

# Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Daten gem. Art. 32 DSGVO

## Verantwortlicher:

### 101skills GmbH

Rostocker Str. 68 ,20099 Hamburg, Deutschland

E-Mail: [mail@fobizz.com](mailto:mail@fobizz.com)

## Datenschutzbeauftragter:

### Herting Oberbeck Datenschutz GmbH

Herr Sebastian Herting,

Hallerstr. 76, 20146 Hamburg, Deutschland

Telefon: 040-228691140

E-Mail: [datenschutzbeauftragter@fobizz.com](mailto:datenschutzbeauftragter@fobizz.com)

## Präambel

Die EU-Datenschutzgrundverordnung (DSGVO) schreibt vor, dass jeder Verantwortliche sowie Auftragsverarbeiter 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 geeignete technische und organisatorische Maßnahmen zu treffen hat, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Teil der Erfüllung unserer Rechenschaftspflicht aus Art. 5 Abs. 2 DSGVO ist die Dokumentation der getroffenen technischen und organisatorischen Maßnahmen. Dieser Zweck soll mit dem vorliegenden Dokument erfüllt werden.

## Hinweis zu Maßnahmen bei weiteren (Unter)-Auftragsverarbeitern:

Die maßgebliche Datenverarbeitung im Zusammenhang mit den fobizz-Plattform (Online-Fortbildungen, digitale Tools und digitale Unterrichtsmaterialien) erfolgt auf IT-Systemen, die von unserem weiteren Auftragsverarbeiter Scalingo SAS betrieben werden. Bitte beachten Sie diesbezüglich ergänzend **Scalingo's Information Systems Security Policy** (wird auf Anfrage bereitgestellt).

Die Nachfolgend dokumentierten Maßnahmen werden durch den Verantwortlichen umgesetzt.

## A. Vertraulichkeit (Art. 32 Abs. 1 Buchst. b DSGVO)

Personenbezogene Daten müssen einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Das Unternehmen hat geeignete technische und organisatorische Maßnahmen getroffen für den Schutz personenbezogener Daten

- vor unbefugter oder unrechtmäßiger Verarbeitung
- vor unbeabsichtigtem Verlust
- vor unbeabsichtigter Zerstörung
- vor unbeabsichtigter Schädigung

## 1. Zutrittskontrolle

Geeignete Maßnahmen der Zutrittskontrolle **verwehren unbefugten Personen physisch den Zutritt** zu Datenverarbeitungsanlagen. Sie stellen sicher, dass nur autorisierte Personen Zutritt zu den Datenverarbeitungsanlagen erhalten. Wirksame Zutrittskontrollmaßnahmen minimieren insbesondere folgende Risiken:

- Verlust/Zerstörung/Beschädigung von Datenverarbeitungsanlagen
- unrechtmäßige oder unbefugte Verarbeitung wie z.B. Einsichtnahme

### *Technische Maßnahmen*

- Chipkarten- oder Transpondersystem
- Alarmanlage
- Zugang durch Tür mit Knauf auf der Außenseite

- Absicherung der Gebäudeschächte
- Zutrittssicherung Gebäudetechnik
- Zutrittssicherung Router (Access Point)
- Sicherheitsschlösser
- Fenstersicherung

### *Organisatorische Maßnahmen*

- Gebäude außerhalb der Geschäftszeiten verschlossen
- Schlüsselregelung / -dokumentation
- Schließordnung (Regelung betreffend Öffnen / Verschließen von Gebäuden und Räumen)
- Richtlinie/ Anweisung für Zutritt Externer
- Richtlinie/ Anweisungen für Umgang mit Besuchern (Zutritt nur bei ständiger Begleitung)
- Sorgfalt bei der Auswahl von Reinigungsdiensten

## 2. Zugangskontrolle

Die Zugangskontrolle soll die **unbefugte Nutzung von Datenverarbeitungssystemen verhindern**, so dass nur autorisierte Personen Zugang zu Datenverarbeitungssystemen erhalten und sie nutzen können. Wirksame Zutrittskontrollmaßnahmen minimieren insbesondere folgende Risiken:

- Verlust/Zerstörung/Beschädigung von Datenverarbeitungsanlagen
- unrechtmäßige oder unbefugte Verarbeitung wie z.B. Einsichtnahme

### *Technische Maßnahmen*

- Benutzer-Authentifikation (Name und Passwort)
- Zugangssicherung Netzwerk (Kabelverbindung)
- Virenschutz auf Datenverarbeitungssystemen
- Firewall
- Zugangssicherung des WLAN
- Automatische Desktopsperrung
- Zugangssicherung des Gäste-WLAN
- Verschlüsselung von Laptops, Tablets, Smartphones

### *Organisatorische Maßnahmen*

- Passwortrichtlinie
- Richtlinie Löschen / Vernichten von personenbezogenen Daten
- Richtlinie für den Umgang mit Laptops/ Tablets / Smartphones
- Clear Desktop Policy
- Anweisung zur manuellen Desktopsperrung
- Richtlinie zur Löschung/Vernichtung von Dokumenten mit personenbezogenen Daten
- Verwalten von Benutzerrechten

## 3. Zugriffskontrolle

Zugriffskontrollmaßnahmen sollen gewährleisten, dass ein Benutzer des Datenverarbeitungssystems ausschließlich auf solche personenbezogenen Daten **Zugriff** erhält, zu deren Verarbeitung eine **Berechtigung** vorliegt. Eine wirksame Zugriffskontrolle minimiert folgende Risiken:

- unbefugte Einsichtnahme bei Verarbeitung und Nutzung
- unbefugtes Kopieren
- unbefugte Veränderung • unbefugte Löschung

### *Technische Maßnahmen*

- Aktenschredder
- Verwaltung der Zugriffsrechte durch wenige notwendige Administratoren
- Abschließbare Dokumentenschränke
- Zugriffsprotokolle (Datenverarbeitungsanlagen)

### *Organisatorische Maßnahmen*

- Verwaltung von Benutzerberechtigungen (Berechtigungskonzept)
- Clear Desktop Policy
- Vertraulichkeitsverpflichtung

- Übereinstimmung von Zugriffsberechtigungen „digital und analog“
- Formaler Prozess für Erteilung von Zugriffsberechtigungen
- Anweisung Entsorgung von Papierdokumenten und Datenträgern

#### 4. Trennungskontrolle

Maßnahmen der Trennungskontrolle sollen gewährleisten, dass personenbezogene Daten, die zu unterschiedlichen Verarbeitungszwecken erhoben wurden, **zweckgebunden und getrennt** verarbeitet werden. Außerdem gewährleistet die Trennungskontrolle die Mandantenfähigkeit der Verarbeitungsvorgänge, insoweit dies erforderlich ist (z.B. bei Nutzerkonten einer Online-Plattform) Eine wirksame Trennungskontrolle minimiert folgende Risiken:

- unbefugte Einsichtnahme personenbezogener Daten
- Verarbeitung von personenbezogenen Daten in einer nicht mit den Verarbeitungszwecken zu vereinbarenden Weise

##### *Technische Maßnahmen*

- Trennung von Test- und Produktivumgebung
- Physikalische Trennung (Systeme / Datenbanken / Datenträger)
- Physikalische Trennung von Unterlagen (z.B. Ordner)

##### *Organisatorische Maßnahmen*

- Verwaltung von Benutzerberechtigungen für Datenbanken/ Anwendungen
- Verzeichnis von Verarbeitungstätigkeiten
- Anweisung zur Trennung privater und betrieblicher Daten
- Keine Nutzung privater Geräte für betriebliche Verarbeitungsprozess
- Keine private Nutzung betrieblicher Geräte

## B. Integrität (Art. 32 Abs. 1 Buchst. b DSGVO)

Personenbezogene Daten müssen einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Das Unternehmen hat geeignete technische und organisatorische Maßnahmen getroffen für den Schutz personenbezogener Daten

- vor unbefugter oder unrechtmäßiger Verarbeitung
- vor unbeabsichtigtem Verlust
- vor unbeabsichtigter Zerstörung • vor unbeabsichtigter Schädigung

### 1. Weitergabekontrolle

Weitergabekontrolle verhindert, dass personenbezogene Daten bei der elektronischen **Übertragung** oder während ihres Transports oder ihrer Speicherung auf Datenträgern **unbefugt gelesen, kopiert, verändert oder entfernt** werden.

Außerdem wird im Rahmen der Weitergabekontrolle überprüfbar dokumentiert, welche Empfänger personenbezogene Daten Datenübermittlungen erhalten sollen.

##### *Technische Maßnahmen*

- Bereitstellung nur über verschlüsselte Verbindungen wie sftp, https
- Protokollierung der Zugriffe
- Einsatz digitaler Signaturverfahren (z.B. digitale Unterschrift auf PDF)

##### *Organisatorische Maßnahmen*

- Sorgfältige Auswahl Auftragsverarbeiter
- Sorgfältige Auswahl Dienstleister

### 2. Eingabekontrolle

Maßnahmen der **Eingabekontrolle** sollen gewährleisten, dass **nachträglich überprüft** und festgestellt werden kann, ob und wie personenbezogene Daten eingegeben, verändert oder entfernt worden sind, um die **Richtigkeit** und Integrität der personenbezogenen Daten sicherstellen zu können.

##### *Technische Maßnahmen*

- Automatisches Protokollieren von Änderungen und Eingaben
- Protokollieren von Löschvorgängen

- Kollisionsprüfung bei Datenbanken

### *Organisatorische Maßnahmen*

- Zuständigkeit für Löschung definiert
- Berechtigungskonzept

## C. Pseudonymisierung (Art. 32 Abs. 1 Buchst. a DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten in einer Weise verarbeitet werden, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

### *Organisatorische Maßnahmen*

- Kundennummern
- Personalnummern

## D. Verschlüsselung personenbezogener Daten (Art. 32 Abs. 1 Buchst. a DSGVO)

Art. 32 Abs. 1 Buchst. a DSGVO zeigt die **Verschlüsselung** von personenbezogenen Daten als Maßnahme zum Schutz der Sicherheit personenbezogener Daten auf.

### *Technische Maßnahmen*

- SSL-Verschlüsselung auf Website(s)

- Verschlüsselte E-Mail-Kommunikation

### *Organisatorische Maßnahmen*

- Richtlinie zum Umgang mit Verschlüsselungsmöglichkeiten

## E. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 Buchst. b DSGVO)

Durch Maßnahmen wird gewährleistet, dass personenbezogene **Daten gegen Zerstörung, oder Verlust geschützt** sind. Eine wirksame Verfügbarkeitskontrolle stellt sicher, dass personenbezogene Daten zu den erforderlichen Zeiten auch **tatsächlich verfügbar** sind.

- Die Datenverarbeitung erfolgt auf IT-Systemen, die durch weitere Auftragsverarbeiter bereitgestellt werden. Diese ergreifen die erforderlichen Maßnahmen, um die Verfügbarkeit und Belastbarkeit sicherzustellen.

## F. Wiederherstellbarkeit (Art. 32 Abs. 1 Buchst. c DSGVO)

Maßnahmen zur regelmäßigen Überprüfung der **Wiederherstellbarkeit des Datenbestands**.

- Die Datenverarbeitung erfolgt auf IT-Systemen, die durch weitere Auftragsverarbeiter bereitgestellt werden. Diese ergreifen die erforderlichen Maßnahmen, um die Wiederherstellbarkeit sicherzustellen.

## G. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 Buchst. d. DSGVO)

Es wurden Verfahren zur regelmäßigen **Überprüfung, Bewertung und Evaluierung der Wirksamkeit** der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung eingerichtet.

## 1. Datenschutz-Management

### *Organisatorische Maßnahmen*

- Regelmäßige Überprüfung Zutrittskontrollmaßnahmen
- Jährliche Schulungsmaßnahme der Beschäftigten
- Bestellung Datenschutzbeauftragte/r
- Bestellung IT-Sicherheitsbeauftragte/r
- Jährliche Überprüfung technischer und organisatorischer Maßnahmen
- Regelmäßige Überprüfung von Auftragsverarbeitern
- Datenschutzfolgeabschätzungen werden bei Bedarf durchgeführt

## 2. Datenschutz-Prozesse

### *Technische Maßnahmen*

- Einsatz von Virenschutz-Anwendungen
- Einsatz von Monitoring-Anwendungen

### *Organisatorische Maßnahmen*

- Löschkonzept
- Definierte Prozesse zur Erfüllung von Betroffenenrechten
- Definierter Prozess zur Meldung von Datenpannen (über externen Datenschutzbeauftragten)
- Dokumentation von Sicherheitsvorfällen

## 3. Auftragskontrolle

Diese Maßnahmen gewährleisten, dass personenbezogene Daten, die in unserem Auftrag verarbeitet werden, **nur entsprechend unserer Weisungen** verarbeitet werden.

### *Organisatorische Maßnahmen*

- Vorherige Prüfung der TOM des Auftragnehmers
- Sorgfältige Auswahl von Auftragnehmern
- Schriftliche/elektronisch dokumentierte Weisungen an Auftragsverarbeiter
- Abschluss von AVV
- Einsatz von EU-Standard-Vertragsklauseln

## H. Datenschutz durch Technikgestaltung (Art. 25 Abs. 1 DSGVO) und datenschutzfreundliche Voreinstellungen

Maßnahmen zur Berücksichtigung der Anforderung des Datenschutzes durch **Technikgestaltung** und des Datenschutzes durch **datenschutzfreundliche Voreinstellungen**.

### *Technische Maßnahmen*

- Datenerhebung nach Sparsamkeitsprinzip
- Einfache Ausübung des Widerrufsrechts des Betroffenen möglich
- Einbindung von KI-Modellen via API erfolgt über zwischengeschalteten fobizz-Server als Proxy

## Stand der Dokumentation

### **Version**

- v 1.0 Dezember 2018
- v 2.0 Dezember 2019
- v 2.1 Dezember 2020
- v 2.2 Dezember 2021
- v 2.3 September 2022
- v 2.4 August 2023
- v. 2.5 Juni 2025