protokollierung der Ergebnisse |
| ☒ Serverraum klimatisiert | ☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort ausserhalb des Serverraums |
| ☒ USV-Anlage und Notstrom-Dieselaggregate RZ | ☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums |
| ☒ Schutzsteckdosenleisten Serverraum | ☒ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4) |
| | ☒ Regelmässige Tests der Dieselaggregate RZ |
| ☒ RAID System / Festplattenspiegelung | |
| ☒ Videoüberwachung Serverraum | |
| ☒ Alarmmeldung bei unberechtigtem Zutritt zu Serverraum | |
| ☒ Einsatz von Schutzprogrammen gegen Schadsoftware | |

## 4.2 Wiederherstellbarkeit

Massnahmen, die dazu befähigen, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen.

| **Technische Massnahmen** | **Organisatorische Massnahmen** |
|---|---|
| ☒ Backup-Monitoring und -Reporting | ☒ Recovery-Konzept |
| ☒ Wiederherstellbarkeit aus Automatisierungs-Tools | ☒ Kontrolle des Sicherungsvorgangs |
| ☒ Backup-Konzept nach Kritikalität und Kundenvorgaben | ☒ Regelmässige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse |
| | ☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort ausserhalb des Serverraums |

# 5 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

## 5.1 Datenschutz-Management

| Technische Massnahmen | Organisatorische Massnahmen |
|---|---|
| ☒ Zentrale Dokumentation aller Regelungen zum Datenschutz mit technischer Zugriffsmöglichkeit für Mitarbeiter | ☒ Datenschutzmanagementsystem implementiert |
| ☒ Eine Überprüfung der Wirksamkeit der Technischen Schutzmassnahmen wird jährlich durchgeführt | ☒ Informationssicherheitsmanagement implementiert |
| ☒ Sicherheitszertifizierung nach ISO 27001 | ☒ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt |
| ☒ Datenschutzmanagementsystem nach ISO 27701 | ☒ Die Organisation kommt den Informations- pflichten nach Art. 13 und 14 DSGVO nach |
| ☒ Eine Überprüfung der Wirksamkeit der Technischen Schutzmassnahmen wird jährlich durchgeführt | |

## 5.2 Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen sowie Data Breach-Prozess.

| Technische Massnahmen | Organisatorische Massnahmen |
|---|---|
| ☒ Einsatz von Firewall und regelmässige Aktualisierung | ☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheits- und Datenschutzvorfällen |
| ☒ Einsatz von Spamfilter und regelmässige Aktualisierung | ☒ Dokumentation von Sicherheitsvorfällen und Datenpannen via Ticketsystem |
| ☒ Einsatz von Virenscanner und regelmässige Aktualisierung | |
| ☒ Intrusion Detection System (IDS) | |
| ☒ Intrusion Prevention System (IPS) | |

## 5.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

"Privacy by design" / "Privacy by default" gem. Art 25 Abs 2 DSGVO

| Technische Massnahmen | Organisatorische Massnahmen |
|---|---|
| ☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind | |
| ☒ Berücksichtigung der Grundsätze "Datenschutz durch Technikgestaltung" ("Data Protection by Design") und "Datenschutz durch datenschutzfreundliche Voreinstellungen" ("Data Protection by Default") bei der Softwareentwicklung | |

## 5.4 Auftragskontrolle (Outsourcing, Subauftragnehmer und Auftragsverarbeitung)

Massnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

| **Technische Massnahmen** | **Organisatorische Massnahmen** |
|---|---|
| ☒ Überwachung von Remote-Zugriffen Externer z. B. im Rahmen von Remote-Support | ☒ Lieferantenbewertungen werden risikobasiert durchgeführt |
| ☒ Überwachung von Subunternehmern nach den Prinzipien und mit den Technologien gem. vorausgehenden Kapiteln | ☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmassnahmen und deren Dokumentation |
| | ☒ Auswahl des Auftragnehmers auf Basis definierter Kriterien |
| | ☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung |
| | ☒ Regelmässige Überprüfung des Auftragnehmers und seines Schutzniveaus |

# 6 Technische und organisatorische Massnahmen Infrastruktur bereitstellender Subunternehmer

Als Subunternehmer im betrieblichen und betriebswirtschaftlichen Sinn werden von der Chancental Works GmbH Rechenzentrumsdienstleister in Anspruch genommen.

Es handelt sich hierbei nicht um "weitere Auftragsverarbeiter" gem. DSGVO, da deren Kerntätigkeit zu keinem Zeitpunkt in der Verarbeitung personenbezogener Daten liegt, sondern um eine sogenannte untergeordnete Nebenleistung in Form von Infrastrukturbereitstellung.

Aufgrund der informationssicherheitstechnischen Relevanz für den AN sowie für den AG - vor allem betreffend die Verfügbarkeit - werden vom AN für diese Nebentätigkeiten ausschliesslich sorgfältig ausgewählte Betriebe eingesetzt und regelmässig überprüft.