# Vorlage Technische und Organisatorische Maßnahmen (TOM)

der abl social federation GmbH

## Wichtige Informationen zum Dokument

| | |
|---|---|
| **Empfängerkreis** | **External** |
| **Klassifizierung** | **Public** |
| **Bearbeitungsstatus** | **Freigabe** |

| | **Erstellung / Letzte Änderung** | **Prüfung** | **Freigabe** |
|---|---|---|---|
| **Datum** | 06.11.2020 | 06.11.2020 | 06.11.2020 |
| **Name** | Matthias Köbrich | Benjamin Becker | Benjamin Becker |
| **Unterschrift** | [unterschrieben] | [unterschrieben] | [unterschrieben] |

## Empfängerkreis

Alle Mitarbeiter der abl und alle betreffenden externen Partner und Dienstleister.

abl social federation GmbH
Headquarters: Hugo-Junkers-Straße 9 / D-90411 Nürnberg
German Branch Office Berlin: Am Studio 2a / D-12489 Berlin
T: +49 911 477 157 0 / M: info@abl-solutions.com / H: www.abl-solutions.com

**Anlage 2**

**zur Vereinbarung über Auftragsverarbeitung**

**Technische und organisatorische Maßnahmen**

## 1. VORBEMERKUNG

Diese Dokumentation enthält die technischen und organisatorischen Maßnahmen gemäß Art. 24, 32 Abs. 1 DSGVO. Die Maßnahmenkategorien werden den Schutzbedarfszielen Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit untergeordnet, wobei die Belastbarkeit als Unterkategorie der Verfügbarkeit betrachtet wird.

## 2. VERTRAULICHKEIT, ART. 32 ABS. 1 LIT. B DSGVO

### 2.1. Zutrittskontrolle

Konkrete Maßnahmen:

- Alarmanlage in den Büroräumlichkeiten
- Schließsystem mit Codesperre in den Büroräumlichkeiten
- Dezidierte Schlüsselregelung
- Manuelles Schließsystem in den Büroräumlichkeiten
- Sicherheitsschlösser
- Videoaufzeichnung
- Zutrittskontrollsystem
- Transponderverwaltung
- Besucherregelungen
- Begleitpflicht bei betriebsfremden Personen
- Abschließbare Büroräume
- Anweisung zum Verschließen der Büroräume
- Sorgfältige Auswahl des Reinigungspersonals

### 2.2. Zugangskontrolle

Konkrete Maßnahmen:

- Zuweisung individueller personenbezogener Benutzerkennungen
- Zuordnung von Benutzerrechten
- Passwortvergabe
- Authentifikation mit Benutzername / Passwort
- Schlüsselregelung
- Einsatz von Intrusion-Detection-Systemen
- Erstellung von Benutzerprofilen
- Zuordnung von Benutzerprofielen zu IT-Systemen
- Einsatz von VPN Technologie

- Sicherheitsschlösser
- Einsatz von Anti-Viren Software
- Einsatz einer Hardware Firewall
- Einsatz einer Software Firewall
- Zugangssperre bei Falscheingabe von Passwörtern
- Persönliche Überwachung bei Fernwartung der DV-Anlagen
- Nutzung von Remote-Tools nur für berechtigtes Personal

### 2.3. Zugriffskontrolle

Konkrete Maßnahmen:

- Erstellen eines Berechtigungskonzepts
- Restriktive Vergabe von Berechtigungen auf Dateien
- Vergabe von differenzierten Berechtigungen (lesen, schreiben, ändern, löschen)
- Verwaltung der Rechte durch Administrator
- Restriktive Vergabe von Administratorenrechten
- Restriktive Vergabe von Anwendungen sowie (differenzierten) Berechtigungen in Anwendungen
- Anzahl der Administratoren auf das „Notwendigste" reduziert
- Einsatz von Datenschutztonnen und Aktenvernichtern bzw. DSGVO geprüftem Dienstleister
- Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel

### 2.4. Trennungskontrolle

Konkrete Maßnahmen:

- Festlegung von Datenbankrechten
- Logische Mandantentrennung (softwareseitig)
- Trennung von Produktiv- und Testsystemen

### 2.5. Pseudonymisierung/Anonymisierung

Konkrete Maßnahmen:

- Einsatz von Hash- & Salt-Verfahren

## 3. INTEGRITÄT

### 3.1. Weitergabekontrolle

Konkrete Maßnahmen:

- Einrichtung von Standleitungen bzw. VPN-Tunneln
- Übertragung der Daten von Hotspot zu abl mit Maßnahmen aufnehmen!

### 3.2. Eingabekontrolle

Konkrete Maßnahmen:

- Protokollierung von Zugriffen und Änderungen auf User-Daten erklären und Maßnahmen aufnehmen!

## 4. Verfügbarkeit & Belastbarkeit

### 4.1. Verfügbarkeitskontrolle

Konkrete Maßnahmen:

- Unterbrechungsfreie Stromversorgung (USV)
- Feuer- und Rauchmeldeanlagen
- Schutzsteckdosenleisten in Serverräumen
- Feuerlöscher in den Büroräumlichkeiten
- Alarmmeldung bei unberechtigtem Zutritt zu den Server-/Büroräumen
- Erstellen eines regelmäßigen Backup- und Recovery-Konzepts
- Serverräumen nicht unter sanitären Anlagen
- Erstellen eins Notfallplans und Konzept
- Testen von Datenwiederherstellungen

### 4.2. Rasche Wiederherstellbarkeit

Konkrete Maßnahmen:

- Festplattenspiegelung (RAID)
- Erstellen regelmäßiger Backups
- Regelmäßige Überprüfung der Backups
- Räumlich getrennte Aufbewahrung der Backups

## 5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

### 5.1. Maßnahmen der Überprüfung, Bewertung und Evaluierung

Konkrete Maßnahmen:

**Datenschutz-Management**

- Nutzung einer Datenschutz-Managementsoftware zur Abbildung aller datenschutzrelevanter Prozesse
- Bestellung eines externen Datenschutzbeauftragten
- Regelmäßige Rücksprache mit den zuständigen Aufsichtsbehörden (BNetzA, BayLDA)
- Verteilung von Zuständigkeiten innerhalb des etablierten Datenschutz-Managementsystems
- Integration des Datenschutz-Managementsystems in das Informationssicherheits-Managementsystem (ISO 27001)

- Verpflichtung der Mitarbeiter auf Vertraulichkeit und das Fernmeldegeheimnis bei Aufnahme des Beschäftigungsverhältnisses
- Etablierung mehrerer Richtlinien über Datenschutz, IT-Sicherheit und Informationssicherheit
- Regelmäßige Sensibilisierung der Mitarbeiter im Datenschutz, der IT-Sicherheit und Informationssicherheit
- Vorhalten von definierten Prozessen und Vorlagen für die Beantwortung und Unterstützung der Beantwortung von Betroffenenanfragen

**Incident-Response-Management**

- Erstellung eines Prozesses zum Umgang mit Datenschutzverletzungen und Sicherheitsvorfällen
- Vorhalten eines Notfallkonzepts

**Beachtung von Privacy-by-design / Privacy-by-default**

- Prüfung aller Verarbeitungstätigkeiten durch den Datenschutzbeauftragten auf Einhaltung der Datenschutzgrundsätze nach Art. 5 Abs. 1 DSGVO
- Prinzipiell wird das Verbot mit Erlaubnisvorbehalt in allen Bereichen des Datenschutzes vorausgesetzt
- Das ‚need-to-know'-Prinzip wird strikt durchgesetzt
- Einbeziehung des Datenschutzbeauftragten bereits bei der Planung neuer Projekte
- Beachtung anerkannter Verhaltensregeln
- Regelmäßige Kontrolle der Maßnahmen und Verfahren

## 5.2. Auftragskontrolle

Konkrete Maßnahmen:

- Sorgfältige Auswahl der Auftragnehmer
- Einholen von Referenzen über potenzielle Auftragsverarbeiter
- Forderung des Datensicherheitskonzepts
- Vorhalten von geprüften und speziellen Vertragsvorlagen
- Kontrolle und Dokumentation der Auftragsdurchführung

| | |
|---|---|
| Ort, Datum | Ort, Datum |
| Unterschrift und Funktion Auftragnehmer (abl social federation GmbH) | Unterschrift und Funktion Auftraggeber |

## Versionskontrolle

| Version | Datum | Bearbeiter | Änderungen | Bemerkungen |
|---|---|---|---|---|
| 1.0 | 03.02.2020 | Hanna Metzger | Ersterstellung | |
| 1.1 | 06.11.2020 | Matthias Köbrich | Änderung | Lenkung, Klassifizierung, CI |

abl social federation GmbH
Headquarters: Hugo-Junkers-Straße 9 / D-90411 Nürnberg
German Branch Office Berlin: Am Studio 2a / D-12489 Berlin
T: +49 911 477 157 0 / M: info@abl-solutions.com / H: www.abl-solutions.com