JHS CONSULTING
DATENSCHUTZ UND INFORMATIONSSICHERHEIT

Checkliste

Umsetzungsleitfaden / -hinweise zur EU-DSGVO

Auf dem Weg zur EU Datenschutz-Grundverordnung - Anregungen für Unternehmen -

Die Europäische Datenschutz-Grundverordnung (DS-GVO) ist am 5. Mai 2016 in Kraft getreten. Ab dem **25. Mai 2018** ist sie direkt anwendbares Recht (**Art. 99 Abs. 2 DS-GVO**). Nationale Regelungsspielräume bestehen nur noch in einem begrenzten Umfang. Die bisher für Unternehmen einschlägigen Regelungen des deutschen Datenschutzrechts werden damit weitgehend durch die Verordnung ersetzt.

Die 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.

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.

Damit verbunden ist auch eine Sensibilisierung der Mitarbeiter in Form von Datenschutzschulungen und einer Erklärung zur Vertraulichkeit.

2. Mitarbeiter schulen und Vertraulichkeitserklärung einholen

Um ein unternehmensweites Verständnis über den Datenschutz zu erreichen, sind auch die Mitarbeiter in den Datenschutz einzuweisen. Die Unterrichtung der Beschäftigten, die die Verarbeitungen durchführen, hinsichtlich ihrer Rechte und Pflichten nach der DS-GVO und dem DSAnpUG-EU bzw. dem BDSG-neu ist daher von großer Bedeutung. Des Weiteren sind Erklärungen zur Vertraulichkeit und dem Datengeheimnis im Unternehmen zu regeln.

3. Bestandsaufnahme machen und Verfahren dokumentieren

Um Änderungsbedarf identifizieren zu können, sollte in einem ersten Schritt eine Bestandsaufnahme der Verfahren und Prozesse durchgeführt werden, in denen personenbezogene Daten verarbeitet werden. Das Verfahrensverzeichnis nach § 4d BDSG ist ein Ausgangspunkt zur Identifizierung von Verarbeitungsverfahren. Sollte dies nicht vorliegen ist eine Bestandsaufnahme zwingend erforderlich. In der Grundverordnung ist dies in **Art. 30 DS-GVO** „Verzeichnis von Verarbeitungstätigkeiten" beschrieben. Die identifizierten Verarbeitungstätigkeiten sind dann nach den in der Verordnung genannten Anforderungen zu beschreiben und zu dokumentieren.

Wichtig: Anforderungen an personenbezogene Daten (**Art. 4 Abs. 1 DS-GVO**) prüfen. Besondere Anforderungen bestehen für den Umgang mit personenbezogenen Daten von Kindern, wenn es um die Einwilligung in Bezug auf Dienste der Informationsgesellschaft geht (**Art. 8 DS-GVO**).

4. Dokumentation organisieren

Die DS-GVO enthält an verschiedenen Stellen Dokumentationspflichten, beispielsweise in **Art. 30 DS-GVO** (Verzeichnis von Verarbeitungstätigkeiten), in **Art. 33 Abs. 5 DS-GVO** (Dokumentation von Datenschutzvorfällen) oder auch in **Art. 28 Abs. 3 lit. a DS-GVO** (Dokumentation von Weisungen im Rahmen von Auftragsverarbeitungsverhältnissen).

Checkliste

Umsetzungsleitfaden / -hinweise zur EU-DSGVO

5. Rechtsgrundlage prüfen

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

Auslegung: Die Erwägungsgründe der DS-GVO können zur Auslegung herangezogen werden. Sie entfalten zwar keine unmittelbare normative Wirkung, verdeutlichen aber Motive und bieten Erläuterungen.

6. Verträge checken

Unternehmen sollten insbesondere ihre bestehenden Verträge zur Auftragsverarbeitung überprüfen und überarbeiten. In den **Art. 26 bis 28 DS-GVO** sind Vorgaben für Vereinbarungen mit Auftragsverarbeitern und zwischen gemeinsam für die Verarbeitung Verantwortlichen geregelt.

7. Sicherheit der Verarbeitung sowie Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellung

Zum Schutz der in Bezug auf die Verarbeitung personenbezogener Daten bestehenden Rechte und Freiheiten natürlicher Personen ist es erforderlich, dass geeignete technische und organisatorische Maßnahmen unter Berücksichtigung des Stands der Technik getroffen werden (**Art. 32 DS-GVO**). Darüber hinaus enthält die DS-GVO bestimmte Rahmenbedingungen für die Art und Weise, wie die Anforderungen der DS-GVO schon bei der Prozessgestaltung und bei Voreinstellungen („Privacy-by-Design" und „Privacy-by-Default") umzusetzen sind (**Art. 25 DS-GVO**).

8. Datenschutz-Folgeabschätzung 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 (**Art. 35 DS-GVO**). An eine Datenschutz-Folgeabschätzung kann sich eine verpflichtende Konsultation der zuständigen Aufsichtsbehörde anschließen (**Art. 36 DS-GVO**).

9. Betroffenenrechte und Informationspflichten umsetzten

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

10. Melde- und Konsultationspflichten organisieren

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

Zuständige Datenschutzbehörde: Nach **Art. 55 Abs. 1 DS-GVO** ist jede Aufsichtsbehörde für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig.

Quelle: [LDI NRW]