Inhaltsverzeichnis

1 Einleitung

Die EU-Datenschutzgrundverordnung (DSGVO) enthält Vorgaben darüber, wie in technischer und organisatorischer Hinsicht mit personenbezogenen Daten umgegangen werden soll. Dies dient dem Ziel der Datensicherheit. Die Datensicherheit stellt damit einen weiteren und ergänzenden Aspekt des Datenschutzes dar.

Gesetzlich geregelt ist die Datensicherheit in Art. 32 Abs. 1 DSGVO. Diese Vorschriften fordern, dass solche technischen und organisatorischen Maßnahmen zu treffen sind, die erforderlich sind, um den Schutz personenbezogener Daten zu gewährleisten.

Die DSGVO nennt verschiedene Kontrollbereiche, die jeweils noch verschiedene Unterpunkte beinhalten:

(1) Vertraulichkeit

(2) Integrität

(3) Verfügbarkeit und Belastbarkeit

(4) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

(5) Pseudonymisierung und Verschlüsselung

Diese Maßnahmen stellen wir in der Folge vor, um unseren Informationspflichten aus Art. 28 Abs. 3 lit. C nachzukommen.

2 Organisatorisches

Die Intobis GmbH & Co. KG gewährleistet die schriftliche Dokumentation des aktuellen Datenschutzniveaus, sowie der schriftlichen Arbeitsanweisungen, Richtlinien und Merkblätter für Mitarbeiter. Die bei der Datenverarbeitung eingesetzten Mitarbeiter sind auf das Datengeheimnis bzw. auf die Vertraulichkeit verpflichtet.

3 Sicherungsmaßnahmen

Die folgenden Punkte beschreiben die technischen und organisatorischen Maßnahmen, die von der Intobis GmbH & Co. KG betrieben werden.

3.1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

3.1.1 Zutrittskontrolle

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

- Automatisches Zugangskontrollsystem
- Chipkarten-/Transponder-Schließsystem
- Sicherheitsschlösser mit Schlüsselregelung
- Lichtschranken/Bewegungsmelder
- Protokollierung Besucher/Besucherbuch
- Alarmanlage
- Videoüberwachung der Zugänge
- Server der Intobis GmbH & Co. KG werden im Rechenzentrum RIZ IT-Motion GmbH verwaltet Zugang via VPN nur mit persönlichen Zugangsdaten möglich
- Zutrittskontrollanlage vorhanden
- Auswertung protokollierter Daten nach (versuchten) Sicherheitsverletzungen
- 2 Factor Schließsystem
- einbruchhemmende Maßnahmen

3.1.2 Zugangskontrolle

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

- Formale Benutzer-Registrierung und Deregistrierung für Informationssysteme und Dienste zur Vergabe und Rücknahme von Zugangsberechtigungen
- Mandanten- und Benutzerverwaltung mit abgestufter Rechtevergabe
- Eine eindeutige Zuordnung von Benutzerkonten zu Benutzern ist möglich.
- Admin und User werden namentlich, eindeutig zugeordnet.
- Ein verbindliches Verfahren zur Vergabe von Berechtigungen ist implementiert.
- Unbefugten wird der Zugang auf das Unternehmensnetzwerk verwehrt. Nur bekannte/registrierte Geräte können sich anmelden. Eine Anmeldung ist nur möglich, wenn Benutzerkonto und Passwort bekannt sind.
- Einsatz von VPN-Technologie
- Zugriff auf Software über VPN mit 2-Phasen-Authentifikation (Benutzernamen/Passwort)
- Explizite Freigabe von Zugriffsrechten
- Zugang zu Netzdiensten und Netzwerkkomponenten nur von ausdrücklich Befugten

- Einsatz von Intrusion-Detection-Systemen
- Verschlüsselung von Datenträgern in Laptops/Notebooks
- Einsatz Anti-Viren-Software
- Einsatz Software-Firewall
- Einsatz Hardware-Firewall
- Reduktion zugriffsberechtigter Personen auf ein Minimum
- Automatische Bildschirmsperren (passwortgeschützt)
- Netzwerkmonitoring mit Alarmierung

3.1.3 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.

- Die Einschränkung der Zugriffsmöglichkeiten des zur Benutzung eines DV-Systems Berechtigten ausschließlich auf die seiner Zugriffsberechtigung unterliegenden Daten wird gewährleistet durch:
  - Organisationsanweisung für Mitarbeiter, freie Mitarbeiter und Unterauftragnehmer
  - Die Vergabe, der Entzug und die Änderung von Berechtigungen (Benutzerverwaltung) ist nachvollziehbar.
  - Differenzierte Zugriffsberechtigung auf Anwendungsprogramme.
  - Differenzierte Verarbeitungsmöglichkeiten (Lesen/Ändern/Löschen).
  - Eingeschränkte Domänenfunktionen.
  - Abgestufte Zugriffsrechte mit Logging/Protokollierung
  - Softwareseitigen Ausschluss (Berechtigungskonzept)
  - Einschränkung Zugriffsmöglichkeiten der Benutzer
  - Restriktive Zugriffsberechtigung/projektbezogene Zugänge
  - Unterschiedliche Userarten
  - Herausgabe u. Erstellung von Hardware/Datenträgern obliegt Genehmigung der Geschäftsführung

3.1.4 Trennungsgebot

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

- Softwareseitiger Ausschluss (Mandantentrennung)
- Datenbankprinzip, Trennung über Zugriffsregelung
- Trennung von Test- und Produktivdaten
  Separierung auf Testdatenbank, um Software-Weiterentwicklung vor dem Einsatz auf dem Echtsystem auf der Testdatenbank zu prüfen
- Funktionstrennung
- Berechtigungskonzept und Datenbankrechte
- Auf der Anwenderebene wird zwischen verschiedenen Userarten mit unterschiedlichen Zugriffsrechten (Nutzerprofil) unterschieden.

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

3.2.1 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.

- Ein Versand physischer Datenträger ist verboten bzw. erfolgt nur auf explizite Anfrage des Auftraggebers.
- VPN-Zugänge für mobile Arbeitsplätze/Heimarbeitsplätze der Software-Entwickler.
- Verpflichtung Mitarbeiter, freier Mitarbeiter, Unterauftragnehmer auf Datengeheimnis und Vertraulichkeit.
- Jährliche, regelmäßige Datenschutzschulung Mitarbeiter, freier Mitarbeiter u. Unterauftragnehmer
- Fortbestehen der Verpflichtung auf Vertraulichkeit nach Ausscheiden
- Verfügung sofortiger Freistellung u. Sperrung aller Zugänge der Nutzerprofile
- Die Software ist grundsätzlich SSL-verschlüsselt. Sofern eine Verschlüsselung der Software aufgrund Kompatibilitätsproblemen mit anderen Programmen des Auftraggebers nicht eingesetzt wird, kann die Software auch unverschlüsselt genutzt werden. Eine Umstellung auf SSL-Verschlüsselung wird empfohlen und kann vom Auftraggeber in der Software eigenständig umgesetzt werden.

3.2.2 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.

- Ob und von wem Daten in DV-Systeme eingegeben, verändert oder entfernt worden sind, kann nachträglich überprüft und festgestellt werden durch:
    - Benutzerprofile.
    - Benutzeridentifikation.
    - Berechtigungskonzepte
    - Protokollierung über Active Directory.
    - Firewall-Protokollierung (TCP/IP).
    - Zugriffsprotokollierung im Rahmen von (Fern-) Wartungstätigkeiten
    - Auf Anwenderebene wird zwischen verschiedenen Userarten mit unterschiedlichen Zugriffsrechten (Nutzerprofil) unterschieden.
    - Protokollierung eingegebener Daten (Verarbeitungsprotokoll).

3.3 Verfügbarkeit, Belastbarkeit und rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind und bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Schutz der Daten gegen zufällige Zerstörung oder Verlust:

- Einsatz unterbrechungsfreie Stromversorgung inkl. Überspannungsschutz und Notstromaggregat
- Feuer-/Rauchmeldeanlage
- Blitzschutzeinrichtungen
- Einsatz Klimaanlage inkl. Dokumentation Klimatechnik
- Verteilung Netzwerkkomponenten zum Zweck der Risiko-/Ausfallminimierung auf mehrere geschützte Bereiche
- Überwachung Raumtemperatur/Luftfeuchtigkeit etc.
- Alarmanlage inkl. Weiterleitung an Leitstelle, Werkschutz, Feuerwehr, Wachdienst etc.
- Backupdaten werden in separaten Brandabschnitt aufbewahrt. Es werden komplette Images der Server erstellt.
- Backup-/Recovery-Konzept vorhanden (siehe TOMs RIZ IT-Motion GmbH – Rechenzentrum)
- Notfallhandbuch/Notfallkonzept vorhanden (siehe TOMs RIZ IT-Motion GmbH – Rechenzentrum)

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

3.4.1 Datenschutz-Management

Die Einführung eines Datenschutz-Managementsystem (DSMS) ist geplant und wird zeitnah erfolgen. Das DSMS wird vom Unternehmen geführt und beinhaltet die wichtigsten datenschutzrechtlichen Vorgaben und eine umfassende Struktur zur Abbildung der Datenschutzmaßnahmen.

3.4.2 Incident-Response-Management

Ein prozessualisierter Umgang mit Sicherheitsvorfällen ist implementiert. Im Falle eines Vorfalls informieren die Mitarbeiter die IT bzw. ihren Vorgesetzten unverzüglich. Im Anschluss erfolgt die Abstimmung mit dem Datenschutzbeauftragten. Die Bearbeitung durch diesen ist durch entsprechende Vertretungsregelungen sichergestellt.

3.4.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Grundsätzlich werden nur Daten erhoben und verarbeitet, die für die Geschäftszwecke zweckmäßig und erforderlich sind. Verfahren der automatisierten Datenerfassung- und -verarbeitung sind so gestaltet, dass nur die erforderlichen Daten erhoben werden können.

3.4.4 Auftragskontrolle

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

Mitarbeiter, die als Administratoren Zugriff auf die Systeme haben, sind alle hinsichtlich des Datenschutzes belehrt, auf das Datengeheimnis verpflichtet und haben als Bestandteil ihres Arbeitsvertrags entsprechende Verschwiegenheits- und Geheimhaltungsvereinbarungen akzeptiert.

Sollte die Intobis GmbH & Co. KG bei der Datenverarbeitung Unterauftragnehmer einsetzen, werden bestimmte Vorgaben umgesetzt. Hierzu zählt die Sicherstellung der technisch-organisatorischen Maßnahmen der Unterauftragnehmer im Sinne des Art. 28 Abs. 3 lit. c DSGVO und Art. 32 Abs. 1 DSGVO.

Voraussetzungen für das Eingehen eines Unterauftragsverhältnisses:

- Es bestehen detaillierte Angaben über Zweck, Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers nach Vorgabe des Art. 28 Abs. 3 DSGVO. Die entsprechenden Angaben sind vertraglich fixiert.
- Auswahl der Auftragsverarbeiter unter festen Sorgfaltsgesichtspunkten (insbesondere Datensicherheit).
- Bestellung eines Datenschutzbeauftragten beim Auftragsverarbeiter soweit gesetzlich vorgeschrieben.
- Verpflichtung der Mitarbeiter der Auftragsverarbeiter auf die Vertraulichkeit.
- Restriktive Zugriffsberechtigungen

- Auf die betreffenden technischen Umgebungen werden nur restriktive Zugriffsberechtigungen vergeben. Bei externem Zugriff auf das System wird der Zugang nach Beendigung der Zusammenarbeit deaktiviert oder gesperrt.

3.5 Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

- Zugriff auf Daten innerhalb der Software erfolgt i.d.R. über verschlüsselte Zugangsverfahren.
- Mailanhänge mit personenbezogenen Daten werden i.d.R. verschlüsselt verschickt.
- Datenübertragung von der Website über SSL Verschlüsselung.
- Die Software ist grundsätzlich SSL-verschlüsselt. Sofern eine Verschlüsselung der Software aufgrund Kompatibilitätsproblemen mit anderen Programmen des Auftraggebers nicht eingesetzt wird, kann die Software auch unverschlüsselt genutzt werden. Eine Umstellung auf SSL-Verschlüsselung wird empfohlen und kann vom Auftraggeber in der Software eigenständig umgesetzt werden.

3.6 Kooperation mit der Deutschen Datenschutzkanzlei

Zur Einhaltung der datenschutzrechtlichen Vorgaben der datenschutzrechtlichen Vorgaben, arbeitet die Intobis GmbH & Co. KG mit der Deutschen Datenschutzkanzlei zusammen. Neben der Erstellung von Richtlinien und Handlungshilfen, berät die Deutsche Datenschutzkanzlei die Intobis GmbH & Co. KG auf Anfrage in allen Fragen rund um den Datenschutz.

Ansprechpartner der Deutschen Datenschutzkanzlei ist:

Deutsche Datenschutzkanzlei

Büro Bodensee

Richard-Wagner-Straße 2, 88094 Oberteuringen

www.deutsche-datenschutzkanzlei.de

DEUTSCHE DATENSCHUTZ KANZLEI

Maximilian Musch

Magister Artium, geprüfter fachkundiger Datenschutzbeauftragter (udis)

E-Mail: musch@ddsk.de

Tel. 07544 / 904 96 92