Industrie- und Handelskammer
zu Dortmund

Merkblatt "EU-Datenschutz-Grundverordnung"

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

1 Allgemeines

Die *Datenschutz-Grundverordnung (DSGVO)* löst die bisherige Datenschutzrichtlinie aus dem Jahr 1995 ab und regelt den Datenschutz innerhalb der EU weitgehend einheitlich und verbindlich. In Deutschland unmittelbar anwendbar ist die Verordnung ab dem **25. Mai 2018**. Aufgrund des für EU-Verordnungen geltenden Anwendungsvorrangs gilt dann das bisherige Bundesdatenschutzgesetz (BDSG), soweit es der DSGVO widerspricht, nicht mehr. Daher wird auch ein „neues" BDSG als Teil des Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU (DSAnpUG-EU) am 25.05.2018 zusammen mit der DSGVO in Kraft treten. Doch allein juristisch lässt sich das Thema DSGVO keinesfalls erfassen. Weit mehr als in anderen Regelungsbereichen gilt hier: „Grau ist alle Theorie." Denn die wesentlichen Herausforderungen liegen auf der (dv-)technischen sowie auf der organisatorischen Ebene. Daher dürfte hier das rechtzeitige Hinzuziehen einschlägiger Spezialisten auch oftmals das „Gebot der Stunde" sein.

2 Räumlicher Anwendungsbereich der DSGVO – das Marktortprinzip

Der räumliche Anwendungsbereich der DSGVO orientiert sich nicht am Sitz eines Unternehmens, sondern daran, ob ein Anbieter von Waren oder Dienstleistungen personenbezogene Daten von in der EU befindlichen Personen verarbeitet. Dies soll dem Verbraucherschutz Rechnung tragen und gleiche Anforderungen für alle Marktteilnehmer aufstellen. Daneben ist die DSGVO auch dann anzuwenden, wenn die Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU dient. Hierunter fallen etwa auch die Analyse des „Surfverhaltens" im Internet und die Speicherung von Cookies, egal zu welchem Zweck.

3 Grundsätze der Datenverarbeitung

Die Grundsätze der Datenverarbeitung bleiben im Kern bestehen. In Art. 5 DSGVO werden die bekannten Grundsätze der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben, der Zweckbindung, der Datensparsamkeit, der Richtigkeit sowie der Begrenzung der Speicherdauer genannt und durch die „Integrität und Vertraulichkeit" der Datenverarbeitung ergänzt. Die Zweckbindung wird dadurch gestärkt, dass sie nun durch die Verordnung ohne Abweichungsmöglichkeit der Mitgliedstaaten verbindlich ist und die Betroffenen vor Zweckänderungen der Datennutzungen informiert werden müssen. Die Nutzung von zweckgebunden erhobenen Daten zu einem mit dem ursprünglichen Erhebungszweck unvereinbaren Zweck ist nicht zulässig. Für eine solche Zweckänderung müssen die Daten also auf rechtmäßigem Weg erneut erhoben werden.

4 Verzeichnis aller Datenverarbeitungstätigkeiten

Art. 30 DSGVO ordnet an, dass Verantwortliche und Auftragsdatenverarbeiter ein Verzeichnis über alle Verarbeitungstätigkeiten unter der Angabe der dort genannten Punkte führen müssen. Dieses Verzeichnis ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen.

5 Erweiterung der Informationspflichten

Um die Verwendung von Daten nachvollziehbar zu machen, wurden die Informationspflichten der Datenverarbeiter gegenüber den Betroffenen in Art. 13 und 14 DSGVO erheblich erweitert. Danach ist der Betroffene vor der Erhebung personenbezogener Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache über die in den Artikeln genannten Verwendungsgesichtspunkte zu informieren. Im Einzelnen sind dies:

- Name und Kontaktdaten des für die Datenerhebung Verantwortlichen
- die Kontaktdaten des Datenschutzbeauftragten
- die Zwecke und die Rechtsgrundlage der Verarbeitung
- das berechtigte Interesse des Verantwortlichen oder eines Dritten
- Empfänger der personenbezogenen Daten
- die Absicht der Übermittlung an ein Drittland oder eine internationale Organisation.

Daneben ist der Betroffene auch zu informieren über

- die voraussichtliche Dauer der Datennutzung
- die betroffenen Rechte auf Auskunft, Berichtigung, Löschung und eventuelle Einschränkungen dieser Rechte
- das Recht auf jederzeitigen Widerruf der Einwilligung
- das Beschwerderecht bei einer Aufsichtsbehörde
- die Bereitstellung der personenbezogenen Daten
- eine automatische Entscheidungsfindung.

Falls die Daten nicht vom Betroffenen stammen, ist dieser in gleicher Weise zu informieren und darüber hinaus über die Quelle seiner Daten in Kenntnis zu setzen.

6 Recht auf Löschung, nicht auf „Vergessen“

Art. 17 DSGVO enthält ein Recht auf Löschung. Es handelt sich insofern nicht um ein Recht auf „Vergessen“, denn der Betroffene muss selbst die Löschung verlangen. Dann allerdings ist der Verantwortliche verpflichtet, die Löschung unter den dort genannten Voraussetzungen unverzüglich vorzunehmen. Wurden personenbezogene Daten über einen Betroffenen öffentlich gemacht (Internetveröffentlichung!), ist der Verantwortliche zusätzlich dazu verpflichtet, angemessene Maßnahmen zu treffen und andere verantwortliche Stellen darüber zu informieren, wenn der Betroffene die Löschung aller Links zu diesen Daten sowie von Kopien verlangt hat.

7 Personenbezogene Daten von Kindern

Erstmals wird in Art. 8 DSGVO ausdrücklich festgelegt, dass eine Einwilligung in die Verarbeitung personenbezogener Daten erst mit 16 Jahren möglich ist. Jüngere Personen bedürfen der vorherigen elterlichen Einwilligung. Eine nachträgliche elterliche Genehmigung ist dagegen nicht ausreichend.

8 Datenschutzfolgenabschätzung

Die DSGVO verlangt natürlich nicht bei jeder Datenverarbeitung eine Meldung an die Aufsichtsbehörde, sondern fordert von den Verpflichteten eine sog. Datenschutzfolgenabschätzung. Diese muss durchgeführt werden, wenn durch die Datenverarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen besteht. Unabhängig vom Risiko ordnet Art. 35 DSGVO für besonders sensible Fälle die zwingende Durchführung der Folgenabschätzung an. Dies sind die automatische Verarbeitung von Daten, Profilbildungsmaßnahmen und die systematische Überwachung öffentlich zugänglicher Bereiche. Weitere Fälle werden durch die Aufsichtsbehörden in Form einer „Blacklist“ und einer „Whitelist“ festgelegt.

9 Prinzip des „One-Stop-Shop“

Das Prinzip des „One-Stop-Shop“ – oder der einheitlichen Anlaufstelle – besagt, dass künftig für grenzüberschreitende Datenvereinbarungen innerhalb der EU grundsätzlich die Aufsichtsbehörde am Sitz der Hauptniederlassung federführend zuständig sein wird. Diese ist dann auch alleiniger Ansprechpartner für die Verpflichteten.

10 Meldepflicht von „Datenpannen“

Die Verletzung des Schutzes personenbezogener Daten muss der Verantwortliche, also etwa das Unternehmen, ohne schuldhaftes Zögern und möglichst binnen 72 Stunden nachdem die Verletzung bekannt wurde, der zuständigen Aufsichtsbehörde melden, sofern nicht ein Risiko für die Rechte und Freiheiten natürlicher Personen ausgeschlossen ist (Art. 33 DSGVO).

11 Haftung

Durch die DSGVO wird die Haftung erheblich verschärft. So wird bei Verstößen gegen die Grundprinzipien der DSGVO ein Bußgeld von bis zu 20 Mio. EUR oder bis zu vier Prozent des weltweiten letztjährigen Jahresumsatzes angedroht. Für leichtere Verstöße gegen Pflichten aus der DSGVO ist ein Bußgeld von maximal zehn Mio. EUR oder von zwei Prozent des weltweiten letztjährigen Jahresumsatzes vorgesehen.

12 Weiterführende Lektüre

Einen ausführlichen Leitfaden zur DSGVO hat der Bitkom e. V. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. entwickelt. Er steht im Internet zum download bereit unter:

https://www.bitkom.org/NP-Themen/NP-Vertrauen-Sicherheit/Datenschutz/161109-EU-DS-GVO-FAQ-03.pdf

---