Kurzpapier Nr. 1
Verzeichnis von Verarbeitungstätigkeiten – Art. 30 DS-GVO

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.

Altes Recht = neues Recht?

Das aus dem BDSG bekannte Verfahrensverzeichnis (§ 4g Abs. 2 und 2a BDSG; dort „Übersicht" genannt) wird mit der DS-GVO abgelöst durch ein (schriftliches oder elektronisches) Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten. Dieses Verzeichnis betrifft sämtliche – auch teilweise – automatisierte Verarbeitungen sowie nichtautomatisierte Verarbeitungen personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Grundsätzlich ist jeder Verantwortliche (z. B. Unternehmen, Freiberufler, Verein) und – neu – auch jeder Auftragsverarbeiter zur Erstellung und Führung eines solchen Verzeichnisses verpflichtet. Es wird in der Praxis wegen der Unterschiede bei den eingesetzten Verfahren notwendigerweise oft aus einer Reihe von Einzelbeiträgen bestehen müssen. Das Verfahrensverzeichnis wird somit die Summe der einzelnen Verfahrensbeschreibungen sein.

Stellen mit weniger als 250 Mitarbeitern

Unternehmen und Einrichtungen mit weniger als 250 Mitarbeitern müssen kein Verzeichnis von Verarbeitungstätigkeiten führen, es sei denn, der Verantwortliche bzw. Auftragsverarbeiter führt Verarbeitungen personenbezogener Daten durch,

- die ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen (dazu gehören regelmäßig Fälle von Scoring und Überwachungsmaßnahmen) oder
- die nicht nur gelegentlich erfolgen (z.B. die regelmäßige Verarbeitung von Kunden- oder Beschäftigtendaten) oder
- die besondere Datenkategorien gemäß Art. 9 Abs. 1 DS-GVO (Religionsdaten, Gesundheitsdaten, usw.) oder strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO betreffen.

Die Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten besteht also bereits dann, wenn mindestens eine der genannten Fallgruppen erfüllt ist. Da es anders als in Art. 35 DS-GVO (Datenschutz-Folgenabschätzung) nicht darauf ankommt, dass es sich voraussichtlich um ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen handelt, sondern jedes Risiko für die Rechte und Freiheiten bezüglich der Verarbeitung zu betrachten ist, wird vielfach das Erstellen eines Verzeichnisses von Verarbeitungstätigkeiten geboten sein.

Kein öffentliches Verzeichnis und keine Meldepflicht mehr

Anders als im bisherigen BDSG ist eine Möglichkeit für jedermann, in das Verzeichnis von Verarbeitungstätigkeiten Einsicht zu nehmen, nach der DS-GVO nicht vorgesehen. Ebenso entfallen mit der DS-GVO die bisher in § 4d und § 4e BDSG geregelten Meldepflichten von manchen Unternehmen an die Aufsichtsbehörde. Erstellt und vorgehalten werden müssen die Verzeichnisse dennoch, da sie den Aufsichtsbehörden jederzeit auf Anfrage zur Verfügung

zu stellen sind (siehe Art. 30 Abs. 4 DS-GVO und ErwGr. 82).

Inhalt des Verzeichnisses für Verantwortliche (Art. 30 Abs. 1 DS-GVO)

Das Verzeichnis der Verantwortlichen muss nach Art. 30 Abs. 1 DS-GVO wesentliche Angaben zur Verarbeitung beinhalten wie z. B. die Zwecke der Verarbeitung und eine Beschreibung der Kategorien der personenbezogenen Daten, der betroffenen Personen und der Empfänger.

Verantwortliche Stellen, die bereits jetzt über ein strukturiertes Verfahrensverzeichnis oder eine strukturierte Datenschutzdokumentation zu den Verfahren verfügen, sollten mit den geforderten Pflichtangaben des neuen Artikels aus der DS-GVO keine Probleme haben.

Inhalt des Verzeichnisses für Auftragsverarbeiter (Art. 30 Abs. 2 DS-GVO)

Ein Verzeichnis beim Auftragsverarbeiter zu allen Kategorien der von ihm im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung war vom BDSG bislang nicht vorgeschrieben. Nach Art. 30 Abs. 2 DS-GVO ist ein solches Verzeichnis jedoch künftig zu erstellen.

Auch hier sind die Pflichtangaben überschaubar, so dass der Aufwand, dieses Verzeichnis zu erstellen, als eher gering einzustufen sein wird.

Beschreibung technischer und organisatorischer Maßnahmen

Art. 30 Abs. 1 lit. g und Art. 30 Abs. 2 lit. d DS-GVO geben vor, dass das Verzeichnis, wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1 DS-GVO enthalten soll. Wie detailliert diese Beschreibung sein muss, lässt sich der DS-GVO nicht unmittelbar entnehmen. Jedenfalls sollte die Beschreibung der Maßnahmen nach Art. 32 DS-GVO so konkret erfolgen, dass die Aufsichtsbehörden eine erste Rechtmäßigkeitsüberprüfung vornehmen können.

Rechtsfolgen bei Verstoß

Verstöße durch eine fehlende oder nicht vollständige Führung eines Verzeichnisses oder das Nichtvorlegen des Verzeichnisses nach Aufforderung durch die Aufsichtsbehörde können nach Art. 83 Abs. 4 lit. a DS-GVO mit einer Geldbuße sanktioniert werden.

Das Verzeichnis als Teil der Rechenschaftspflicht

Mit der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten sind keinesfalls alle von der DS-GVO geforderten Dokumentationspflichten erfüllt. Das Verzeichnis ist nur ein Baustein, um der in Art. 5 Abs. 2 normierten Rechenschaftspflicht zu genügen. So müssen beispielsweise auch das Vorhandensein von Einwilligungen (Art. 7 Abs. 1), die Ordnungsmäßigkeit der gesamten Verarbeitung (Art. 24 Abs. 1) und das Ergebnis von Datenschutz-Folgenabschätzungen (Art. 35 Abs. 7) durch entsprechende Dokumentationen nachgewiesen werden.

Ausblick: Wesentliche Rolle des Verzeichnisses und Muster-Vorlage der Datenschutzaufsichtsbehörden

Das Verzeichnis von Verarbeitungstätigkeiten nach der DS-GVO wird wie die bisherigen internen Verfahrensverzeichnisse eine wesentliche Rolle spielen, um datenschutzrechtliche Vorgaben überhaupt einhalten zu können. Nur wer die eigenen Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um eine rechtmäßige Verarbeitung personenbezogener Daten sicherstellen zu können.
Die deutschen Aufsichtsbehörden werden im Jahr 2017 eine Muster-Vorlage sowie weitere Hinweise für ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO bereitstellen.

Unsere Empfehlung

Es ist ratsam, rechtzeitig im eigenen Interesse ein vollständiges Verzeichnis von Verarbeitungstätigkeiten zu erstellen. Das Verzeichnis von Verarbeitungstätigkeiten dient als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und hilft dem Verantwortlichen dabei, gemäß Art. 5 Abs. 2 DS-GVO nachzuweisen, dass die Vorgaben aus der DS-GVO eingehalten werden (Rechenschaftspflicht). Die Übergangszeit bis zur Geltung der DS-GVO am 25.05.2018 sollte dazu genutzt werden, die bereits bestehende Verfahrensdokumentation an die neuen Anforderungen anzupassen.

****

Anmerkung zur Nutzung dieses Kurzpapiers: