

EU-Datenschutz-Grundverordnung (DS-GVO)

Das BayLDA auf dem Weg zur Umsetzung der Verordnung

Wichtiger Hinweis zu diesem Dokument:

Die DS-GVO wird nach der Übergangsphase von zwei Jahren am 25. Mai 2018 wirksam. Die Aufsichtsbehörden sind aktuell bemüht, durch intensive Abstimmungsrunden eine einheitliche Sichtweise der neu geregelten Grundlagen und Anforderungen an den Datenschutz auf europäischer Ebene zu erzielen. Das BayLDA beteiligt sich deshalb an verschiedenen Arbeitskreisen, die sich dieser Herausforderung auch in Deutschland stellen. In der Zwischenzeit möchte das BayLDA Interessierten einen Einblick gewähren, welche Themenkomplexe der DS-GVO derzeit auch in der bayerischen Aufsichtsbehörde intensiv diskutiert werden. Das BayLDA veröffentlicht deshalb in regelmäßigen Abständen (geplant: zweimal im Monat) ein kurzes Papier zu einem ausgewählten Schwerpunkt. Das BayLDA weist ausdrücklich darauf hin, dass es sich hierbei um keine verbindlichen Auffassungen handelt, sondern um gegenwärtige Interpretationen und Meinungen zur DS-GVO. Kommentare zum dargestellten gegenwärtigen Verständnis nimmt das BayLDA gerne entgegen.

V

Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO

Altes Recht = neues Recht?

Die aus dem BDSG bekannten Dokumentationen (§ 4g Abs. 2 und Abs. 2a BDSG)

- öffentliches Verzeichnisseverzeichnis und
- interne Verarbeitungsübersicht

werden mit der DS-GVO abgelöst durch ein (schriftliches oder elektronisches) Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten, das grundsätzlich jeder Verantwortliche (z. B. Unternehmen, Freiberufler, Verein) und *-neu-* auch ein Auftragsverarbeiter zu erstellen und zu führen hat. Dieses Verzeichnis wird in der Praxis wegen der Unterschiede bei den eingesetzten Verfahren notwendigerweise oft aus einer Reihe von Einzelverzeichnissen bestehen müssen.

Stellen mit weniger als 250 Mitarbeitern

Ein Verzeichnis von Verarbeitungstätigkeiten müssen nach Art. 30 Abs. 5 DS-GVO nicht Verantwortliche und Auftragsverarbeiter mit weniger als 250 Mitarbeitern 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 (z. B. Scoring),
- die nicht nur gelegentlich erfolgen oder
- die besondere Datenkategorien gemäß Art. 9 Abs. 1 DS-GVO (Religionsdaten, Gesundheitsdaten, usw.) oder über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10 DS-GVO betreffen.

Für diese drei Fallgruppen müssen also trotzdem die Angaben in das Verzeichnis aufgenommen werden.

Kein öffentliches Verzeichnis und keine Meldepflicht mehr

Eine öffentlich für jedermann zugängliche Übersicht zu den eingesetzten automatisierten Verfahren für die Verarbeitung personenbezogener Daten ist in der DS-GVO *nicht* vorgesehen, ebenso entfallen mit der DS-GVO die bisher in § 4d und § 4e BDSG geregelten Melde-

pflichten von manchen Unternehmen an die Aufsichtsbehörde.

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

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

Verantwortliche Stellen, die bereits jetzt über eine strukturierte Verfahrensübersicht verfügen, sollten mit den geforderten Pflichtangaben des neuen Artikels aus der DS-GVO keine größeren Probleme haben.

Inhalt des Verzeichnisses für Auftragsdatenverarbeiter (Art. 30 Abs. 2)

Ein *Verzeichnis beim Auftragsverarbeiter* zu allen Kategorien der von 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.

Verzeichnis nicht öffentlich zugänglich

Künftig wird das Verzeichnis über die eingesetzten Verfahren nicht mehr öffentlich zugänglich sein. 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 EW Nr. 82.)

Rechtsfolgen bei Verstoß

Verstöße durch eine fehlende oder nicht vollständige Führung eines Verzeichnisses oder das Nichtvorlegen des Verzeichnisses nach Aufforderung durch die Aufsichtsbehörde sind nach Art. 83 Abs. 4 a DS-GVO mit Geldbuße bedroht. Allein aus diesem Grund ist es ratsam, *rechtzeitig* im eigenen Interesse ein vollständiges Verzeichnis von Verarbeitungstätigkeiten zu erstellen.

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

Das Verzeichnis von Verarbeitungstätigkeiten nach der DS-GVO wird wie die bisherigen internen Verarbeitungsübersichten 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.

Spannend wird sicherlich die Frage, in welchem Detailgrad die technischen und organisatorischen Maßnahmen im neuen Verzeichnis aufgenommen werden *müssen*. Art. 30 Abs. 1 g und Art. 30 Abs. 2 d sprechen lediglich von einer Möglichkeit einer allgemeinen Beschreibung dieser Maßnahmen. Wie dies in der Praxis ausgestaltet werden kann, um dennoch einen datenschutzrechtlichen Mehrwert zu bieten, ist derzeit noch nicht absehbar.

Die deutschen Aufsichtsbehörden haben bereits eine Arbeitsgruppe gegründet, die das Ziel verfolgt, bis ca. Mitte 2017 eine Muster-Vorlage für ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO zu erarbeiten.