dig.at

DIG

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

Der aktuelle Stand findet sich stets auf der DIG-Homepage unter folgendem Link:
https://dig.at/de/Datenschutz

DIG GmbH
Wildbergstraße 32 | 4040 Linz | Tel. +43 732 615 119 0 | office@dig.at
UID-Nr. ATU53309209 | Firmenbuch: FN217243a | Landesgericht Linz

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**
☒ Manuelles Schließsystem	☒ Schlüsselregelung / Liste
☒ Sicherheitsschlösser	☒ Besucher in Begleitung durch Mitarbeiter
☒ Türen mit Knauf Außenseite	☒ Sorgfalt bei Auswahl Reinigungsdienste

Technische Maßnahmen am Standort Datacenter Wien

Technische Maßnahmen	**Organisatorische Maßnahmen**
☒ Alarmanlage	☒ Schlüsselregelung / Liste
☒ Automatisches Zugangskontrollsystem	☒ Empfang / Rezeption / Pförtner
☒ Chipkarten / Transpondersysteme	☒ Besucherbuch / Protokoll der Besucher
☒ Sicherheitsschlösser	☒ Mitarbeiter- / Besucherausweise
☒ Absicherung der Gebäudeschächte	☒ Besucher in Begleitung durch Mitarbeiter
☒ Türen mit Knauf Außenseite	☒ Sorgfalt bei Auswahl des Wachpersonals
☒ Videoüberwachung der Eingänge	☒ 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
☒ Login mit Benutzername + Passwort	☒ Verwalten von Benutzerberechtigungen
☒ Anti-Viren-Software Server	☒ Erstellen von Benutzerprofilen
☒ Anti-Virus-Software Clients	☒ Zentrale Passwortvergabe
☒ Anti-Virus-Software mobile Geräte	☒ Richtlinie „Sicheres Passwort“
☒ Firewall	☒ Richtlinie „Löschen / Vernichten“
☒ Intrusion Detection SystemeIntrusion Detection Systeme	☒ Richtlinie „Clean desk“
☒ Einsatz VPN bei Remote-Zugriffen	☒ Allg. Richtlinie Datenschutz und / oder Sicherheit
☒ Verschlüsselung von Datenträgern	☒ Mobile Device Policy
☒ Verschlüsselung Smartphones	☒ Anleitung „Manuelle Desktopsperre“
☒ Automatische Desktopsperre	☒ Berechtigungen werden nach dem Minimal-prinzip vergeben und dokumentiert. Eine Überprüfung findet regelmäßig statt.
☒ Verschlüsselung von Notebooks / Tablet	☐

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
☒ Aktenschredder (mind. Stufe 3, cross cut)	☒ Einsatz Berechtigungskonzepte
☒ Physische Löschung von Datenträgern	☒ Minimale Anzahl an Administratoren
☒ Protokollierung von Zugriffen auf Anwendungen, konkret bei der Eingabe, Änderung und Löschung von Daten	☒ Verwaltung Benutzerrechte durch Administratoren
☒ Sämtliche Datenträger sind im Rechenzentrum der A1 Telekom gesichert.	☒ Mitarbeiter sind angewiesen, Daten nur nach dienstlicher Notwendigkeit zu verwenden.
☒ 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
☒ Trennung von Produktiv- und Test-umgebung	☒ Steuerung über Berechtigungskonzept
☒ Physikalische Trennung (Systeme / Datenbanken / Datenträger)	☒ Festlegung von Datenbankrechten
☒ 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
	☒ Interne Anweisung, personenbezogene Daten im Falle einer Weitergabe oder auch nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren / pseudonymi-sieren

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
☒ Email-Verschlüsselung	☒ Dokumentation der Datenempfänger sowie der Dauer der geplanten Überlassung bzw. der Löschfristen
☒ Einsatz von VPN	☒ Übersicht regelmäßiger Abruf- und Übermittlungsvorgängen
☒ Protokollierung der Zugriffe und Abrufe	☒ Sorgfalt bei Auswahl von Transport-Personal und Fahrzeugen
☒ Bereitstellung über verschlüsselte Verbindungen wie sftp, https	☒ Persönliche Übergabe mit Protokoll
☒ Nutzung von Signaturverfahren	
☒ 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
☒ Technische Protokollierung der Eingabe, Änderung und Löschung von Daten	☒ Übersicht, mit welchen Programmen welche Daten eingegeben, geändert oder gelöscht werden können
☒ Eine Änderung der Daten ist in der Applikation nicht vorgesehen.	☒ Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
	☒ 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
☒ Feuer- und Rauchmeldeanlagen	☒ Backup & Recovery-Konzept (ausformuliert)
☒ Feuerlöscher Serverraum	☒ Kontrolle des Sicherungsvorgangs
☒ Serverraumüberwachung Temperatur und Feuchtigkeit	☒ Regelmäßige Tests zur Datenwiederherstellung und Protokollierung der Ergebnisse
☒ Serverraum klimatisiert	☒ Aufbewahrung der Sicherungsmedien an einem sicheren Ort außerhalb des Serverraums
☒ USV	☒ Keine sanitären Anschlüsse im oder oberhalb des Serverraums
☒ Schutzsteckdosenleisten Serverraum	☒ Existenz eines Notfallplans (z.B. BSI IT-Grundschutz 100-4)
☒ RAID System / Festplattenspiegelung	☒ Getrennte Partitionen für Betriebssysteme und Daten
☒ Videoüberwachung Serverraum	
☒ 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 exisitiert 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
☒ Zentrale Dokumentation aller Verfahrens-weisen und Regelungen zum Datenschutz mit Zugriffsmöglichkeit für Mitarbeiter nach Bedarf / Berechtigung (z.B. Wiki, Intranet …)	☒ Interner / externer Datenschutzbeauftragter Name / Firma / Kontaktdaten Mag. (FH) Jakob Eidenberger datenschutz@dig.at
☒ Eine Überprüfung der Wirksamkeit der Technischen Schutzmaßnahmen wird mind. jährlich durchgeführt	☒ Mitarbeiter geschult und auf Vertraulichkeit/ Datengeheimnis verpflichtet
	☒ Regelmäßige Sensibilisierung der Mitarbeiter (mindestens jährlich)
	☒ Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt
	☒ Die Organisation kommt den Informations-pflichten nach Art. 13 und 14 DSGVO nach

5.2. Incident-Response-Management

Unterstützung bei der Reaktion auf Sicherheitsverletzungen

Technische Maßnahmen	Organisatorische Maßnahmen
☒ Einsatz von Firewall und regelmäßige Aktualisierung	☒ Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen / Daten-Pannen (auch im Hinblick auf Meldepflicht gegenüber Aufsichtsbehörde)
☒ Einsatz von Spamfilter und regelmäßige Aktualisierung	☒ Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen
☒ Einsatz von Virenscanner und regelmäßige Aktualisierung	☒ Einbindung von ☒ DSB und ☐ ISB in Sicherheitsvorfälle und Datenpannen
☒ Intrusion Detection System (IDS)	☒ Dokumentation von Sicherheitsvorfällen und Datenpannen z.B. via Ticketsystem
☒ 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
☒ Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind	☒ Einfache Ausübung des Widerrufrechts 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
	☒ Vorherige Prüfung der vom Auftragnehmer getroffenen Sicherheitsmaßnahmen und deren Dokumentation
	☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (gerade in Bezug auf Datenschutz und Datensicherheit
	☒ Abschluss der notwendigen Vereinbarung zur Auftragsverarbeitung bzw. EU Standard-Vertragsklauseln
	☒ Vereinbarung wirksamer Kontrollrechte gegenüber dem Auftragnehmer
	☒ Regelung zum Einsatz weiterer Subunternehmer
	☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags
	☒ 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 Mag. (FH) Jakob Eidenberger
Email datenschutz@dig.at

Ort, Datum
Linz, 23.5.2018