D_07a Technisch organisatorische Maßnahmen

Im Zuge der Umsetzung der DSGVO-Vorgaben wird von Unternehmen erwartet dafür Sorge zu tragen, dass die Datensicherheit bei der Verarbeitung von personenbezogenen Daten gewährleistet ist.

Zum Schutz von personenbezogenen Daten haben die Verantwortlichen und Auftragsverarbeiter die Grundsätze des Datenschutzes schon in Ihre Anwendungen zu integrieren (privacy by design) und datenschutzfreundliche Voreinstellungen zu verwenden (privacy by default).

Für die Umsetzung technisch/organisatorischer Maßnahmen gelten folgende Grundsätze:

- **Sicherheit**: Daten müssen gegen unbefugten Zugriff durch technische und organisatorische Maßnahmen geschützt sein.
- **Vertraulichkeit**: personenbezogene Daten dürfen niemand anderem, als im eigentlichen Zweck vorgesehen, zur Verfügung gestellt werden, bzw. muss verhindert werden, dass jemand anderer darauf Zugriff erhält.
- **Integrität**: Datensätze dürfen nicht fälschlicherweise verändert werden. Es muss die Korrektheit gewährleistet werden.
- **Verfügbarkeit**: Die Systeme und Dienste müssen verfügbar bleiben. Sie dürfen nicht unwiederbringlich verloren gehen durch Systemabsturz oder Verlust eines Ordners.

Zusätzliche sollen Unternehmen Verfahren zur laufenden Überprüfung, Bewertung und Evaluierung der Wirksamkeit der festgelegten Maßnahmen zur Gewährleistung der Sicherheit entwickeln.

Folgende Maßnahmen können Sie beispielsweise zur Umsetzung der technischen Sicherheit heranziehen:

- Virenschutz
- Firewall
- Passwortregelungen
- Berechtigungskonzept
- Regelmäßige Datensicherung
- Verschlüsselung von E-Mails
- Verwendung von VPNs
- Protokollierung von Zugriffen
- Blocken von Funktionen (USB-Ports oä)
- Pseudonymisierung und Verschlüsselung von personenbezogenen und sensiblen Daten

Folgende Sicherheitsanwendungen können Sie beispielhaft zur Umsetzung von organisatorischen Maßnahmen heranziehen:

- Mitarbeiter bezüglich IT-Sicherheit schulen
- Richtlinien zur sicheren Nutzung von sozialen Medien
- Freiwillige/r Datenschutzbeauftragte/n
- IT-Sicherheitsbeauftragte/n
- Zugangskontrollen zu sensibler Hardware (zB Server)
- Notfallpläne für IT-Sicherheitsvorfälle
- Richtlinie zur sicheren Nutzung von IT und Internet

Die für Datenschutz verantwortliche Person hat dafür zu sorgen, dass geeignete technische und organisatorische Maßnahmen festgelegt werden die sicherstellen, dass durch Voreinstellungen nur die personenbezogenen oder sensiblen Daten verarbeitet werden können, deren Verarbeitung für den jeweiligen Verarbeitungszweck vorgesehen und erforderlich sind. Ein möglicher Nachweis der Einhaltung kann durch genehmigte Zertifizierungsverfahren stattfinden.

Sollten die Verpflichtungen zu den Datensicherheitsmaßnahmen sowie die Erfordernisse nach Datenschutz durch Technik (privacy by design) und datenschutzfreundlichen Voreinstellungen (privacy by default) verletzt werden, können Strafen von bis zu EUR 10 Mio oder 2 % des letztjährigen weltweiten Umsatzes verhängt werden.

In unserem Unternehmen sind die folgenden technischen und organisatorischen Maßnahmen vorhanden:

Maßnahme	**Technisch/organisatorisch**
Beispiel: Virenscanner	Technisch
Beispiel: versperrter Schrank für Personalakten	Technisch
Beispiel: Anweisung zur Verwahrung von Personalakten	Organisatorisch
Beispiel: Berechtigungskonzept mit Rollen die den Zugriff auf die Daten beschränken	Organisatorisch mit technischer Umsetzung

Hinweis: Dieses Muster dient der beispielsweisen Umsetzung der Regelungen der DSGVO in Bezug auf den Datenschutmanager im Unternehmen. Dieses ist an die Bedürfnisse des jeweiligen Unternehmens individuell anzupassen.

Dieses Muster wurde mit größter Sorgfalt erstellt, für die Richtigkeit, Vollständigkeit, Aktualität oder Qualität des bereitgestellten Musters können wir jedoch keine Gewähr übernehmen. Haftungsansprüche gegen Personen, welche dieses Muster erstellt haben, sind daher ausgeschlossen.