

Anhang I

Technische und organisatorische Maßnahmen (TOM)

i.S.d. Art. 32 DSGVO

der Organisation
DIG GmbH („DIG“)

1. Versionshistorie

Version	Geändert am	Geändert von	Änderung
1	04.04.2018	Jakob Eidenberger	Original
2	22.05.2018	Dieter Dobersberger	Maßnahmen aktualisiert
3	24.05.2018	Jakob Eidenberger	Formatierungen und Formulierungen angepasst, Maßnahmen zusammengeführt
4	04.06.2018	Jakob Eidenberger	Maßnahme „E-Mail-Verschlüsselung“ formuliert
5	28.06.2019	Jakob Eidenberger	Anpassung neues Design
6	16.02.2021	Michael Neumüller	Änderung Datenschutzbeauftragter

Der aktuelle Stand findet sich stets auf der DIG-Homepage unter folgendem Link:

<https://dig.at/de/Datenschutz>

Organisationen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften der Datenschutzgesetze zu gewährleisten.

Die DIG erfüllt diesen Anspruch durch folgende Maßnahmen:

2. Vertraulichkeit gem. Art. 32 Abs. 1 lit. DSGVO

2.1. Zutrittskontrolle

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

Technische Maßnahmen am Standort Büro Linz

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Manuelles Schließsystem	<input checked="" type="checkbox"/> Schlüsselregelung / Liste
<input checked="" type="checkbox"/> Sicherheitsschlösser	<input checked="" type="checkbox"/> Besucher in Begleitung durch Mitarbeiter
<input checked="" type="checkbox"/> Türen mit Knauf Außenseite	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl Reinigungsdienste

Technische Maßnahmen am Standort Datacenter Wien

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Alarmanlage	<input checked="" type="checkbox"/> Schlüsselregelung / Liste
<input checked="" type="checkbox"/> Automatisches Zugangskontrollsystem	<input checked="" type="checkbox"/> Empfang / Rezeption / Pförtner
<input checked="" type="checkbox"/> Chipkarten / Transpondersysteme	<input checked="" type="checkbox"/> Besucherbuch / Protokoll der Besucher
<input checked="" type="checkbox"/> Sicherheitsschlösser	<input checked="" type="checkbox"/> Mitarbeiter- / Besucherausweise
<input checked="" type="checkbox"/> Absicherung der Gebäudeschächte	<input checked="" type="checkbox"/> Besucher in Begleitung durch Mitarbeiter
<input checked="" type="checkbox"/> Türen mit Knauf Außenseite	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl des Wachpersonals
<input checked="" type="checkbox"/> Videoüberwachung der Eingänge	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl Reinigungsdienste

Weitere Maßnahmen:

Am Bürostandort der DIG in Linz sind lokal keine Daten gespeichert. Sämtliche Server laufen im Datacenter. Das Datacenter wird von der A1 Telekom Austria betrieben. Vor Ort ist 24x7 ein Wachdienst im Einsatz. Die Serverräume sind nur für berechtigte Personen nach persönlicher Identifikation erreichbar. Alarmanlage und Videoüberwachung sind vorhanden. Das Datacenter ist ISO27001 zertifiziert.

2.2. Zugangskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Login mit Benutzername + Passwort	<input checked="" type="checkbox"/> Verwalten von Benutzerberechtigungen
<input checked="" type="checkbox"/> Anti-Viren-Software Server	<input checked="" type="checkbox"/> Erstellen von Benutzerprofilen
<input checked="" type="checkbox"/> Anti-Virus-Software Clients	<input checked="" type="checkbox"/> Zentrale Passwortvergabe
<input checked="" type="checkbox"/> Anti-Virus-Software mobile Geräte	<input checked="" type="checkbox"/> Richtlinie „Sicheres Passwort“
<input checked="" type="checkbox"/> Firewall	<input checked="" type="checkbox"/> Richtlinie „Löschen / Vernichten“
<input checked="" type="checkbox"/> Intrusion Detection System Intrusion Detection System	<input checked="" type="checkbox"/> Richtlinie „Clean desk“
<input checked="" type="checkbox"/> Einsatz VPN bei Remote-Zugriffen	<input checked="" type="checkbox"/> Allg. Richtlinie Datenschutz und / oder Sicherheit
<input checked="" type="checkbox"/> Verschlüsselung von Datenträgern	<input checked="" type="checkbox"/> Mobile Device Policy
<input checked="" type="checkbox"/> Verschlüsselung Smartphones	<input checked="" type="checkbox"/> Anleitung „Manuelle Desktopsperre“
<input checked="" type="checkbox"/> Automatische Desktopsperre	<input checked="" type="checkbox"/> Berechtigungen werden nach dem Minimalprinzip vergeben und dokumentiert. Eine Überprüfung findet regelmäßig statt.
<input checked="" type="checkbox"/> Verschlüsselung von Notebooks / Tablet	<input type="checkbox"/>

Weitere Maßnahmen:

Alle Systeme verfügen über ein Berechtigungssystem. Es wird vom System vorgegeben, dass nur starke Passwörter verwendet werden können. Wo es sinnvoll ist, wird ein regelmäßiges Ändern der Passwörter erzwungen. Benutzersessions laufen nach einer vorgegebenen Zeit ab. Zugang zu sensiblen Systemen ist nur über VPN möglich. Alle Zugriffe von außen erfolgen grundsätzlich mit Verschlüsselung (STARTTLS, TLS, SSH, VPN).

2.3. 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.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Aktenschredder (mind. Stufe 3, cross cut)	<input checked="" type="checkbox"/> Einsatz Berechtigungskonzepte
<input checked="" type="checkbox"/> Physische Löschung von Datenträgern	<input checked="" type="checkbox"/> Minimale Anzahl an Administratoren
<input checked="" type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	<input checked="" type="checkbox"/> Verwaltung Benutzerrechte durch Administratoren
<input checked="" type="checkbox"/> Sämtliche Datenträger sind im Rechenzentrum der A1 Telekom gesichert.	<input checked="" type="checkbox"/> Mitarbeiter sind angewiesen, Daten nur nach dienstlicher Notwendigkeit zu verwenden.
<input checked="" type="checkbox"/> Backupdatenträger, die den Serverraum verlassen, sind immer verschlüsselt.	

Weitere Maßnahmen:

Alle Systeme verfügen über ein Rollen/Rechte Konzept. Zugriff wird nur für autorisierte Personen erteilt. Bei sensiblen Systemen erfolgt eine Protokollierung der Erteilung und des Entzugs von Rechten. Änderungen bei Rechten von Kunden-Usern können nur per Ticketsystem erfolgen.

2.4. Trennungskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Trennung von Produktiv- und Testumgebung	<input checked="" type="checkbox"/> Steuerung über Berechtigungskonzept
<input checked="" type="checkbox"/> Physikalische Trennung (Systeme / Datenbanken / Datenträger)	<input checked="" type="checkbox"/> Festlegung von Datenbankrechten
<input checked="" type="checkbox"/> Mandantenfähigkeit relevanter Anwendungen	

Weitere Maßnahmen:

Es gibt mehrere getrennte Systemlandschaften für Entwicklungs-, Test- und Produktivsysteme. Diese sind durch VLANs im Datacenter getrennt. Die Trennung der Mandanten im Echtsystem erfolgt durch getrennte Datenbanken und eine softwareseitige Mandantentrennung in der Applikation.

2.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO; Art. 25 Abs. 1 DSGVO)

Die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechende technischen und organisatorischen Maßnahmen unterliegen.

Technische Maßnahmen	Organisatorische Maßnahmen
	<input checked="" type="checkbox"/> Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymisieren

3. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

3.1. 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.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Email-Verschlüsselung	<input checked="" type="checkbox"/> Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
<input checked="" type="checkbox"/> Einsatz von VPN	<input checked="" type="checkbox"/> Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
<input checked="" type="checkbox"/> Protokollierung der Zugriffe und Abrufe	<input checked="" type="checkbox"/> Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
<input checked="" type="checkbox"/> Bereitstellung über verschlüsselte Verbindungen wie sftp, https	<input checked="" type="checkbox"/> Persönliche Übergabe mit Protokoll
<input checked="" type="checkbox"/> Nutzung von Signaturverfahren	
<input checked="" type="checkbox"/> Verschlüsselung von Datenträgern	

Weitere Maßnahmen:

Berechtigungssystem und Verwendung nur bei dienstlicher Notwendigkeit.

Die Übertragung von Daten von und zum DIG Datacenter erfolgt immer verschlüsselt durch VPN oder vergleichbare Maßnahmen. Gespeicherte Daten sind nur mit der nötigen Berechtigung durch autorisierte Mitarbeiter lesbar. Die Übermittlung an externe System ist nur an definierten Stellen möglich. Zwischen den Mailservern der DIG und dem Geschäftspartner wird beim Versand immer eine Ad-Hoc Verschlüsselung durchgeführt. Diese basiert auf sehr modernen und starken Standards (aktuell RSA, AES256, SHA384). Die Übermittlung per Fax oder an veraltete Emailsysteme bei Lieferanten kann unverschlüsselt erfolgen. Daten können an Internetprovider der Kommunikationspartner übergeben werden, wenn deren Mailserver und DNS Server entsprechend konfiguriert sind.

Datenträger, die das Datacenter verlassen (z.B. für Offsite Backups) sind immer verschlüsselt.

Zustimmung des Betroffenen zur Anfertigung und Veröffentlichung von Porträtfotos

- Einladung: Hinweis auf Verarbeitung der Fotos
- Vor der Anfertigung von Porträtfotos wird der Fotograf eine Zustimmung einholen (mit Fotograf abklären).

3.2. 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.

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	<input checked="" type="checkbox"/> Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
<input checked="" type="checkbox"/> Eine Änderung der Daten ist in der Applikation nicht vorgesehen.	<input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	<input checked="" type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen wurden

Weitere Maßnahmen:

Bei kritischen Systemen erfolgt eine Protokollierung von Änderungen. Dies betrifft vor allem Usernamen, Passwörter, Erteilen und Entziehen von Berechtigungen.

4. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

4.1. Verfügbarkeitskontrolle

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

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen	<input checked="" type="checkbox"/> Backup & Recovery-Konzept (ausformuliert)
<input checked="" type="checkbox"/> Feuerlöscher Serverraum	<input checked="" type="checkbox"/> Kontrolle des Sicherungsvorgangs
<input checked="" type="checkbox"/> Serverraumüberwachung Temperatur und Feuchtigkeit	<input checked="" type="checkbox"/> Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
<input checked="" type="checkbox"/> Serverraum klimatisiert	<input checked="" type="checkbox"/> Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
<input checked="" type="checkbox"/> USV	<input checked="" type="checkbox"/> Keine sanitären Anschlüsse im oder oberhalb des Serverraums
<input checked="" type="checkbox"/> Schutzsteckdosenleisten Serverraum	<input checked="" type="checkbox"/> Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
<input checked="" type="checkbox"/> RAID System / Festplattenspiegelung	<input checked="" type="checkbox"/> Getrennte Partitionen für Betriebssysteme und Daten
<input checked="" type="checkbox"/> Videoüberwachung Serverraum	
<input checked="" type="checkbox"/> Alarmmeldung bei unberechtigtem Zutritt zu Serverraum	

Weitere Maßnahmen:

Das Rechenzentrum wird nach aktuellem Stand der Technik durch A1 Telekom betrieben. Das Rechenzentrum ist klimatisiert, brandgeschützt und redundant mit Strom versorgt. Es existiert ein Ausfallrechenzentrum an einem zweiten Standort. Es werden regelmäßig Backups angelegt.; Backups die das Data-Center verlassen sind verschlüsselt; Einmal pro Monat wird stichprobenartig ein Teil der Backups restored.

5. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

5.1. Datenschutz-Management

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Zentrale Dokumentation aller Verfahrenswesen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet ...)	<input checked="" type="checkbox"/> Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten Michael Neumüller datenschutz@dig.at
<input checked="" type="checkbox"/> Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	<input checked="" type="checkbox"/> Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
	<input checked="" type="checkbox"/> Regelmäßige Sensibilisierung der Mitarbeiter (mindestens jährlich)
	<input checked="" type="checkbox"/> Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	<input checked="" type="checkbox"/> Die Organisation kommt den Informationspflichten nach Art. 13 und 14 DSGVO nach

5.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Einsatz von Firewall und regelmäßige Aktualisierung	<input checked="" type="checkbox"/> Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Datenpannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
<input checked="" type="checkbox"/> Einsatz von Spamfilter und regelmäßige Aktualisierung	<input checked="" type="checkbox"/> Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
<input checked="" type="checkbox"/> Einsatz von Virens Scanner und regelmäßige Aktualisierung	<input checked="" type="checkbox"/> Einbindung von <input checked="" type="checkbox"/> DSB und <input type="checkbox"/> ISB in Sicherheitsvorfälle und Datenpannen
<input checked="" type="checkbox"/> Intrusion Detection System (IDS)	<input checked="" type="checkbox"/> Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
<input checked="" type="checkbox"/> Intrusion Prevention System (IPS)	

Weitere Maßnahmen:

Das Systemmonitoring der A1 Telekom überwacht die Netzwerkverbindung des Datacenters und verhindert Angriffe auf dieser Ebene. DIG betreibt eine zusätzliche Firewall am Perimeter des eigenen Netzwerksegments.

5.3. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO);

Privacy by design / Privacy by default

Technische Maßnahmen	Organisatorische Maßnahmen
<input checked="" type="checkbox"/> Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	<input checked="" type="checkbox"/> Einfache Ausübung des Widerrufsrechts des Betroffenen durch organisatorische Maßnahmen (Newsletter)

5.4. Auftragskontrolle (Outsourcing an Dritte)

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

Technische Maßnahmen	Organisatorische Maßnahmen
	<input checked="" type="checkbox"/> Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	<input checked="" type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit)
	<input checked="" type="checkbox"/> Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
	<input checked="" type="checkbox"/> Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	<input checked="" type="checkbox"/> Regelung zum Einsatz weiterer Subunternehmer
	<input checked="" type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	<input checked="" type="checkbox"/> Bei längerer Zusammenarbeit: Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus

Weitere Maßnahmen:

Unterzeichnung von Auftragsverarbeiter-Vereinbarungen mit cloud-Systemherstellern (vTiger Systems India Pvt Ltd, Google Inc., Microsoft Corporation)

Datenschutzbeauftragter

Name Michael Neumüller
Email datenschutz@dig.at

Ort, Datum
Linz, 16.02.2021