Industrie- und Handelskammer
zu Dortmund

Checkliste "EU-Datenschutz-Grundverordnung"

Kontakt: Ass. Jost Leuchtenberg, j.leuchtenberg@dortmund.ihk.de (Stand: Januar 2018)

1 Sensibilisierung

Wenn am **25. Mai 2018** die *Datenschutz-Grundverordnung (DSGVO)* in Kraft tritt, ändert sich auch in Deutschland mehr als nur der Name der wichtigsten Datenschutzvorschriften. Für die Geschäftsführungen, Datenschutzbeauftragten und alle für das Thema Datenschutz im Unternehmen Zuständigen ist es daher notwendig, sich auf die möglichen Auswirkungen dieser neuen EU-Verordnung vorzubereiten. Da diese Auswirkungen längst nicht „nur" juristischer Natur sein werden, sollte das Projekt *„Start in die DSGVO"* in jedem Unternehmen als datenverarbeitende Stelle möglichst breit angelegt werden. Den Einstieg in die dabei anzustellenden Überlegungen soll diese Checkliste ein wenig erleichtern. Einen deutlich umfangreicheren Leitfaden zur DSGVO hat z.B. der Verband Bitkom (www.bitkom.org) entwickelt, anhand dessen die Unternehmen die richtigen Prozesse in Gang setzen können (Fundstelle: Kapitel 10). Da die wesentlichen Herausforderungen auf der (dv-)technischen sowie auf der organisatorischen Ebene liegen, ist das rechtzeitige Hinzuziehen einschlägiger Spezialisten aber oftmals das „Gebot der Stunde".

2 Bestandsaufnahme

Um feststellen zu können, wo gegebenenfalls Anpassungen erforderlich sind, sollte eine sorgfältige Bestandsaufnahme sämtlicher Prozesse und Verfahren durchgeführt werden, in denen personenbezogene Daten verarbeitet werden. Ein möglichst aktuelles Verfahrensverzeichnis nach § 4 d Bundesdatenschutzgesetz (BDSG) kann dabei ein wertvoller Anknüpfungspunkt sein. Wegen des gegenüber dem BDSG deutlich stärker risikobasierten Ansatzes der DSGVO kommen neben der Nutzung bereits bestehender Datenschutzstrukturen auch die Adaption von Prozessen und Strukturen eines bestehenden Compliance-Managements oder Qualitätsmanagementsystems in Betracht.

3 Risikoanalyse

Auf der Basis dieser Bestandsaufnahme ist sodann eine auf das gesamte Unternehmen und die einzelnen Geschäftsbereiche bezogene Risikoanalyse empfehlenswert. Denkbare Risiken sind z.B.:

- Betroffenenrechte
- Arbeitsrechtliche Aspekte
- Umgang mit Aufsichtsbehörden
- Mögliche Bußgelder
- Reputationsschäden
- Zivilrechtliche Haftungsrisiken

4 Gap-(= Lücken-)Analyse

Für die erfolgreiche Umsetzung der Vorgaben der DSGVO sollte im Unternehmen ein strukturierter Abgleich des Ist-Zustandes mit dem künftigen Soll-Zustand vorgenommen werden. Denn erst wenn man die zu schließende „Lücke" (engl.: gap) kennt, lassen sich alle weiteren Schritte planen. Insbesondere bei der Umsetzung vorgeschriebener Transparenz- und Dokumentationspflichten ist die Gap-Analyse ein wichtiger Baustein der Projektplanung. In einem ersten Schritt sollten alle von der Umsetzung der DSGVO betroffenen Organisationseinheiten und

Prozesse und rechtlichen Einheiten identifiziert werden. Unternehmen sollten außerdem ihre bestehenden Verträge mit Auftragsdatenverarbeitern (ADV) überprüfen und bei Bedarf überarbeiten lassen.

5 Einbindung des Datenschutzbeauftragten

Der betriebliche oder externe Datenschutzbeauftragte muss ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden. Außerdem sollte das Unternehmen die Umsetzung dieser Anforderung in einer dem Art. 24 Abs. 1 DSGVO entsprechenden Weise dokumentieren. Der Datenschutzbeauftragte ist nicht nur fachlicher Experte auf dem Gebiet des Datenschutzes; er ist zugleich auch verpflichtet, sein Unternehmen und die Beschäftigten in Datenschutzfragen zu beraten. Neben der Erfüllung der rechtlichen Pflichten ist die Einrichtung einer im Unternehmen gut kommunizierten und akzeptierten Datenschutzberatung ein wichtiges Mittel, um Fehler bei der Verarbeitung personenbezogener Daten und daraus folgende Risiken zu vermeiden.

6 Datenschutzkommunikation

Viele Unternehmen werden dem Datenschutz aufgrund der Vorgaben der DSGVO in Zukunft einen höheren Stellenwert zumessen müssen als nach den bisherigen Vorgaben des BDSG. Dies setzt ein klares Bekenntnis der Unternehmensführung zum Datenschutz sowie eine klare Kommunikation gegenüber der Belegschaft und den Kunden voraus. Bei größeren Unternehmen bietet sich dazu – sofern nicht bereits vorhanden – die Einführung einer Datenschutzrichtlinie oder eine entsprechende Überarbeitung der EDV-Richtlinie an.

7 Mitarbeiterschulungen

Aufgrund der Komplexität des Themas sollten von den Änderungen im Bereich Datenschutz betroffene Mitarbeiter gründlich geschult werden. Der Datenschutzbeauftragte ist nach Art. 39 Abs. 1 lit. b) der DSGVO ausdrücklich zur *„Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter“* angehalten.

8 Betriebsrat und Betriebsvereinbarungen

Die DSGVO zählt zu den Schutzvorschriften, über die der Betriebsrat zum Schutz der Arbeitnehmer zu wachen hat. Aus Unternehmersicht empfiehlt es sich deshalb, den Betriebsrat in die Prozesse zur Umsetzung der DSGVO frühzeitig mit einzubeziehen. Aufgrund der DSGVO werden zudem sicherlich zumeist Anpassungen bestehender Betriebsvereinbarungen – oder der Abschluss neuer Betriebsvereinbarungen – notwendig.

9 Rechtzeitige Planung neuer Prozesse und Strukturen

Aufgrund der Anforderungen der DSGVO werden auch Prozesse neu zu etablieren bzw. neue Strukturen zu schaffen sein. Zu denken ist dabei etwa an folgende Anforderungen:

a) Datenschutzdokumentation

Die DSGVO enthält zahlreiche Dokumentationspflichten, wie etwa das Führen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO), die Dokumentation von Weisungen bei Auftragsverarbeitungsverhältnissen (Art. 28 Abs. 3 lit. a) DSGVO) sowie die rechtzeitige Meldung von Datenschutzvorfällen (Art. 33 Abs. 5 DSGVO).

b) “Privacy by design, privacy by default”

Unternehmen sind nach Art. 25 DSGVO dazu verpflichtet, die geltenden Datenschutzvorschriften durch eine datenschutzfreundliche Gestaltung der eingesetzten IT und entsprechende Voreinstellungen umzusetzen. Unternehmen müssen dies durch geeignete technische Maßnahmen umsetzen, etwa durch auf Datenminimierung ausgerichtete IT-Systeme und eine möglichst frühzeitige Pseudonymisierung von personenbezogenen Daten.

c) Transparenzgebot

Eines der wichtigsten Gebote der DSGVO ist das Transparenzgebot. Die von der Verarbeitung personenbezogener Daten betroffenen Personen müssen von der verantwortlichen Stelle über

eine Vielzahl von Angaben bezüglich der geplanten Datenverarbeitung rechtzeitig informiert werden. Dies äußert sich in gegenüber dem bisherigen BDSG deutlich erweiterten Mitteilungs- und Hinweispflichten (Art. 13 u. 14 DSGVO). So müssen etwa Zweck und Zweckänderung einer erstmaligen Erhebung oder geplanten Datenverarbeitung gegenüber den Betroffenen transparent kommuniziert werden. Darüber hinaus werden Unternehmen verpflichtet, ein Löschkonzept mit entsprechenden Löschfristen zu entwickeln.

d) Datenschutzfolgenabschätzung

Sofern eine geplante Datenverarbeitung hohe Risiken für die Rechte und Freiheiten natürlicher Personen beinhaltet, ist der Verantwortliche verpflichtet, vor dem erstmaligen Einsatz des Verfahrens eine sog. Folgenabschätzung (Art. 35 DSGVO) durchzuführen. Hierzu sollte in den Unternehmen rechtzeitig ein Konzept zur Durchführung und Dokumentation eines solchen Verfahrens erarbeitet werden.

e) Beschwerdemanagement zur Wahrung der Betroffenenrechte

Nach der DSGVO stehen den von einer Verarbeitung von personenbezogenen Daten betroffenen Personen verschiedenen Mechanismen zur Geltendmachung ihrer Rechte zur Verfügung. Dies äußert sich etwa in dem Auskunftsrecht nach Art. 15 DSGVO, das deutlich umfangreicher ist als das bisher nach § 34 BDSG bestehende. Außerdem sieht die DSGVO u.a. ein Recht auf Berichtigung (Art. 16 DSGVO), das „Recht auf Vergessenwerden“ (Art. 17 Abs. 2 DSGVO), ein Recht auf Datenübertragbarkeit (Art. 20 DSGVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 Abs. 1 DSGVO) sowie ein Widerspruchsrecht (Art. 21 DSGVO) vor. Die Umsetzung dieser Betroffenenrechte legt nahe, dass Unternehmen ein entsprechendes Beschwerdemanagement einrichten sollten, um die Geltendmachung der genannten Ansprüche umsetzen zu können und damit verbundene Haftungsrisiken zu minimieren.

f) Vertragsmanagement

Unternehmen sollten ein Vertragsmanagement für Verträge mit datenschutzrechtlichem Bezug einführen und bis zur Geltung der DSGVO sicherstellen, dass bestehende Auftragsdatenverarbeitungsverträge (ADV), Verträge zur Übermittlung von personenbezogenen Daten und sonstige Verträge, die die Verarbeitung personenbezogener Daten beinhalten, den Anforderungen der Art. 28 und 29 DSGVO entsprechen.

g) Einwilligungsmanagement

Die DSGVO stellt hohe Anforderungen an die Einwilligung betroffener Personen in die Verarbeitung ihrer personenbezogenen Daten. Daher sollte strukturiert geprüft und dokumentiert werden, an welchen Stellen personenbezogene Daten auf welcher Grundlage verarbeitet werden, um bestehende Prozesse von den bisherigen Vorgaben auf die des Art. 7 DSGVO umzustellen. Nach dem Beschluss des Düsseldorfer Kreises vom 14. September 2016 gelten bisher erteilte Einwilligungen fort, sofern sie der Art nach den Bedingungen der DSGVO entsprechen (Erwägungsgrund 171, Satz 3 DSGVO). Bereits rechtswirksam erteilte Einwilligungen erfüllen grundsätzlich diese Bedingungen. Informationspflichten nach Art. 13 DSGVO müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.

10 Weiterführende Lektüre

Leitfaden zur DSGVO des Bitkom e. V. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.; download unter: https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/161109-EU-DS-GVO-FAQ-03.pdf