Datensicherheit – Appendix B

DSGVO

Die DSGVO schreibt einige Verhaltensregeln und Maßnahmen zum Thema Datensicherheit vor - Maßnahmen sowohl in technischer, als auch organisatorischer Hinsicht.
Personenbezogene Daten müssen in einer nachvollziehbaren Weise verarbeitet werden (***Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz*** – Art. 5, Abs. 1 Ziff. a), sind einer „***Zweckbindung***" unterworfen (Art. 5, Abs. 1, Ziff. b), müssen auf das ***notwendige Maß beschränkt*** sein (***Datenminimierung*** nach Art. 5, Abs. 1, Ziff. c), auf dem ***neuesten Stand*** sein und ***angemessene Maßnahmen für die Korrektur*** bei unrichtiger Daten getroffen werden (***Richtigkeit*** nach Art. 5, Abs. 1, Ziff. d), in einer Form gespeichert werden, die die Identifizierung nur so lange ermöglicht, wie für den Zweck der Verarbeitung notwendig ist (***Speicherbegrenzung*** nach Art. 5, Abs. 1, Ziff. e) sowie in einer Weise verarbeitet werden, die eine ***angemessene Sicherheit der Daten*** gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung (***Integrität*** und ***Vertraulichkeit*** nach Art. 5, Abs. 1, Ziff. f).

Weiters schreibt die DSGVO dem Verantwortlichen die Pflicht zu, ***unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen*** umzusetzen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt (Art. 24, Abs. 1). Zudem sind geeignete Datenschutzvorkehrungen zu treffen (Art. 24, Abs. 2).
Neben dem in Art. 25 Abs. 1 genannten „***Datenschutz durch Technikgestaltung***" (Privacy by Design) ist auch gem. Abs. 2 der „***Datenschutz durch datenschutzfreundliche Voreinstellung***" (Privacy by Default) zu gewährleisten. Dies bedeutet, dass durch Technikgestaltung (z.B. mittels Verschlüsselung oder Pseudonymisierung) die Datenschutzgrundsätze wirksam umgesetzt werden, bzw. dass durch Voreinstellung nur jene Daten erhoben werden, die für den jeweiligen bestimmten Verarbeitungszweck erforderlich sind, sowie den Umfang der Verarbeitung, Speicherfrist und Zugänglichkeit begrenzen.
Die unter Art. 32 Abs. 1 genannten „geeigneten technischen und organisatorischen Maßnahmen" zur Gewährleistung eines dem „Risiko angemessenen Schutzniveaus" schließen unter anderem folgendes ein:

- Pseudonymisierung oder Verschlüsselung der Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Bei der Beurteilung des angemessenen Schutzniveaus sind die mit der Verarbeitung verbundenen Risiken (Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung – ob unbeabsichtigt oder unrechtmäßig) zu berücksichtigen. Zudem stellen der Verantwortliche und der Auftragsverarbeiter sicher, dass ihnen unterstellte Personen nur auf Anweisung des Verantwortlichen Daten verarbeitet werden.

DSG (idF. Datenschutz-Anpassungsgesetz 2018)

Während die DSGVO im Artikel 32, Absatz 1 die Implementierung geeigneter „technischer und organisatorischer Maßnahmen“ fordert, ohne diese zu konkretisieren, enthält §54 Abs. 2 DSG eine detaillierte Aufstellung:
Der Verantwortliche und der Auftragsverarbeiter haben im Hinblick auf die automatisierte Verarbeitung (= IT-gestützte Verarbeitung unter Zuhilfenahme von z.B. Computer, Smartphones, Kameras, Scanner, Kopierer, ...) nach einer Risikobewertung Maßnahmen zu ergreifen, um nachstehende Zwecke zu erreichen.

Zugangskontrolle: Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte

Datenträgerkontrolle: Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern

Speicherkontrolle: Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten

Benutzerkontrolle: Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte

Zugriffskontrolle: Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben

Übertragungskontrolle: Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können

Eingabekontrolle: Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind

Transportkontrolle: Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können

Wiederherstellung: Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können

Zuverlässigkeit und Datenintegrität: Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) und gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität)

Mögliche Maßnahmen zur Umsetzung

Durch welche konkreten Maßnahmen kann die Umsetzung dieser geforderten 10 Zweckvorgaben der Datensicherheit erfüllt werden? Die nachfolgende beispielhafte Zusammenstellung zeigt entsprechende Möglichkeiten auf:

Umsetzung der Zugangskontrolle

Bauliche Maßnahmen:

- Perimeter- (=Außengrenze) und Gebäudesicherung
- Einsatz von Sicherheitsschlössern oder Codeschlössern
- Zutrittskontrolle mittels Chipkartensystem
  Anmerkung: von Biometrischen Zugangskontrollen sei in Bezug auf Art. 9 DSGVO (besondere Kategorien von Daten) und den entsprechend notwendigen höheren Schutzanforderungen abgeraten
- Einbruchshemmende Maßnahmen (Fenster und Türen)
- Alarmanlagen und Videoüberwachung

Technische Maßnahmen (elektr. Zugangskontrolle bei Informationssystemen):

- Formales Verfahren für die An- und Abmeldung von Benutzern
- Verwaltung von Sonderzugangsrechten (z.B.: hochprivilegierte Administratorenkonten)
- Verwendung sicherer Passwörter mit ausreichend hoher Länge und technischer Komplexität

Organisatorische Maßnahmen:

- Anmeldung beim Empfang mit Personenkontrolle
- Tragen von Firmen-/Besucherausweisen
- Begleitung von Besuchern im Unternehmensgebäude
- Wachdienst
- Protokollierung der physischen Zutritte und Abgänge
- Passwortrichtlinie
- Protokollierung der An- und Abmeldungen sowie Anmeldeversuche an Informationssystemen
- Regelmäßige Prüfung von Zugangsberechtigungen (Deaktivieren inaktiver Konten)

Umsetzung der Datenträgerkontrolle

Technische Maßnahmen:

- Einrichtung eines Datenträgerarchivs
- Sichere Aufbewahrung von Speichermedien (versperrte Kästen, Datenträger-Safes)
- Kontrolliertes und dokumentiertes Kopieren
- Verschlüsselung der gespeicherten Daten
- Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger
- Datenschutzgerechte Wiederverwendung von Datenträgern (sichere Löschung von Inhalten bei Weitergabe von Datenträgern)

Organisatorische Maßnahmen:

- Datenträgerverwaltung, Bestandskontrolle
- Protokollierung der autorisierten Weitergabe von Datenträgern
- Kopierkontrolle

Umsetzung der Speicherkontrolle

Technische Maßnahmen:

- Einsatz von Identifikations- und Authentisierungsmaßnahmen der Benutzer

- Bildschirmsperre bei längerer Inaktivität des Benutzers
- Protokollierung des Benutzerverhaltens
- Verschlüsselte Speicherung von Daten
- Trennung von Test- und Produktionsbetrieb

Organisatorische Maßnahmen:

- Protokollierung der Art des Datenzugriffs

Umsetzung der Benutzerkontrolle

Technische Maßnahmen:

- Einsatz von Firewalls, Intrusion-Detection- und -Prevention-Systemen
- Identifikation und Authentifizierung der Benutzer
- Verwendung sicherer Passwörter (Prüfung der Passwortqualität)
- Sicherung der Datenstationen, Netze und Übertragungsleitungen

Organisatorische Maßnahmen:

- Festlegung der nutzungsberechtigen Personen
- Protokollierung der Benutzer und deren Aktivitäten
- Passwortrichtlinie
- Clear-Desk- und Clear-Screen-Policy

Umsetzung der Zugriffskontrolle

Technische Maßnahmen:

- Berechtigungskonzept
- Identifikation und Authentifizierung der Benutzer
- Sicherung der Schnittstellen
- Verschlüsselungsverfahren nach dem Stand der Technik
- Kopierkontrolle
- Abweisung nicht autorisierter Computer- und Endgeräte im Netzwerk
- Automatisierte Überprüfung der Berechtigungen

Organisatorische Maßnahmen:

- Prüfung von Zugriffsberechtigungen der Benutzer
- Entzug oder Anpassung von Zugriffsberechtigungen
- Zeitliche Begrenzung der Zugriffsmöglichkeiten
- Benutzerbezogene Protokollierung der Zugriffe
- Dokumentation von Datenvernichtungsmaßnahmen

Umsetzung der Übertragungskontrolle

Technische Maßnahmen:

- Protokollierung der Datenübermittlungen
- Auswertungsmöglichkeiten der Übermittlungsprotokolle, um die Empfänger oder Abrufenden gezielt feststellen zu können

Organisatorische Maßnahmen:

- Leitlinien und Verfahren für die Informationsübertragung
- Dokumentation der Abruf- und Übermittlungsprogramme
- Festlegung und Dokumentation der Übermittlungswege und der Datenempfänger

Umsetzung der Eingabekontrolle

Technische Maßnahmen:

- Identifikation und Authentifizierung von Benutzern
- Protokollierung der Eingabe, Änderung und Löschung von Daten
- Einsatz von Protokollauswertungssystemen
- Einsatz elektronischer Signaturen

Organisatorische Maßnahmen:

- Definition der zur Eingabe, Änderung und Löschung personenbezogener Daten Berechtigten
- Definition von Plausibilitätskontrollen zur Eingabe, Änderung und Löschung
- Sichere Ablage und fristgerechte Löschung von Protokollen

Umsetzung der Transportkontrolle

Technische Maßnahmen:

- Verschlüsselte Übertragung von Daten
- Verschlüsselte Speicherung von Daten auf Datenträgern
- Sicherung von Zugriffen über verschlüsselte VPN
- Protokollierung der Datenübermittlung
- Duplizierung der Datenträger
- Schutz der Datenübermittlungen und Datenträger vor Schadsoftware (Viren etc.)
- Sicheres Löschen von Daten auf Datenträgern
- Verwendung sicherer Transportbehälter

Organisatorische Maßnahmen:

- Eskalation bei Sicherheitsmeldungen
- Beauftragung zuverlässiger Transportunternehmen
- Dokumentation des Transportweges
- Überwachung der Transportzeit
- Führung eines Datenträger-Eingangs- bzw. Ausgangsbuches

Umsetzung der Wiederherstellung

Technische Maßnahmen:

- Regelmäßige Datensicherung
- Einsatz von RAID-Systemen
- Einsatz von Snapshot-Technologien
- Redundante Basisinfrastruktur (Stromversorgung, Netzwerkversorgung, Klimatisierung...)

Organisatorische Maßnahmen:

- Notfallvorsorgekonzept
- Datensicherungs- und Wiederherstellungskonzept
- Sichere Aufbewahrung der Backup-Datenträger

Umsetzung der Datenintegrität

Technische Maßnahmen:

- Tägliche Sicherung aller relevanten Daten
- Einsatz von Schutzprogrammen (Virenscanner, Firewalls, Verschlüsselungsprogramme, Spam-Filter)
- DDoS-Schutz

- Unterbrechungsfreie Stromversorgung
- Elektronische Signatur

Organisatorische Maßnahmen:

- Datensicherungs- und Wiederherstellungskonzept
- Systemüberwachung aller relevanten IT-Systeme

Protokollierung der Verarbeitung nach §50 DSG

Jeder Verarbeitungsvorgang ist in geeigneter Weise so zu protokollieren, dass die Zuverlässigkeit der Verarbeitung nachvollzogen und überprüft werden kann (§50 Abs. 1).

In automatisierten Verarbeitungssystemen (IT-Systeme) sind alle Verarbeitungsvorgänge gem. §50 Abs. 2 in automatisierter Form zu protokollieren und haben zumindest folgende Protokolldaten zu umfassen:

- Zweck der Verarbeitung
- Die verarbeiteten Daten
- Datum und Uhrzeit der Verarbeitung
- Identifizierung der verarbeitenden Person (Benutzerkennung)
- Identität der allfälligen Empfänger der Daten

In nicht automatisierten Verarbeitungssystemen (analoge Systeme wie Aktenordner, Datenablagen, ...) sind gem. §50 Abs. 3 zumindest nachfolgende Protokollierungen anzufertigen:

- Abfragen und Offenlegungen
- Übermittlung
- Veränderung sowie Löschung

Jedoch bezieht sich §50 Abs. 3 auch auf die Bestimmungen von §50 Abs. 2, weswegen eigentlich auch die Bestimmungen der automatisierten Systeme für die nichtaustomatisierten Systeme gilt.

DISCLAIMER und Verwendungshinweise

Die Autoren weisen ausdrücklich darauf hin, dass die hier vorliegende Unterlage nach Treu und Glauben angefertigt und im Wesen den Inhalt der aktuellen Gesetzgebung wiedergibt, jedoch keine juristische Beratung durch einen eingetragenen Rechtsanwalt ersetzt.

Alle Rechte, insbesondere das Recht der Vervielfältigung und Verbreitung sowie der Übersetzung, ist ausschließlich den Autoren vorbehalten. Kein Teil dieser Unterlage darf in irgendeiner Form (durch Fotokopie, Mikrofilm oder ein anderes Verfahren) ohne schriftliche Genehmigung der Autoren reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Sie erreichen die Autoren unter www.derSchenner.at bzw. www.sevian7.com oder unter der gemeinsamen Projektseite www.dsgvo2018.at.

Die Autoren sind zertifizierte Datenschutz-Experten, zertifizierte IT-Security-Experten und zertifizierte Unternehmensberater. Beide unterrichten auf Fachhochschulen und sind Trainer bei Wifi, Incite und weiteren Bildungsträgern.

CERTIFIED DATA & IT SECURITY EXPERT CMC CERTIFIED DIGITAL CONSULTANT

WIR NEHMEN **WISSEN** IN BETRIEB.