Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich

Auf dem Weg zur EU Datenschutz-Grundverordnung — Anregungen für Unternehmen
Die europäische Datenschutz-Grundverordnung (DS-GVO) bringt eine Reihe von Veränderungen in den datenschutzrechtlichen Anforderungen für den Umgang mit personenbezogenen Daten mit sich. Auch Auftrags(daten)verarbeiter müssen sich auf geänderte Rahmenbedingungen einstellen. Wir haben in 10 Punkten Anregungen für Unternehmen zusammengestellt.

1. Sensibilisierung durchführen

Geschäftsführungen, Datenschutzbeauftragte 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 DS-GVO wird direkte Auswirkungen auf Unternehmen als datenverarbeitende Stellen haben. Anders als eine EU-Richtlinie ist eine EU-Verordnung direkt in den Mitgliedstaaten der Europäischen Union anwendbar, also auch in Deutschland. Neben der DS-GVO wird es weiterhin ein – neues – Bundesdatenschutzgesetz und sektorales Fachrecht mit ausführenden Regelungen zur DS-GVO geben. Bitte beachten Sie: bis zum 24.05.2018 (einschließlich) gilt das JETZIGE Bundesdatenschutzgesetz!

2. Bestandsaufnahme machen

Um Änderungsbedarf identifizieren zu können, sollte in einem ersten Schritt eine Bestandsaufnahme der Prozesse durchgeführt werden, in denen personenbezogene Daten verarbeitet werden. Das Verfahrensverzeichnis nach § 4d Bundesdatenschutzgesetz (BDSG) ist ein Ausgangspunkt zur Identifizierung von Verarbeitungsverfahren. Im Folgenden haben wir beispielhaft einige Themen zusammengestellt, bei denen sich für Unternehmen Änderungsbedarf ergeben kann.

3. Rechtsgrundlage prüfen

Auch unter der DS-GVO ist für die Verarbeitung personenbezogener Daten eine Rechtsgrundlage erforderlich (Artikel 6 bis 11 DS-GVO). Es ist zu prüfen, ob das neue Recht für alle Prozesse Rechtsgrundlagen bereitstellt.

4. Personenbezogene Daten von Kindern besonders prüfen

Besondere Anforderungen bestehen für den Umgang mit personenbezogenen Daten von Kindern, wenn es um die Einwilligung in Bezug auf Dienste der Informationsgesellschaft geht (Artikel 8 DS-GVO).

5. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („Privacy-by-Design“ und „Privacy-by-Default“) umsetzen

Die DS-GVO enthält bestimmte Rahmenbedingungen für die Art und Weise, wie die Anforderungen der DS-GVO schon bei der Prozessgestaltung und bei Voreinstellungen umzusetzen sind (Artikel 25 DS-GVO).

6. Verträge checken

Unternehmen sollten insbesondere ihre bestehenden Verträge zur Auftrags(daten)verarbeitung überprüfen und überarbeiten. In den Artikeln 26 bis 28 DS-GVO sind Vorgaben für Vereinbarungen mit Auftrags(daten)verarbeitern und zwischen gemeinsam für die Verarbeitung Verantwortlichen geregelt.

7. Datenschutzfolgeabschätzung implementieren

Der europäische Gesetzgeber hat die bisherige Vorabkontrolle (§ 4d Abs. 5 BDSG) nicht in die DS-GVO übernommen. Sie wird abgelöst durch die Datenschutz-Folgeabschätzung (Artikel 35 DS-GVO). An eine Datenschutz-Folgeabschätzung kann sich eine verpflichtende Konsultation der zuständigen Aufsichtsbehörde anschließen (Artikel 36 DS-GVO).

8. Melde– und Konsultationspflichten organisieren

Die Melde- und Konsultationspflichten gegenüber den Aufsichtsbehörden (Artikel 33, 36 und 37 DS-GVO) müssen in den internen Abläufen des Unternehmens abgebildet werden.

9. Betroffenenrechte und Informationspflichten umsetzen

Die in der DS-GVO geregelten Betroffenenrechte müssen in den unternehmensinternen Abläufen abgebildet und gegenüber den Betroffenen umgesetzt werden, etwa das Recht auf Löschung (Artikel 17) und das Recht auf Datenübertragbarkeit (Artikel 20) einschließlich der übergreifenden Rahmenbedingungen (Artikel 12) sowie die Informationspflichten des Verantwortlichen (Artikel 13, 14).

10. Dokumentation organisieren

Die DS-GVO enthält an verschiedenen Stellen Dokumentationspflichten, beispielsweise in Artikel 30 (Verarbeitungsver-zeichnis), Artikel 33 Abs. 5 (Dokumentation von Datenschutzvorfällen) oder Artikel 28 Abs. 3 lit. a (Dokumentation von Weisungen im Rahmen von Auftragsverarbeitungsverhältnissen).