Die EU-Datenschutz-Grundverordnung

Checkliste für die Umsetzung in Unternehmen *

Ab dem 25. Mai 2018 wird die europäische Datenschutz-Grundverordnung (EU-DSGVO) unmittelbar anwendbar sein. Sie bringt eine Reihe von Veränderungen und neuen Anforderungen für den Umgang mit personenbezogenen Daten mit sich. Die folgenden Punkte geben Anregungen zur Umsetzung in Unternehmen.

1. Kommunikation und Sensibilisierung

Geschäftsleitung und andere für das Thema Datenschutz Zuständige sollten innerhalb des Unternehmens dafür sensibilisieren, dass sich ab dem 25.05.2018 nicht nur der Name einer europäischen Datenschutzregelung ändern wird. Die EU-DSGVO wird direkte Auswirkungen auf datenverarbeitende Unternehmen haben. Anders als eine EU-Richtlinie ist eine EU-Verordnung in den Mitgliedstaaten der Europäischen Union unmittelbar anwendbar, also auch in Deutschland. Neben der EU-DSGVO wird es weiterhin ein – neues – Bundesdatenschutzgesetz und bereichsspezifisches nationales Datenschutzrecht geben. Bitte beachten Sie: bis zum 24.05.2018 (einschließlich) gilt das jetzige Bundesdatenschutzgesetz!

2. „Bestandsaufnahme"

Um möglichen Änderungsbedarf im Umgang mit personenbezogenen Daten identifizieren zu können, sollten Unternehmen in einem ersten Schritt eine Bestandsaufnahme der Prozesse durchführen, in denen personenbezogene Daten verarbeitet werden. Das bisherige Verfahrensverzeichnis nach § 4d Bundesdatenschutzgesetz (BDSG) ist ein Ausgangspunkt zur Identifizierung der Datenverarbeitungen. Im Folgenden sind beispielhaft einige Themen zusammengestellt, bei denen sich für Unternehmen Änderungsbedarf ergeben kann.

3. Rechtsgrundlagen prüfen

Auch unter der EU-DSGVO ist für die Verarbeitung personenbezogener Daten stets eine Rechtsgrundlage erforderlich (Verbot mit Erlaubnisvorbehalt). Die Rechtsgrundlage kann sich unmittelbar aus der EU-DSGVO ergeben. In Betracht kommt etwa die Einwilligung des Betroffenen (Art. 6 Abs. 1 lit. a EU-DSGVO). Eine Datenverarbeitung ist ferner u. a. dann zulässig, wenn sie zur Erfüllung eines Vertrages mit dem Betroffenen erforderlich ist (Art. 6 Abs. 1 lit. b EU-DSGVO). Rechtsgrundlagen für Datenverarbeitungen können sich darüber hinaus aus dem BDSG (vgl. u. a. §§ 3, 23, 25 BDSG neu) sowie dem bereichsspezifischen nationalen Datenschutzrecht ergeben. Für jede Datenverarbeitung innerhalb des Unternehmens ist zu prüfen, ob das neue Recht eine Rechtsgrundlage bereitstellt.

4. Anforderungen an die datenschutzrechtliche Einwilligung

Vielen Unternehmen dient die Einwilligung (etwa von Kunden) als Rechtsgrundlage für die Verarbeitung personenbezogener Daten. Bei der Einholung von Einwilligungen sind die spezifischen Anforderungen der EU-DSGVO zu beachten (Art. 7 EU-DSGVO). Für die Einwilligungen von Kindern gelten darüber hinausgehende Vorgaben (Art. 8 EU-DSGVO). Bei der Datenerhebung müssen zudem die –

gegenüber der bisherigen Rechtslage erweiterten – Informationspflichten der EU-DSGVO eingehalten werden (Art. 13 EU-DSGVO).

5. Verträge und Regularien überprüfen

Unternehmen sollten ihre bestehenden Verträge zur Auftragsdatenverarbeitung überprüfen und überarbeiten. In Artikel 28 EU-DSGVO sind Vorgaben für Vereinbarungen mit Auftragsdatenverarbeitern (jetzt: „Auftragsverarbeiter") geregelt. Auch bestehende Geschäftsprozesse, Regularien/Richtlinien und Handbücher, wie z.B. Dienstvereinbarungen, sollten daraufhin überprüft werden, ob sie mit den Anforderungen der EU-DSGVO vereinbar sind.

6. Datenschutz-Folgenabschätzung

Der europäische Gesetzgeber hat die bisherige Vorabkontrolle (§ 4d Abs. 5 BDSG) nicht in die EU-DSGVO übernommen. Sie wird abgelöst durch die Datenschutz-Folgenabschätzung (Artikel 35 EU-DSGVO). Eine Datenschutz-Folgenabschätzung ist durchzuführen, wenn eine Datenverarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten betroffener Personen zur Folge hat (Artikel 35 Abs. 1 EU-DSGVO). An eine Datenschutz-Folgenabschätzung kann sich eine verpflichtende Konsultation der zuständigen Aufsichtsbehörde anschließen, die vor Durchführung der eigentlichen Datenverarbeitung zu erfolgen hat (Artikel 36 EU-DSGVO).

7. Melde– und Konsultationspflichten

Die Melde- und Konsultationspflichten gegenüber den Aufsichtsbehörden (Artikel 33, 36 und 37 EU-DSGVO) müssen in den internen Abläufen des Unternehmens abgebildet werden. Gleichzeitig sollte sichergestellt sein, dass der betriebliche Datenschutzbeauftragte bei datenschutzrechtlichen Fragestellungen und der Ausgestaltung von Datenverarbeitungsprozessen frühzeitig beteiligt wird. Im Rahmen der Datenschutz-Folgenabschätzung sieht die EU-DSGVO dies ausdrücklich vor (Artikel 35 Abs. 2 EU-DSGVO). Wann ein betrieblicher Datenschutzbeauftragter verpflichtend zu benennen ist, regeln Artikel 37 EU-DSGVO und § 38 BDSG neu.

8. Betroffenenrechte und Informationspflichten

Die in der EU-DSGVO geregelten Betroffenenrechte müssen in den Geschäftsabläufen des Unternehmens abgebildet und gegenüber den Betroffenen umgesetzt werden. Hierzu gehören etwa das Recht auf Löschung (Artikel 17), das Recht auf Datenübertragbarkeit (Artikel 20) sowie die Informationspflichten des Verantwortlichen gegenüber dem Betroffenen (Artikel 13, 14) einschließlich der übergreifenden Rahmenvorgaben (Artikel 12). Spezifische Beschränkungen der Betroffenenrechte nach dem neuen BDSG (vgl. etwa § 35 BDSG neu) oder dem bereichsspezifischen Datenschutzrecht sind zu beachten.

9. Dokumentation

Die EU-DSGVO enthält an verschiedenen Stellen Dokumentationspflichten, beispielsweise in Artikel 30 (Verarbeitungsverzeichnis), Artikel 33 Abs. 5 (Dokumentation von Datenschutzvorfällen) oder Artikel

28 Abs. 3 lit. a (Dokumentation von Weisungen im Rahmen von Auftragsverarbeitungsverhältnissen). Die Dokumentationspflichten dienen der betrieblichen Selbstkontrolle sowie der effektiven Überprüfung durch die Aufsichtsbehörde.

10. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („Privacy-by-Design" und „Privacy-by-Default")

Die EU-DSGVO gibt Rahmenbedingungen vor, wie die datenschutzrechtlichen Anforderungen der EU-DSGVO durch die verantwortliche Stelle schon bei der Prozessgestaltung und bei Voreinstellungen umzusetzen sind (Artikel 25 EU-DSGVO). Dies sollte bei Einrichtung und Ausgestaltung der Datenverarbeitungssysteme im Unternehmen frühzeitig bedacht werden.

11. Fazit

Die EU-DSGVO setzt auf ein Datenschutzmanagementsystem mit einem Pflichtenkatalog, der die Einhaltung datenschutzrechtlicher Anforderungen frühzeitig, effektiv und schnell gewährleisten soll. Es liegt in der Verantwortung des Unternehmens, dieses System proaktiv umzusetzen. Datenschutzverletzungen können empfindliche Geldbußen (Artikel 83 EU-DSGVO) und/oder Schadensersatzansprüche der betroffenen Personen (Artikel 82 EU-DSGVO) nach sich ziehen.

* Die Hinweise basieren in wesentlichen Teilen auf einem von den Landesdatenschutzbehörden am 24.5.2017 für Unternehmen veröffentlichten „10-Punkte-Papier", abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2017/05/10-Punkte-Papier_PM_Datenschutz-bleibt-Chefsache.pdf. Sie erheben keinen Anspruch auf Vollständigkeit.