Technische und Organisatorische Massnahmen (TOM)

der Einzelfirma
HOFMANN IT-Advisor
Peter Hofmann
Hegistrasse 39c
8404 Winterthur

Inhalt

Einleitung

Die Einzelfirma hat den Fokus auf die Kundenberatung in belangen der IT-Umgebung, wie Unterstützung und Umsetzung bei der Anbindung und Integration von Softwarelösungen. Zudem erbringt sie Leistungen in den Bereichen Spezifizierung, Planung, Implementierung und Optimierung von IT-Systemen und Schnittstellen. Auf Wunsch werden Support- sowie Projektmanagementleistungen übernommen.

Die Firma hat, ausser dem o.g. Verantwortlichen keine Mitarbeiter und wird keine Aufträge an Subunternehmer vergeben.

Der Verantwortliche hat die nachfolgend benannten technischen und organisatorischen Ma ssnahmen getroffen, um die Vorgaben der jeweils geltenden Datenschutzgesetze, im Hinblick auf ein angemessenes Schutzniveau zu gewährleisten.

I. Vertraulichkeit

1.Zutrittskontrolle

Massnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.	
☐ Automatisches Zugangskontrollsystem	☐ Chipkarten-/Transponder-Schliesssystem
☐ Schliesssystem mit Codesperre	☒ Manuelles Schliesssystem
☐ Biometrische Zugangssperren	☐ Videoüberwachung der Zugänge
☐ Lichtschranken / Bewegungsmelder	☐ Sicherheitsschlösser
☐ Schlüsselregelung (Schlüsselausgabe mit Liste)	☐ Personenkontrolle beim Pförtner / Empfang
☐ Protokoll der Besucher (Besucherbuch)	☒ Sorgfältige Auswahl von Reinigungspersonal
☐ Sorgfältige Auswahl von Wachpersonal	☐ Mitarbeiter- und Besucherausweise
☐ Türen mit Knauf Aussenseite	☐ Klingelanlage mit Kamera
☒ Besucher nur in Begleitung	☐

2. Zugangskontrolle

Massnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme (Computer) von Unbefugten genutzt werden können.	
☐ Zuordnung und Verwaltung von Benutzerrechten	☒ Erstellung von Benutzerprofilen
☐ Passwortvergabe durch Admin	☐ Authentifizierung mit biometrischen Verfahren
☒ Authentifizierung mit Benutzername / Passwort	☐ Einsatz von VPN-Technologie
☐ Gehäuseverriegelungen	☒ Einsatz von Anti-Viren-Software
☒ Malwareschutz	☒ Einsatz einer Software-Firewall
☐ Sperren von externen Schnittstellen (USB etc.)	☒ Konzept „Clean Desk“
☐ Einsatz einer Hardware-Firewall	☒ Verschlüsselung von Notebooks / Tablets
☒ Passwortkonzept inkl. Manuelle Desktopsperre	☒ Verschlüsselung von Datenträgern
☐ Löschkonzept	☐ Verschlüsselung von Smartphones
☐ Einsatz von Intrustion-Detection-Systemen	☒ Datenverkehr nur über LAN-Kabel (WLAN-Modul deaktiviert)

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.	
☐ Erstellung eines Berechtigungskonzepts	☒ Verwaltung der Rechte durch Admin
☐ Einsatz eines Berechtigungskonzepts	☐ Minimale Anzahl an Administratoren
☐ Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	☒ Sichere Aufbewahrung von Datenträgern
☐ Physische Löschung von Datenträgern	☒ Vernichtung von Datenträgern

4.Trennungskontrolle

Massnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.	
☐ Physikalische Trennung (Systeme / Datenbaken / Datenträger)	☒ Logische Mandantentrennung (per Software)
☐ Einsatz 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

II. Integrität

1.Weitergabekontrolle

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.	
☐ Einrichtungen von VPN-Tunneln	☐ Weitergabe von Daten in anonymisierter oder pseudonymisierter 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 Transport: sichere Transportbehälter/-verpackungen/-fahrzeuge
☒ Verschlüsselte Verbindungen, z.B. https, SFTP	☐

2. Eingabekontrolle

Massnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.	
☐ Protokollierung der Eingabe, Änderung und Löschung von Daten	☐ Erstellung 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	☐ Kontrolle der Protokolle
☒ Löschkonzept mit Zuständigkeiten	☐

III. Verfügbarkeit und Belastbarkeit

Massnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind, sowie die gewährleisten, dass personenbezogene Daten rasch wiederhergestellt 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	☒ Erstellung eines Backup- & Recoverykonzepts
☒ Testen von Datenwiederherstellung	☐ Erstellung und Tests eines Notfallplans
☐ Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort	☐ Serverräume nicht unter sowie ohne sanitäre Anlagen
☒ Tägliche Spiegelung von Festplatten auf PC-internem Datenträger	☒ Wöchentliche Spiegelung von Festplatten auf PC-externem Datenträger
☐ Videoüberwachung Serverraum	☒ Software basierte Daten-Synchronisation

IV. Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung

1.Datenschutz-Management

Massnahmen, die die Einhaltung der Datenschutzvorgaben gewährleisten.	
☒ Obengenannte Person als Datenschutzbeauftragten, sofern entsprechende Pflicht besteht	☐ Regelmässige Schulung der Mitarbeiter zum Datenschutzrecht
☐ Meldung des internen oder externen Datenschutzbeauftragten bei der Aufsichtsbehörde	☒ Verpflichtung der Mitarbeiter auf das Datengeheimnis
☐ Prüfung der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung sowie Durchführung im Bedarfsfall	☐ Installation eines Prozesses zur Erfüllung der Informationspflichten

☐ Installation eines Prozesses zur Erfüllung der Auskunftspflicht	☒ Löschkonzept
☐ Installation eines Prozesses zur Erfüllung der Pflichten	☐ Installation eines Prozesses zur Bearbeitung von Widersprüchen
☐ Zentrale Dokumentation aller Verfahrensanweisungen zum Datenschutz nebst Zugriffsmöglichkeiten für die Mitarbeiter	☐ Erstellung eines IT-Sicherheitskonzeptes
☒ Regelmässige Überprüfung der Wirksamkeit der getroffenen TOMs	☐

2. Incident-Response-Management

Massnahmen, die für den Fall bzw. im Falle einer Datenschutzverletzung zu ergreifen sind.	
☐ Dokumentation eines Prozesses zur Erkennung und (rechtzeitigen) Meldung von Datenschutzverletzungen inkl. Festlegung von Zuständigkeiten und Erstellung von Musterformularen (Meldung bei der Aufsichtsbehörde und/oder beim Betroffenen)	☐ Einschaltung des Datenschutzbeauftragten
☐ Regelmässige Durchführung von Testsituationen einer Datenschutzverletzung	☐ Nachbearbeitung von Datenschutzverletzungen

3. Datenschutzfreundliche Voreinstellungen

Massnahmen, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.	
☐ Vorhaltung nur objektiv erforderlicher Checkboxen	☒ Keine Vorhaltung vorausgefüllter Checkboxen
☒ Beachtung des Standorts von Softwareanbietern	☐

4. 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 und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmassnahmen
☐ Dokumentierte Weisungen an den Auftragnehmer	☐ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
☐ Auftragnehmer hat Datenschutzbeauftragten bestellt, sofern entsprechende Pflicht besteht	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
☐ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer	☐ Laufende Überprüfung des Auftragnehmers, seiner Tätigkeiten und seines Schutzniveaus
☐ Vertragsstrafen bei Verstössen	☒ Abschluss eines Auftragsverarbeitungsvertrages
☐ Vereinbarung zur Verwendung von Subunternehmern	☐