Technische und organisatorische Massnahmen i.S.d § 9 BDSG und der DS-GVO i.V. EU-GVO

1. Zutrittskontrolle

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

☒	Alarmanlage	☒	Absicherung von Gebäudeschächten
☒	Automatisches Zugangskontrollsystem	☒	Chipkarten /Transponder-Schliesssystem
☒	Schliesssystem mit Codesperre	☒	Manuelles Schliesssystem
☒	Biometrische Zugangssperren	☒	Videoüberwachung der Zugänge
☒	Lichtschranken / Bewegungsmelder	☒	Sicherheitsschlösser
☒	Schlüsselregelung (Schlüsselausgabe etc.)	☒	Personenkontrolle beim Pförtner / Empfang im Büro
☒	Protokollierung der Besucher	☒	Sorgfältige Auswahl von Reinigungspersonal
☒	Sorgfältige Auswahl von Wachpersonal	☒	Tragepflicht von Berechtigungsausweisen

2. Zugangskontrolle

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

☒	Zuordnung von Benutzerrechten	☒	Erstellen von Benutzerprofilen
☒	Passwortvergabe	☒	Authentifikation mit biometrischen Verfahren
☒	Authentifikation mit Benutzername / Passwort	☒	Zuordnung von Benutzerprofilen zu IT-Systemen
☒	Gehäuseverriegelungen	☒	Einsatz von VPN-Technologie
☐	Sperren von externen Schnittstellen (USB etc.)	☒	Sicherheitsschlösser
☒	Schlüsselregelung (Schlüsselausgabe etc.)	☒	Personenkontrolle beim Pförtner / Empfang
☒	Protokollierung der Besucher	☒	Sorgfältige Auswahl von Reinigungspersonal
☒	Sorgfältige Auswahl von Wachpersonal	☒	Tragepflicht von Berechtigungsausweisen
☒	Einsatz von Intrusion-Detection-Systemen	☒	Verschlüsselung von mobilen Datenträgern
☐	Verschlüsselung von Smartphone-Inhalten	☐	Einsatz von zentraler Smartphone-Administrations-Software (z. B. zum externen Löschen von Daten)
☒	Einsatz von Anti-Viren-Software	☒	Verschlüsselung von Datenträgern in Laptops / Notebooks
☒	Einsatz einer Hardware-Firewall	☒	Einsatz einer Software-Firewall

3. Zugriffskontrolle

Massnahmen, die gewährleisten, dass die 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.

☒	Erstellen eines Berechtigungskonzept	☒	Verwaltung der Rechte durch Systemadministrator
☒	Anzahl der Administratoren auf das «Notwendigste» reduziert	☒	Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
☐	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	☒	Sichere Aufbewahrung von Datenträgern
☒	Physische Löschung von Datenträgern vor Wiederverwendung	☒	Ordnungsgemässe Vernichtung von Datenträgern (DIN 32757)
☒	Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel)	☒	Protokollierung der Vernichtung
☐	Verschlüsselung von Datenträgern		

4. Weitergabekontrolle

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

☒	Einrichtung von Standleitungen bzw. VPN-Tunneln	☐	Weitergabe von Daten in anonymisierter Form
☒	E-Mail-Verschlüsselung	☒	Erstellen einer Übersicht von regelmässigen Abruf- und Übermittlungsvorgängen
☒	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen	☒	Beim physischen Transport: sichere Transportbehälter/-verpackungen
☒	Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und Fahrzeugen		

5. Eingabekontrolle

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

☒	Protokollierung der Eingabe, Änderung und Löschung von Daten	☒	Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können
☒	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)	☐	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
☒	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts		

6. Auftragskontrolle

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

☒	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)	☒	Vorherige Prüfung der Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmassnahmen
☒	Schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG	☒	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG)
☒	Auftragnehmer hat Datenschutzbeauftragten bestellt	☒	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☒	Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart	☒	Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
☒	Vertragsstrafen bei Verstössen		

7. Verfügbarkeitskontrolle

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

☒	Unterbrechungsfreie Stromversorgung (USV)	☒	Klimaanlage in Serverräumen
☒	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	☒	Schutzsteckdosenleisten in Serverräumen
☒	Feuer- und Rauchmeldeanlagen	☒	Feuerlöschgeräte in Serverräumen
☒	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen	☒	Erstellen eines Backup- und Recoverykonzepts
☒	Testen von Datenwiederherstellung	☒	Erstellen eines Notfallplans
☒	Aufbewahrung von Datensicherungen an einem sicheren, ausgelagerten Ort	☒	Serverräume nicht unter sanitären Anlagen
☒	In Hochwassergebieten: Serverräume über der Wassergrenze		

8. Trennungsgebot

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

☒	Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern	☒	Logische Mandantentrennung (softwareseitig)
☒	Erstellung eines Berechtigungskonzepts	☒	Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden
☒	Versehen der Datensätze mit Zweckattributen / Datenfeldern	☐	Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System
☒	Festlegung von Datenbankrechten	☒	Trennung von Produktiv- und Testsystem

Die Geschäftsleitung

Hallwil, 01. September 2023