IT-world
Ihr Full-Service IT Partner

+43 1 32 100 64
office@it-world.eu
www.it-world.eu

Anhang

Beschreibung der technisch-organisatorischen Maßnahmen (TOMs)

Standort:

Büro (1)

IT-world ITW GmbH
Levasseurgasse 3
1230 Wien

RZ NDC2 (2)

Karmarschgasse 23-25
1100 Wien

1. Vertraulichkeit

Unser Unternehmen befindet sich in einem besonderen Vertrauensverhältnis zu unseren Kunden und gehen wir daher mit allen erlangten Informationen verantwortungsbewusst um und wahren die Verschwiegenheit.

a. Zutrittskontrolle

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

Ja	Alarmanlage	NA	Absicherung von Gebäudeschächten
Ja[2]	Automatisches Zugangskontrollsystem	NA	Chipkarten-/Transponder-Schließsystem
NA	Schließsystem mit Codesperre	Ja[1]	Manuelles Schließsystem
NA	Biometrische Zugangssperren	Ja	Videoüberwachung der Zugänge
Ja[1]	Lichtschranken / Bewegungsmelder	Ja	Sicherheitsschlösser
Ja	Schlüsselregelung (Schlüsselausgabe etc.)	Ja[1]	Personenkontrolle beim Pförtner / Empfang
Ja[2]	Protokollierung der Besucher	Ja	Sorgfältige Auswahl von Reinigungspersonal
NA	Sorgfältige Auswahl von Wachpersonal	NA	Tragepflicht von Berechtigungsausweisen
Ja	Verschlossene Türen bei Abwesenheit	NA	Fenstersicherung (Erdgeschoss)

+43 1 32 100 64
office@it-world.eu
www.it-world.eu

b. Zugangskontrolle

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

Ja	Zuordnung von Benutzerrechten	Ja	Erstellen von Benutzerprofilen
Ja	Passwortvergabe	Ja[2]	Authentifikation mit biometrischen Verfahren
Ja	Authentifikation mit Benutzername / Passwort	Ja	Zuordnung von Benutzerprofilen zu IT-Systemen
Ja	Gehäuseverriegelungen	Ja	Richtlinien für Passwörter/Löschen/Clean-desk
Ja*	Sperren von externen Schnittstellen (USB etc.)	Ja	Sicherheitsschlösser
Ja	Schlüsselregelung (Schlüsselausgabe etc.)	Ja[1]	Personenkontrolle beim Pförtner / Empfang
Ja[2]	Protokollierung der Besucher	Ja[2]	Sorgfältige Auswahl von Reinigungspersonal
NA	Sorgfältige Auswahl von Wachpersonal	Ja[1]	Dienstwaffen
Ja	Einsatz von Intrustion-Detection-Systemen	Ja[1]	Verschlüsselung von mobilen Datenträgern
Ja	Verschlüsselung von Smartphone-Inhalten	Ja[1]	Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten)
Ja	Einsatz von Anti-Viren-Software	Ja	Verschlüsselung von Datenträgern in Laptops / Notebooks/USB
Ja	Einsatz einer Hardware-Firewall	Ja	Einsatz einer Software-Firewall

+43 1 32 100 64
office@it-world.eu
www.it-world.eu

c. 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.

Ja	Erstellen eines Berechtigungskonzepts	Ja	Verwaltung der Rechte durch Systemadministrator
Ja	Anzahl der Administratoren auf das „Notwendigste“ reduziert	Ja	Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel
Ja	Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten	Ja	Sichere Aufbewahrung von Datenträgern
Ja	physische Löschung von Datenträgern vor Wiederverwendung	Ja	ordnungsgemäße Vernichtung von Datenträgern
Ja[1]	Einsatz von Aktenvernichtern	Ja	Protokollierung der Vernichtung
Ja	Verschlüsselung von Datenträgern		

2. Integrität

a. 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.

Ja	Einrichtungen von Standleitungen bzw. VPN-Tunneln	Ja[1]	Weitergabe von Daten in anonymisierter oder pseudonymisierter Form; im Einzelfall
Ja	E-Mail-Verschlüsselung bzw. Nutzung von Signaturverfahren	NA	Erstellen einer Übersicht von regelmäßigen Abruf- und Übermittlungsvorgängen
NA	Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen	Ja[1]	Beim physischen Transport: sichere Transportbehälter/-verpackungen
Ja[1]	Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen	Ja	Verschlüsselung der übertragenen Daten

+43 1 32 100 64
office@it-world.eu
www.it-world.eu

b. 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.

Ja	Protokollierung der Eingabe, Änderung und Löschung von Daten	NA	Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können.
Ja	Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen)	NA	Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind
Ja	Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts	Ja_1	Klare Zuständigkeiten für Löschungen

c. Auftragskontrolle

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

Ja_1	Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten	Ja_1	vorherige Prüfung und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen (AV-Datenschutzkonzept)
Ja_1	schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsverarbeitungsvertrag)	Ja_1	Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis
NA	Auftragnehmer hat Datenschutzbeauftragten bestellt	Ja_1	Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
Ja_1	Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart	Ja_1	laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
NA	Vertragsstrafen bei Verstößen		

+43 1 32 100 64
office@it-world.eu
www.it-world.eu

3. Verfügbarkeitskontrolle

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

Ja	Unterbrechungsfreie Stromversorgung (USV)	Ja$_2$	Klimaanlage in Serverräumen
Ja	Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen	Ja	Schutzsteckdosenleisten in Serverräumen
Ja	Feuer- und Rauchmeldeanlagen	Ja	Feuerlöschgeräte in Serverräumen
Ja	Alarmmeldung bei unberechtigten Zutritten zu Serverräumen	Ja	Erstellen eines Backup- & Recoverykonzepts
Ja	Testen von Datenwiederherstellung	Ja	Erstellen eines Notfallplans
Ja	Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort	Ja	Serverräume nicht unter sanitären Anlagen
NA	In Hochwassergebieten: Serverräume über der Wassergrenze		

4. Trennungsgebot

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

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

5. Wiederherstellbarkeit

Siehe Backup-Strategie

+43 1 32 100 64
office@it-world.eu
www.it-world.eu

6. Datenschutz-Management

Maßnahmen, die für ein Datenschutz-Konzept bzw. DSMS zumindest notwendig sind.

NA	Software-Lösungen für Datenschutz-Management im Einsatz		
NA	Zentrale Dokumentation aller Verfahrens-weisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	Ja	Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
NA	Sicherheitszertifizierung nach ISO 27001, BSI IT-Grundschutz oder ISIS12	Ja	Regelmäßige Sensibilisierung der Mitarbeiter Mindestens jährlich
Ja	Anderweitiges dokumentiertes Sicherheits-Konzept	NA	interner / externer Informationssicherheits-Beauftragter Name / Firma Kontakt
Ja	Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	NA	Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
Ja	Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)	Ja	Die Organisation kommt den Informations-pflichten nach Art. 13 und 14 DSGVO nach
NA	Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen (Newsletter)	Ja	Formalisierter Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener ist vorhanden

Datum

Unterschrift des Verantwortlichen

+43 1 32 100 64
office@it-world.eu
www.it-world.eu

7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

a. Risikoanalyse

b. Datenschutzfreundliche Voreinstellungen

c. Ein Kontroll- und Verbesserungsprozess wird mindestens 1x jährlich durchgeführt

d. Weiterbildung: siehe Schulung

e. Auftragskontrolle: Datenschutzkonzept verlangen, keine Auftragsdatenverarbeitung im Sinne von Art 28 DSGVO ohne entsprechende Weisung des Auftraggebers, z.B.: eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Auftragsverarbeiters, sichere und verschlüsselte Speicherung und Übertragung, (z.B. DATB, Vorabüberzeugungspflicht, Nachkontrollen)

Jahr	Ergebnisse der Überprüfung, Bewertung und Evaluierung
2024	Keine Verbesserungen notwendig
2025	Keine Verbesserungen notwendig

Referenzen: Art 32 Z 1 DSGVO