© **FM Forum Business Solutions GmbH**
A-1200 Wien, Dresdner Straße 45
E-Mail: kundenservice@forum-media.at

Meldung eines Data Breach bei der DSB

A. Vertraulichkeit

Zutrittskontrolle: Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen durch:

☐ Schlüssel	☐ Magnet- oder Chipkarten
☐ Elektrische Türöffner	☐ Portier
☐ Sicherheitspersonal	☐ Alarmanlagen
☐ Videoanlage	☐ Einbruchshemmende Fenster und/oder Sicherheitstüren
☐ Anmeldung beim Empfang mit Personenkontrolle	☐ Begleitung von Besuchern im Unternehmensgebäude
☐ Tragen von Firmen-/Besucherausweisen	☐ Sonstiges:

Zugangskontrolle: Schutz vor unbefugter Systembenutzung durch:

☐ Kennwörter (einschließlich entsprechender Policy)	☐ Verschlüsselung von Datenträgern
☐ Automatische Sperrmechanismen	☐ Sonstiges:
☐ Zwei-Faktor-Authentifizierung	

Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch:

☐ Standard-Berechtigungsprofile auf „need to know-Basis“	☐ Standardprozess für Berechtigungsvergabe
☐ Protokollierung von Zugriffen	☐ Sichere Aufbewahrung von Speichermedien
☐ Periodische Überprüfung der vergebenen Berechtigungen, insb von administrativen Benutzerkonten	☐ Datenschutzgerechte Wiederverwendung von Datenträgern
☐ Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger	☐ Clear-Desk/Clear-Screen Policy
☐ Sonstiges:	

Pseudonymisierung: sofern für die jeweilige Datenverarbeitung möglich, werden die primären Identifikationsmerkmale der personenbezogenen Daten in der jeweiligen Datenverarbeitung entfernt, und gesondert

aufbewahrt.

☐ ja	☐ nein

Klassifikationsschema für Daten: Aufgrund gesetzlicher Verpflichtungen oder Selbsteinschätzung (geheim/vertraulich/intern/öffentlich).

☐ ja	☐ nein

B. Datenintegrität [Fußnote: Verhinderung von (unbeabsichtigter) Zerstörung/Vernichtung, (unbeabsichtigter) Schädigung, (unbeabsichtigtem) Verlust, (unbeabsichtigter) Veränderung von personenbezogenen Daten.]

Weitergabekontrolle: kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch:

☐ Verschlüsselung von Datenträgern	☐ Verschlüsselung von Dateien
☐ Virtual Private Networks (VPN)	☐ Elektronische Signatur
☐ Sonstiges:	

Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch:

☐ Protokollierung	☐ Dokumentenmanagement
☐ Sonstiges:	

C. Verfügbarkeit und Belastbarkeit

Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw Verlust durch:

☐ Backup-Strategie (online/offline; on-site/off-site)	☐ Unterbrechungsfreie Stromversorgung (USV, Dieselaggregat)
☐ Virenschutz	☐ Firewall
☐ Meldewege und Notfallpläne	☐ Security Checks auf Infrastruktur- und Applikationsebene
☐ Mehrstufiges Sicherungskonzept mit verschlüsselter Auslagerung der Sicherungen in ein Ausweichrechenzentrum	☐ Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern
☐ Sonstiges:	

Rasche **Wiederherstellbarkeit:**

☐ ja	☐ nein

D. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

Datenschutz-Management, einschließlich regelmäßiger Mitarbeiter-Schulungen:

☐ ja	☐ nein

Incident-Response-Management:

☐ ja	☐ nein

Datenschutzfreundliche Voreinstellungen:

☐ ja	☐ nein

Auftragskontrolle: keine Auftragsdatenverarbeitung iSv Art 28 DS-GVO ohne entsprechende Weisung des Auftraggebers durch:

☐ Eindeutige Vertragsgestaltung	☐ Formalisiertes Auftragsmanagement
☐ Strenge Auswahl des Auftragsverarbeiters (ISO-Zertifizierung, ISMS)	☐ Vorabüberzeugungspflicht
☐ Nachkontrollen	☐ Sonstiges: