Industrie- und Handelskammer
Osnabrück - Emsland - Grafschaft Bentheim

Was verlangt die EU-DSGVO als Datenschutzmanagement? (Merkblatt Nr. 3)

Vorbemerkungen

Die EU-Datenschutz-Grundverordnung (DS-GVO) verlangt von den Unternehmen die Erfüllung der Rechenschaftspflicht. Damit ist die verantwortliche Stelle, also das Unternehmen oder die Institution, verantwortlich für den Datenschutz und seine Beachtung. Dazu ist ein Datenschutzmanagement notwendig – natürlich abhängig von der Größe des Unternehmens, der personenbezogenen Daten, die verarbeitet werden, und der Menge und der Qualität der Daten. Zumindest muss aber auch in kleineren und mittleren Unternehmen ein Mindestmaß an Dokumentation vorhanden sein, um die Einhaltung des Datenschutzes nachweisen zu können. Denn die Verletzung der Datenschutzpflichten zieht empfindliche Bußgelder nach sich: bis zu 20 Mio. Euro oder 4 % des weltweiten Umsatzes können von den Aufsichtsbehörden verhängt werden.

Was verlangt ein Datenschutzmanagement?

1. Planung und Konzeption

Die Risiken, die sich aus der Datenverarbeitung in dem Unternehmen ergeben, müssen hinsichtlich Art, Umfang, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit von Verletzungen und Schäden beachtet werden. Insbesondere geht es um die Risiken für die persönlichen Rechte und Freiheiten der betroffenen Personen.

Das Unternehmen muss zunächst seine „Datenschutzpolitik“ beschreiben, also festlegen:

- die Zuständigkeiten für den Datenschutz im Unternehmen
  - hierzu gehört auch die Einbindung und Aufgabenstellung des betrieblichen Datenschutzbeauftragten
- die Sensibilisierung und Schulung der Mitarbeiter
- Verpflichtung auf das Datengeheimnis
  - das ist zwar gesetzlich nicht mehr vorgeschrieben, aber anzuraten; alternativ muss sichergestellt werden, dass die Mitarbeiter, die personenbezogenen Daten verarbeiten, dies nur entsprechend ihrer Aufgabenerfüllung tun. Für Auftragsverarbeiter ist vorgeschrieben, dass sie ihre Mitarbeiter auf die Vertraulichkeit verpflichten müssen.
- die Durchführung von Kontrollen, ob die getroffenen Regelungen/Anweisungen auch eingehalten werden

- den Einsatz datenschutzfreundlicher Technologien

- den Stand der Technik als Anforderung an die IT-Sicherheit

- die Führung des Verzeichnisses von Verarbeitungstätigkeiten

- den Prozess zum Abschluss von Auftragsverarbeitungen oder – bei gemeinsamer Verantwortlichkeit – zum Abschluss entsprechender Vereinbarungen

- den Prozess zur Umsetzung der Betroffenenrechte und der Transparenz der Datenverarbeitung

- den Prozess zur Durchführung einer Risikobewertung

- den Prozess zur Durchführung von Datenschutz-Folgenabschätzungen und einer eventuellen Meldung an die Aufsichtsbehörde

- den Prozess zur Meldung von Verletzungen des Datenschutzes (Datenpannen).

Es sollte geprüft werden, ob es im Unternehmen Anknüpfungspunkte für ein Datenschutzmanagement gibt. Herfür bieten sich z. B. bereits bestehende Compliance-Richtlinien oder ein Qualitätsmanagement sowie ein IT-Sicherheits- oder ein Risikomanagement an.

2. Umsetzung

Hiervon umfasst ist die Konkretisierung der unter 1. genannten Maßnahmen in der Praxis. Dazu gehört eine ausreichende Dokumentation sowie die geeigneten technisch-organisatorischen Maßnahmen.

3. Erfolgskontrolle und Überwachung

Die Planung und Konzeption sowie ihre Umsetzung müssen stetig auf ihre Wirksamkeit hin kontrolliert werden.

4. Optimierung und Verbesserung

Wird unter 3. festgestellt, dass Anpassungen notwendig sind, müssen sie vorgenommen werden. Hierzu gehört auch die Erfüllung des angemessenen Stands der Technik bei den technischen IT-Sicherheitsmaßnahmen, denn die DS-GVO verlangt die Anpassung an entsprechende technische Entwicklungen.

Ergebnis muss jedenfalls sein, dass die Rechtskonformität der Verarbeitung in rechtlicher, technischer und organisatorischer Hinsicht jederzeit nachweisbar ist.