Praxisbeispiel

SICHERHEIT DER VERARBEITUNG
Technische und organisatorische Maßnahmen

Hinweise zur Anwendung

Die Firma XYZ betreibt einen Webshop und hat sich das Angebot der Stiftung Datenschutz zu Herzen genommen und die vorgeschlagenen Maßnahmen so gut es geht eingeplant und umgesetzt. Die nähere Dokumentation zur Umsetzung der einzelnen Maßnahmen erfolgt getrennt und in einem internen Tabellenblatt.

Die Allgemeinen Maßnahmen wurden in einem Dokument festgehalten. **Die Firma kann dieses Dokument nun für folgende Zwecke nutzen:**

1. Im Verzeichnis der Verarbeitungstätigkeiten (VVT) kann auf dieses Dokument verwiesen werden.
2. Für die Kunden stellt Firma XYZ einen eigenen Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO bereit. Dieser enthält das Dokument als Anlage zum AVV.

? **FRAGE EINES FREUNDES:** „Cool, dann ist da ja alles Wichtige drin und ich kann das Musterbeispiel ja einfach für uns nutzen!"

! **ANTWORT:** „Die getroffenen Maßnahmen müssen sich auf **Ihre individuelle** Datenverarbeitungssituation beziehen und unter Berücksichtigung verschiedener Faktoren getroffen werden. Die DSGVO macht außerdem keine Angaben dazu, WELCHE Maßnahmen getroffen und WIE diese umgesetzt werden sollen. Aus diesem Grunde stehen sehr viele unterschiedliche Informationen und Checklisten von verschiedenen Anbietern im Internet zur Verfügung.

Auch die Form der Darstellung von TOM bleibt offen. Sie können eine Tabelle erstellen, eine Fließtextform wählen oder die Maßnahmen im Verzeichnis der Verarbeitungstätigkeiten (VVT) mit aufführen.

Wichtig ist in jedem Fall, dass die Maßnahmen auf die konkreten Tätigkeiten und Gegebenheiten Ihrer Organisation abgestimmt sind. Daher können bestehende Checklisten immer nur als Beispiel und Muster dienen, aber eine individuelle Befassung mit dem Thema niemals ersetzen."

Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit bei der Verarbeitung von personenbezogenen Daten gemäß Artikel 32 DSGVO

Allgemeine organisatorische Maßnahmen

- für Datenschutzangelegenheiten haben wir eine feste Ansprechperson kommuniziert
- IT-Angelegenheiten haben wir eine feste Ansprechperson kommuniziert
- Durchführung von regelmäßigen Datenschutz-Schulungen
- Schriftliche Verpflichtung der Beschäftigten auf Vertraulichkeit bei der Verarbeitung von personenbezogenen Daten,
- Anweisungen zum Datenschutz an Beschäftigte,
- Anweisungen zum Arbeiten im Home-Office,
- Vorhalten einer Passwort-Richtlinie,
- sorgfältige Auswahl und Prüfung von Auftragsverarbeitern,
- Interne Vorgaben zur Umsetzung von datenschutzfreundlichen Prinzipien, wie:
  Datenminimierung
  Umsetzung und Kontrolle des Berechtigungskonzeptes
  Pseudonymisierung, Sperrung von Daten

Maßnahmen zur Vertraulichkeit (Zutritts-, Zugangs- und Zugriffsbeschränkungen)

Technische/Physische Maßnahmen

- Schlüssel, Sicherheitsschlösser an allen Türen und Fenstern
- Abschließbare Türen und Schränke
- Sichtschutz an Fenstern und Monitoren
- Kopiergerät/Drucker/Fax sind in geschützten Bereichen aufgestellt
- Diskretionsabstände im Eingangs
- Alarmanlage mit Aufschaltung an einen Wachdienst
- Videokamera am Eingang zum Bürokomplex durch Vermieter
- Passwortschutz
- 2-Faktor-Authentifizierung
- Differenzierung zwischen administrativen Nutzerkonten und Sachbearbeitern

Organisatorische Maßnahmen

- Berechtigungsvorgaben: Wer benötigt welche Schlüssel, wer hat Zugang zu PCs und IT-Systemen, wer darf welche Softwareanwendungen nutzen und auf Videoaufzeichnungen oder IT-Protokolldaten zugreifen
- Entziehung von Zugriffsberechtigungen bei Ausscheiden eines Beschäftigten
- Regelmäßige Kontrolle der Zugriffsberechtigungen
- Möglichkeiten zur Kontrolle der Zugriffe bei Verdachtsfällen geschaffen

Maßnahmen zur Integrität

Technische/Physische Maßnahmen

- Sichere Übertragungsstandards bei Formularen auf Websites nach dem Stand der Technik
- Sicherheitszertifikate für Websites
- Double-Opt-in-Verfahren bei Newslettern
- Veränderungssperre in Datenbank und Dokumenten

Organisatorische Maßnahmen

- Einkauf von neuer Software, welche die Anforderungen der DSGVO berücksichtigt (u. a. Umsetzung von Lösch- und Sperrvermerken, Berechtigungsvergaben, Protokollierungsmöglichkeiten, differenziertes Lizenzmodell)
- Schulungen zum richtigen Umgang mit neuer Software und den Gefahren von Datenmanipulationen
- Differenziertes Berechtigungskonzept innerhalb einer Softwareanwendung
- Einsatz eines Hash-Verfahrens, um Manipulation an Daten zu erkennen
- Ausreichende Lizenzen bei relevanten Softwareanwendungen

Maßnahmen zur Verfügbarkeit

Technische/Physische Maßnahmen

- Datenspeicherungen (Back-ups)
- Daten sind redundant an mehreren Orten gespeichert
- Regelmäßiges Kontrollieren der Back-Ups
- Regelmäßige Tests zur Wiederherstellung von Daten im Ernstfall

Organisatorische Maßnahmen

- Konzept und Vorgabe zur Speicherung von Daten
- Back-up-Konzept für die Datensicherung
- Erstellen eines Notfallplans, für den Ernstfall
- Abschluss einer Cyberversicherung
- fachmännische Hilfe über abgeschlossene Cyber-Versicherung

Maßnahmen zur Belastbarkeit

Technische/Physische Maßnahmen

- Server in sicheren, geschützten, trockenen, klimatisierten Umgebungen
- Regelmäßiger Belastungstest, Stresstest (/Penetrationstest/Pentest)
- Erkennen von Systembelastungen
- Ausreichend Speicher und Verarbeitungskapazitäten vorhalten
- Regelmäßiges Patchen und Updaten der IT-Systeme und Software
- Einsatz von Hard- und Software, die dem aktuellen Stand der Technik entspricht

Organisatorische Maßnahmen

- Einplanung von Zeiten mit hoher Belastung
- Einkauf von Hard- und Software mit laufendem Support für Patching und IT-Helpdesk