Kurzpapier Nr. 8
Maßnahmenplan „DS-GVO“ für Unternehmen

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Bedeutung

Die DS-GVO, die im Mai 2016 in Kraft getreten ist, wird weitreichende Auswirkungen auf nahezu alle Unternehmen in Europa haben. Anders als die bisherige EU-Richtlinie wird diese EU-Verordnung ab dem 25. Mai 2018 unmittelbar in den Mitgliedsstaaten der EU anwendbar sein und wird das bis dahin geltende Bundesdatenschutzgesetz (BDSG) ablösen. Gleichzeitig sieht das deutsche Datenschutz-Anpassungs- und Umsetzungsgesetz-EU (DSAnpUG-EU) eine ergänzende Neufassung des nationalen Rechts vor (z. B. BDSG-neu), soweit in der DS-GVO Spielraum für nationale Regelungen besteht. Viele Unternehmen sind aber noch nicht auf die DS-GVO und deren Auswirkungen auf die Unternehmensprozesse vorbereitet. Daher haben die unabhängigen Datenschutzbehörden einige Tipps zur Erstellung eines Maßnahmenplans für Unternehmen zusammengestellt.

Information der Geschäftsleitung

Alle Entscheidungsträger in einem Unternehmen sollten sich der Auswirkungen der DS-GVO bewusst sein und wissen, was dies für den alltäglichen Betrieb in ihrem Unternehmen bedeutet. In einem ersten Schritt ist daher von den betrieblichen Datenschutzbeauftragten und/oder den IT-Verantwortlichen die Geschäftsleitung zu informieren.

Start eines Projekts zur Umsetzung der DS-GVO

Alle Verfahren, mit denen personenbezogene Daten verarbeitet werden, sind dahingehend zu überprüfen, ob es einen Anpassungsbedarf im Hinblick auf die DS-GVO gibt. Dies betrifft insbesondere die rechtlichen, technischen und organisatorischen Bereiche in einem Unternehmen. Da folglich verschiedene Personen bzw. Abteilungen im Unternehmen beteiligt sind, die untereinander koordiniert werden müssen, bietet es sich an, ein Projekt mit dem Ziel zu initiieren, die Datenschutzkonzeption anhand eines Soll-Ist-Abgleichs zu aktualisieren.
Die Kernaufgabe wird dabei sein, herauszufinden, welche Prozesse im Unternehmen anzupassen sind.

1. Bestandsaufnahme

Um ein genaues Verständnis davon zu bekommen, wie in einem Unternehmen mit personenbezogenen Daten umgegangen wird, sollten die aktuell realisierten Rahmenbedingungen aller Datenverarbeitungen analysiert werden (Ist-Zustand). Dies betrifft u.a.

- die derzeitigen Prozesse im Unternehmen, in denen personenbezogene Daten verarbeitet werden (bestehende Dokumentationen, bspw. ein Verfahrensverzeichnis, können hierfür einen Ausgangspunkt bilden),
- die dazugehörigen Rechtsgrundlagen (die Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn entweder ein Gesetz oder eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat),
- die Datenschutzorganisation (d.h. alle Vorkehrungen und Maßnahmen, die im Unternehmen zum Schutz personenbezogener Daten getroffen werden),

- die Dienstleistungsbeziehungen (wie etwa Verträge über eine Auftragsdatenverarbeitung),
- die Dokumentation (z.B. Verfahrensverzeichnisse, Vorabkontrollen, Datenschutzkonzepte, IT-Sicherheitskonzepte, Sicherheitsvorfälle) und
- sofern vorhanden Betriebsvereinbarungen, denn diese können auch Regelungen zum Umgang mit den Daten der Beschäftigten enthalten.

2. Handlungsbedarf eruieren

Nunmehr ist der Soll-Zustand zu ermitteln und im Anschluss daran eine Lückenanalyse zwischen dem jetzigen Ist-Zustand und dem künftigen Soll-Zustand durchzuführen. Dabei sind u.a. folgende Punkte vor dem Hintergrund der DS-GVO zu beachten (zu den einzelnen Themen erscheinen weitere Kurzpapiere):

- **Rechtsgrundlagen:**
  Auch unter der DS-GVO ist für die Verarbeitung personenbezogener Daten eine Legitimationsgrundlage erforderlich. Folglich ist zu prüfen, ob das neue Recht für alle Prozesse eine Rechtsgrundlage bereitstellt. Sofern sich die Datenverarbeitung auf eine Einwilligung stützt, ist zu prüfen, ob die Anforderungen des Art. 7 DS-GVO erfüllt sind (bei Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft ist zudem Art. 8 DS-GVO zu beachten).
- **Betroffenenrechte:**
  Den betroffenen Personen stehen umfangreiche Rechte zu, die der Verantwortliche zu beachten hat (z.B. Informationspflichten des Verantwortlichen gegenüber den betroffenen Personen nach Art. 13 und Art. 14 DS-GVO, Auskunftsrecht nach Art. 15 DS-GVO, Recht auf Berichtigung nach Art. 16 DS-GVO, Recht auf Löschung nach Art. 17 DS-GVO, das neue Recht auf Datenübertragbarkeit nach Art. 20 DS-GVO, Widerspruchsrecht nach Art. 21 DS-GVO).
- **Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen:**
  Die DS-GVO enthält spezifische Rahmenbedingungen für die Art und Weise, wie die Anforderungen der DS-GVO schon bei der Prozessgestaltung und bei den Voreinstellungen umzusetzen sind (Art. 25 DS-GVO: Data Protection by design und Data Protection by default).
- **Dienstleistungsbeziehungen:**
  Dabei sollten insbesondere die bestehenden Verträge zur Auftragsverarbeitung überprüft werden. Die Art. 28 und 29 DS-GVO enthalten Vorgaben für Vereinbarungen mit Auftragsverarbeitern.
- **Dokumentationspflichten:**
  Die DS-GVO verpflichtet in Art. 5 Abs. 2 DS-GVO den Verantwortlichen zum Nachweis, dass personenbezogene Daten rechtmäßig verarbeitet werden (Rechenschaftspflicht). Zusätzlich sieht die DS-GVO an unterschiedlichen Stellen Dokumentationspflichten vor (z.B. für das Verarbeitungs-verzeichnis in Art. 30 DS-GVO, für die Dokumentation von Datenschutzvorfällen in Art. 33 Abs. 5 DS-GVO oder für die Dokumentation von Weisungen im Rahmen der Auftragsverarbeitung in Art. 28 Abs. 3 lit. a DS-GVO).
- **Datenschutz-Folgenabschätzung:**
  Die aus dem BDSG bekannte Vorabkontrolle wird durch die Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO abgelöst und erfordert eine umfangreiche Dokumentation. Die Datenschutz-Folgenabschätzung kann zudem eine Konsultation der Aufsichtsbehörde nach sich ziehen (Art. 36 DS-GVO).
- **Meldepflichten:**
  Nach Art. 37 Abs. 7 DS-GVO muss der Verantwortliche oder der Auftragsverarbeiter die Kontaktdaten des Datenschutzbeauftragten der zuständigen Aufsichtsbehörde melden. Ebenso ist der Aufsichtsbehörde

die Verletzung des Schutzes personenbezogener Daten zu melden (Art. 33 Abs. 1 DS-GVO).

- **Datensicherheit:**
  Unternehmen müssen ein angemessenes Schutzniveau in Bezug auf die Sicherheit der Verarbeitung gewährleisten und die dafür implementierten Sicherungsmaßnahmen einer regelmäßigen Überprüfung unterziehen (Art. 24 und 32 DS-GVO).
- **Zertifizierung:**
  Schlussendlich besteht im Rahmen eines Zertifizierungsverfahrens die Möglichkeit, den Nachweis zu erbringen, dass die Datenverarbeitung im Einklang mit der DS-GVO erfolgt.

3. Umsetzung bis zum 25. Mai 2018

Bei der Umsetzung sind dann u. a. folgende Punkte wieder zu beachten:

- Anpassung der betroffenen Prozesse und Strukturen,
- Festlegung der Rechtsgrundlagen und des Zwecks der Datenverarbeitung sowie Dokumentation von Interessenabwägungen (sofern erfolgt),
- Implementierung von Informationspflichten, Betroffenenrechten und Löschkonzepten,
- Anpassung der Datenschutzorganisation,
- ggf. Bestellung eines Datenschutzbeauftragten,
- Reaktionsmechanismen auf Datenpannen,
- Organisation von Meldepflichten,
- Anpassung der Dienstleistungsbeziehungen,
- Aufbau der Dokumentation,
- Anpassung der IT-Sicherheit und
- ggf. Anpassung der Betriebsvereinbarungen.