Anlage zur Dokumentation der technischen und organisatorischen Maßnahmen (gem. Art. 32 DSGVO)

1. Präambel

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, treffen der Auftraggeber und der Auftragnehmer die nachfolgenden technischen und organisatorischen Maßnahmen (TOM). Diese gelten für die im Hauptvertrag definierten Leistungen. Bei der Auswahl der Maßnahmen wurden die vier Schutzziele des Art. 32 Abs. 1 b) DSGVO, namentlich die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme, berücksichtigt. Alle technischen und organisatorischen Maßnahmen werden regelmäßig gemäß Art. 32 Abs. 1 d) DSGVO auf ihre Wirksamkeit hin geprüft.

2. Fähigkeit der Vertraulichkeit

Vertraulichkeit heißt, dass personenbezogene Daten vor unbefugter Preisgabe geschützt sind.

Maßnahmen:

-Individuelle Zutrittsberechtigungen gewährleisten den Zutritt zu den gespeicherten Daten nur für autorisierte Personen, sowohl in unseren Büroräumlichkeiten, als auch digital auf den Servern / der Cloud.
-Digitale Zutrittskontrollsysteme durch Chipkarten / Transponder
-Dokumentationen von Zutrittsberechtigungen
-Automatisches Zuziehen und Verschließen von Türen
-Schließung aller Gebäudeeingänge, wie Fenster und Türen
-Büroräume außerhalb der Arbeitszeit sind verschlossen
-Zusätzliche Zugangsbeschränkung und Sicherung des Serverraums
-Protokollierung von Benutzer relevanten Aktivitäten (Anmeldung, Pause, Abmeldung)
-Schutz der Infrastruktur durch Einbruchmeldeanlagen
-W-LAN Verschlüsselung
-Regelmäßige Softwareupdates
-Benutzerauthentifizerung mit Passwortschutz für Systemzugang, Benutzerkonten und Anwendungszugriffe auf Server erforderlich
-Automatische Deaktivierung von Benutzern nach mehreren fehlgeschlagenen Logins
-Erforderliche Mindestkomplexität für Kennwörter
-Verschlüsselte Speicherung von Passwörtern
-Nutzung eines Aktenvernichters (gem. DIN 32757)

3. Fähigkeit der Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf “Daten” angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind.

Maßnahmen:

-Rollenbasiertes Berechtigungskonzept (Lesen, Schreiben, Ändern, Kopieren, Löschen)
-Dokumenation der Vergabe von Zugriffsrechten
-Strenge administrative Aufgabentrennung
-Logische Datentrennung: Separate Datenbanken oder strukturierte Dateiablage
-Spezifische Genehmigungsregelung für die Datenbank und den Anwendungszugriff / Berechtigungskonzept

4. Fähigkeit der Verfügbarkeit

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

Maßnahmen:

-Schutz der Infrastruktur durch Hardware-Firewalls
-Software-Firewall
-Antivirus Software auf allen Systemen
-Kontrollierter Zugang zu E-Mails und Internet
-Trennung von Anwendungs- und Administrationszugängen
-Zugriffsregelungen und Zugriffsverwaltung
-Überspannungsschutz der Gebäudeaußenhaut gegen Blitzeinschlag
-Feuermelder / Rauchmelder
-Sollte es wider Erwarten zu einer Rauchentwicklung oder gar einem Brand kommen, stoppt das Lüftungssystem automatisch die Luftzufuhr
-Regelmäßige Backups und Datensicherung
-Geräte zur Überwachung der Temperatur

5. Verfahren zur regelmäßigen Überprüfung

Wie wird gewährleistet, dass die genannten Datensicherungsmaßnahmen regelmäßig überprüft werden?

Maßnahmen:

-Regelmäßige Überprüfung der Systemzugangsberechtigungen
-Interne Audits
-Disziplinarmaßnahmen im Falle einer Datenschutzverletzung
-Regelmäßige Kontrolle externer Dienstleister

6. Schutz vor unrechtmäßigem Zugang zu personenbezogenen Daten

Wie wird verhindert, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können?

Maßnahmen:

-Kontrollierter Zugang zu E-Mails und Internet
-Regelmäßige Sicherheitsupdates
-Verbot der Nutzung von privaten Datenträgern
-Verbot der privaten Internetnutzung
-Rollenabhängige Zugriffsbeschränkungen

7. Verarbeitung personenbezogener Daten nur nach Anweisung

Wie wird gewährleistet, dass personenbezogene Daten nur entsprechend den Weisungen des Verantwortlichen verarbeitet werden?

Maßnahmen:

-Schriftliche Verpflichtung aller Mitarbeiter auf die Wahrung der Vertraulichkeit
-Regelmäßige Datenschutz Unterweisung der Mitarbeiter
-Geregeltes Löschen / Entsorgen von Datenträgern wie Festplatten, CDs, DVDs, USB Sticks
-Datentransfer und Weitergabe in enger Abstimmung mit dem Auftraggeber
-Datenschutzkonforme Löschung aller Datenkopien und Sicherungen nach Abschluss des Auftrags
-Verarbeitung personenbezogener Daten erfolgt ausschließlich entsprechend den Weisungen des Auftraggebers
-Subunternehmer werden auf die gleichen Regelungen und Bestimmungen verpflichtet wie die digiskill GmbH selbst

8. Anonymisierung / Pseudonymisierung / Verschlüsselung

Anonymisierung, Pseudonymisierung oder Verschlüsselung von Daten des Auftraggebers sind grundsätzlich nicht Gegenstand der von der digiskill GmbH zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.

9. Belastbarkeit der Systeme

Die digiskill GmbH unternimmt die unter Ziffer 4 dargestellten Maßnahmen um eine Belastbarkeit der Systeme sicherzustellen. Penetrationstests der IT-Systeme des Auftraggebers sind grundsätzlich nicht Gegenstand der von der digiskill GmbH zu erbringenden Leistung, sofern hierzu im Hauptvertrag keine gesonderten Vereinbarungen getroffen wurden.