DSGVO

Anforderungen an ein Datenschutz-Management-System

Die Datenschutz-Grundverordnung (DSGVO) hält mannigfaltige Veränderungen zur bisherigen Regelungslage gemäß Bundesdatenschutzgesetz (BDSG) bereit. Aus Unternehmenssicht kommt es im Rahmen der laufenden Umsetzungsfrist bis Mai 2018 darauf an, nicht nur einzelne Datenschutzinstrumente im Unternehmen auf Aktualisierungsbedarf zu prüfen, sondern die Summe aller Einzelteile, also das betriebliche Datenschutz-Management-System (DSMS) an den veränderten Bedingungen neu auszurichten.

Ein Nachjustieren an einzelnen Rädchen wird langfristig nicht reichen, um die Anforderungen der Datenschutz-Grundverordnung systematisch und umfassend umzusetzen (Bild: xpoint / iStock / Thinkstock)

Die DSGVO stellt Unternehmen vor neue Herausforderungen. Das gilt nicht nur im Hinblick auf die Verschärfung einzelner Vorschriften oder die Höhe möglicher Bußgelder. Vielmehr stellt die Grundverordnung in Art. 5 Abs. 2 klar, dass eine Rechenschaftspflicht besteht („Accountability“).

Neu: Die Rechenschaftspflicht für Unternehmen

Unter „Accountability“ ist nicht nur die Zuständigkeit und Verantwortung für die Einhaltung der festgelegten Prinzipien zur Datenverarbeitung nach Art. 5 Abs. 1 DSGVO zu verstehen, sondern auch eine Nachweispflicht. Das Unternehmen muss nachweisen (können), dass es als Verantwortlicher angemessene und wirksame Maßnahmen ergreift, um die datenschutzrechtlichen Grundsätze und Verpflichtungen der DSGVO umzusetzen.

Worauf bezieht sich die Rechenschaftspflicht?

Die Rechenschaftspflicht erstreckt sich auf alle Anforderungen, die die Grundverordnung an den für die Verarbeitung Verantwortlichen stellt. Dazu zählen die allgemeinen Prinzipien der DSGVO ebenso wie spezifische Anforderungen an den Lebenszyklus der Verarbeitung von personenbezogenen Daten im Unternehmen.

Zunächst zu den allgemeinen Prinzipien der Grundverordnung.

Prinzipien der Verarbeitung von personenbezogenen Daten

Zu den allgemeinen Prinzipien der Verarbeitung personenbezogener Daten zählen nach Art. 5 Abs. 1 DSGVO:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz: Verarbeitung auf rechtmäßige Weise, nach dem Grundsatz von Treu und Glauben und in einer für den Betroffenen nachvollziehbaren Weise.
- Zweckbindung: Erhebung für festgelegte, eindeutige und rechtmäßige Zwecke, wobei eine Weiterverarbeitung diesen Zwecken nicht zuwider laufen darf.
- Datenminimierung: Beschränkung auf das für den Zweck der Verarbeitung angemessene und sachlich relevante sowie notwendige Maß.
- Richtigkeit: Sachlich richtige und ggf. aktuellste Daten, Maßnahmen zur unverzüglichen Löschung oder Berichtigung unzutreffender Daten.
- Speicherbegrenzung: Speicherung mit Personenbezug höchstens so lange, wie es für die Verarbeitungszwecke erforderlich ist.
- Integrität, Vertraulichkeit, Verfügbarkeit: Geeignete technisch-organisatorische Maßnahmen zum angemessenen Schutz der Daten, insbesondere vor unbefugter oder unrechtmäßiger Verarbeitung, zufälligem Verlust, zufälliger Zerstörung oder Schädigung.

Pflichten des Verantwortlichen

Eine Vielzahl von Vorschriften konkretisiert diese allgemeinen Grundsätze. Im Hinblick auf die rechtliche Zulässigkeit der Datenverarbeitung betrifft das v.a. folgende Punkte:

- **„Data Privacy by Design“** und **„Data Privacy by Default“**, Art. 25 DSGVO: Der Verantwortliche muss geeignete Maßnahmen zur wirksamen Umsetzung der datenschutzrechtlichen Grundsätze ergreifen (etwa zur Datenminimierung). Dabei muss er durch datenschutzfreundliche Voreinstellungen sicherstellen, dass er nur die jeweils erforderlichen Daten verarbeitet.
- **Datenschutz-Folgenabschätzung**, Art. 35, 36 DSGVO: Der Verantwortliche muss bei einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen vorab eine Analyse der Folgen erstellen. Für die identifizierten Risiken muss er geeignete Maßnahmen, Garantien, Sicherheitsvorkehrungen und Verfahren umsetzen.
- **Rechtmäßigkeit**, Art. 6 DSGVO: Der Verantwortliche muss die Rechtmäßigkeit an den gesetzlich definierten Verarbeitungstatbeständen ausrichten. Dazu zählen v.a. die Voraussetzung einer Einwilligung, Art. 7, 8 DSGVO, Einschränkungen für besondere Datenkategorien und Inhalte, Art. 9, 9a DSGVO, und die Verarbeitung ohne Bestimmung des Betroffenen, Art. 10 DSGVO.
- **Übermittlung in Drittländer**, Art. 44 DSGVO: Bei der Datenübermittlung in ein Drittland muss der Verantwortliche (samt Auftragsverarbeiter) Garantien für eine rechtmäßige Verarbeitung bieten.

Zugleich fordert die DSGVO vom Verantwortlichen geeignete Maßnahmen zur datenschutzrechtlichen Information und Kommunikation, insbesondere für den „Fall des Falles“:

- **Transparenz**, Art. 12 DSGVO: Der Verantwortliche muss Betroffene in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache informieren, und zwar in Bezug auf Name und Kontaktdaten der verantwortlichen Stelle (samt Datenschutzbeauftragtem) sowie Zwecke, ggf. berechtigte Interessen und Empfänger sowie die Drittlandübermittlung
- **Verletzung**, Art. 33, 34 DSGVO: Verletzungen des Schutzes personenbezogener Daten muss der Verantwortliche an die Aufsichtsbehörde melden. Gegebenenfalls muss er die Betroffenen benachrichtigen.

Technisch-organisatorische Maßnahmen nachweisen

Im Rahmen der eigentlichen Verarbeitung personenbezogener Daten muss der Verantwortliche geeignete technisch-organisatorische Maßnahmen v.a. in folgenden Bereichen vorsehen, umsetzen und nachweisen können:

- **Verantwortung**, Art. 24 DSGVO: Der Verantwortliche hat risikobasiert die geeigneten Maßnahmen zum Schutz der von der Verarbeitung betroffenen Daten zu ergreifen. Die Maßnahmen muss er nachweisen und aktuell halten.
- **Auftragsverarbeitung**, Art. 28 DSGVO: Der Verantwortliche darf nur mit Auftragsverarbeitern zusammenarbeiten, die Garantien dafür bieten, dass sie personenbezogene Daten durch geeignete technisch-organisatorische Maßnahmen schützen. Darüber muss ein Vertrag existieren.
- **Datensicherheit**, Art. 32 DSGVO: Der Verantwortliche muss risikobasiert durch geeignete Maßnahmen die klassischen IT-Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit bei der Datenverarbeitung sicherstellen.

Erforderliche interne Maßnahmen

Schließlich fordert die DSGVO vom Verantwortlichen die Umsetzung einer Reihe interner Maßnahmen. Die wichtigsten:

- **Verzeichnis**, Art. 30 DSGVO: Der Verantwortliche muss ein Verzeichnis aller Verarbeitungstätigkeiten führen – ähnlich dem aus dem BDSG bekannten Verfahrensverzeichnis.
- **Dokumentation**,
  26, 28, 31, 44 DSGVO: Der Verantwortliche muss neben dem Führen eines Verzeichnisses seiner Dokumentationspflicht nachkommen, z.B. bei Weisungen, Verletzungen oder Garantien im Rahmen der Drittlandübermittlung.
- **Datenschutzbeauftragter**, Art. 37–39 DSGVO: Der Verantwortliche hat unter bestimmten Voraussetzungen einen Datenschutzbeauftragten zu bestellen, dessen Aufgaben v.a. in der Beratung und in der Überwachung des Einhaltens der DSGVO-Vorgaben liegen.
- **Recht auf Vergessenwerden**, Art. 17 DSGVO: Der Verantwortliche hat nicht nur sicherzustellen, dass personenbezogene Daten nur ausnahmsweise nicht „unverzüglich“ gelöscht werden. Er muss – sofern er die Daten publik macht – auch sicherstellen, dass er Dritte darüber informiert.
- **Recht auf Interoperabilität**, Art. 20 DSGVO: Der Verantwortliche muss sicherstellen, dass er personenbezogene Daten von Betroffenen in einem gängigen, maschinenlesbaren Format ausgeben kann.

Fazit: Ohne Datenschutz-Management-System geht es nicht

Der Verantwortliche muss im Ergebnis einen „bunten Blumenstrauß“ an Maßnahmen (risikobasiert) definieren, umsetzen, dokumentieren und kontrollieren. Angesichts der Fülle von Anforderungen einerseits und der Rechenschafts- und Nachweispflicht aus der DSGVO andererseits wird er dabei um ein geordnetes System nicht herumkommen.

Ausblick: Der PDCA-Zyklus

Die Marschrichtung für ein solches System gibt die DSGVO selbst vor. Denn sie greift etablierte Prinzipien aus Management-Systemen anderer Disziplinen wie etwa der Informationssicherheit oder des Risikomanagements auf. Das zeigt besonders deutlich Art. 24 DSGVO. Danach muss der Verantwortliche unter Berücksichtigung des Kontexts und des Risikos Maßnahmen planen, umsetzen, dokumentieren, prüfen und bei Bedarf verbessern. Nichts anderes besagt im Kern der P(lan)-D(o)-C(heck)-A(ct)-Zyklus als Prinzip eines jeden Management-Systems.

Im nächsten Artikel zu den DSGVO-Anforderungen an das betriebliche Datenschutz-Management-System zeigen wir Ihnen, wie sich die DSGVO-Pflichten anhand des PDCA-Zyklus organisieren lassen.

Autor: Peer Lambertz ist Rechtsanwalt und Datenschutz-Experte.

Quelle: Datenschutz PRAXIS