Anhang 1
Technisch und organisatorische Massnahmen

Auftragnehmer: **zurichnetgroup ag**
Gwattstrasse 15
8808 Pfäffikon SZ

(nachfolgend «Auftragnehmer» genannt)

Version: 1.0

Datum: August 2023

1 Beschreibung der vereinbarten technischen und organisatorischen Massnahmen

1.1 Technisch organisatorische Massnahmen - zurichnetgroup AG i.S.d. Art. 7 nDSG

Unternehmen, die selbst oder als Dienstleister (nach Art. 9 nDSG) personenbezogene Daten verarbeiten oder Zugriff darauf haben, müssen technische und organisatorische Massnahmen treffen und umsetzen, welche die Einhaltung der Datenschutzgrundsätze, sowie die Sicherheit der Bearbeitung (z.B. nach BSI-Richtlinie) personenbezogener Daten gewährleisten.

1.2 Hinweis

Art. 32 DS-GVO / Art. 7 und Art. 8 revDSG: Sicherheit der Verarbeitung (1) 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; diese Massnahmen schliessen gegebenenfalls unter anderem Folgendes ein: a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten; b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen; d) ein Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen zur Gewährleistung der Sicherheit der Verarbeitung. (2) Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - ob unbeabsichtigt oder unrechtmässig - Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden. (3) Die Einhaltung genehmigter Verhaltensregeln gemäss Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäss Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen. (4) Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

2 TOM - Technisch organisatorische Maßnahmen

2.1 Zutrittskontrolle - Technische Massnahmen

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

- Absicherung der Gebäudeschächte
- Chipkarten / Transpondersysteme
- Klingelanlage
- Klingelanlage mit Kamera
- Sicherheitsschlösser
- Videoüberwachung

2.2 Zutrittskontrolle - Organisatorische Massnahmen

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

- Ansprache unbekannter Personen
- Besucher sind immer in Begleitung von Mitarbeitern
- Schlüsselregelung / Liste
- Sorgfalt bei Auswahl des Wachpersonals / Reinigungspersonal

2.3 Zugangskontrolle - Technische Massnahmen

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

- Anti-Virus-Software für Clients und Server
- Automatische Sperre des Systems
- Einsatz von VPN-Technologien
- Einsatz von Firewallsystemen
- Mobile Device Management
- Verschlüsselung von Datenträgern
- Verschlüsselung von Notebooks
- Login mit Benutzername + Passwort

2.4 Zugangskontrolle - Organisatorische Massnahmen

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

- Richtlinie „Sicheres Passwort“
- Verwalten von Benutzerberechtigungen
- Zentrale Passwortvergabe

2.5 Zugriffskontrolle - Technische Massnahmen

Technische Massnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und die personenbezogenen Daten bei der Verarbeitung nicht unbefugt verwendet werden können.

- Aktenschredder (cross cut)

- Externer Aktenvernichter (Dienstleister)
- Verschlüsselung von Datenträgern

2.6 Zugriffskontrolle - Organisatorische Massnahmen

Organisatorische Massnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschliesslich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und die personenbezogenen Daten bei der Verarbeitung nicht unbefugt verwendet werden können.

- Datenschutztresor bzw. sichere Aufbewahrung von Datenträgern
- Einsatz Berechtigungskonzepte
- Protokollierung der Vernichtung von Datenträgern
- Rechteverwaltung durch einen Systemadministrator

2.7 Weitergabekontrolle - Technische Massnahmen

Technische 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.

- Bereitstellung von Diensten über verschlüsselte Verbindungen wie sftp, https, etc.
- Einsatz von VPN
- E-Mail-Verschlüsselung
- Protokollierung der Zugriffe und Abrufe
- Nutzung von Signaturverfahren
- Sichere Transportbehälter

2.8 Eingabekontrolle - Technische Massnahmen

Technische Massnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Manuelle oder automatisierte Kontrolle der Protokolle

2.9 Eingabekontrolle - Organisatorische Massnahmen

Organisatorische Massnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Klare Zuständigkeit für Löschungen
- Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen

2.10 Auftragskontrolle - Technische Massnahmen

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

- Datenaustausch mit Auftragnehmer verschlüsselt

2.11 Auftragskontrolle - Organisatorische Massnahmen

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

- Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU-Standardvertragsklauseln
- Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (Datenschutz und Datensicherheit)
- Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus
- Verpflichtung der Mitarbeiter des Auftragnehmers auf Datengeheimnis

2.12 Verfügbarkeitskontrolle - Technische Massnahmen

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

- Alarmmeldung bei unberechtigtem Zutritt zum Serverraum
- RAID- System/ Festplattenspiegelung
- Serverraum klimatisiert
- Serverraumüberwachung Temperatur und Feuchtigkeit
- USV - Unterbrechungsfreie Stromversorgung
- Videoüberwachung Serverraum

2.13 Verfügbarkeitskontrolle - Organisatorische Massnahmen

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

- Aufbewahrung der Sicherungsmedien an einem sicheren Ort ausserhalb des Serverraums
- Backup & Recovery-Konzept (in schriftlicher Form vorhanden)
- Getrennte Partitionen für Betriebssysteme und Daten
- Keine sanitären Anschlüsse im oder oberhalb des Serverraums
- Kontrolle des Sicherungsvorgangs
- Regelmässige Tests zur Datenwiederherstellung und Protokollierung

2.14 Trennungsgebot - Technische Massnahmen

Technische Massnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testumgebung

2.15 Trennungsgebot - Organisatorische Massnahmen

Organisatorische Massnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Festlegung von Datenbankrechten
- Steuerung über Berechtigungskonzept

3 Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

3.1 Datenschutz-Management

Datenschutz-Management (Massnahmen, die gewährleisten, dass die innerbetriebliche Organisation so gestaltet wird, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.)

- Schriftliche Bestellung eines Datenschutzbeauftragten
- Regelmäßige Schulung der Mitarbeiter zum Datenschutz
- Ein Verzeichnis der Verarbeitungstätigkeiten ist vorhanden, vollständig und aktuell
- Es bestehen Standards für die IT-Sicherheit
- Ein Datenschutzkonzept ist vorhanden

3.2 Incident-Response-Management

Datenschutz-Management (Massnahmen, die gewährleisten, dass die innerbetriebliche Organisation so gestaltet wird, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.)

- Schulung der Mitarbeiter bzgl. Erkennen einer Datenpanne
- Es existiert ein internes Incident-Response-Management-Konzept
- Es gibt ein Konzept zur Meldung von Datenpannen an den Auftraggeber