

Überblick über die Neuerungen

I. Wesentliche Neuerungen der Europäischen Datenschutzgrundverordnung (EU-DSGVO)

1. Räumlicher Anwendungsbereich – das Marktortprinzip

Die EU-DSGVO stellt für ihre räumliche Geltung nicht mehr auf den Sitz eines Unternehmens ab, sondern darauf ob ein Anbieter von entgeltlichen oder unentgeltlichen Waren oder Dienstleistungen personenbezogene Daten von in der EU befindlichen Personen verarbeitet. Diese Erweiterung dient dem Verbraucherschutz und stellt gleiche Anforderungen für alle Marktteilnehmer auf. Daneben ist die EU-DSGVO auch dann anzuwenden, wenn die Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU dient. Unter Letzteres fällt die Analyse des Surfverhaltens im Internet und auch die Speicherung von Cookies, egal zu welchem Zweck (Art. 3 Abs. 2 EU-DSGVO).

2. Grundsätze der Datenverarbeitung

An den Grundsätzen der Datenverarbeitung wurde im Kern nichts geändert. In Art. 5 EU-DSGVO werden die bekannten Grundsätze der Rechtmäßigkeit, der Verarbeitung nach Treu und Glauben, der Zweckbindung, der Datensparsamkeit, der Richtigkeit, 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 nun 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.

3. Verzeichnis aller Datenverarbeitungstätigkeiten

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

4. Erweiterung der Informationspflichten

Um die Verwendung von Daten nachvollziehbar zu machen wurden die Informationspflichten der Datenverarbeiter gegenüber den Betroffenen in Art. 14 und 15 EU-DSGVO erheblich erweitert. Der Betroffene ist vor Erhebung von personenbezogenen 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 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

zu informieren. 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.

5. „Recht auf Vergessenwerden“

In Art. 17 EU-DSGVO wird das Recht auf Löschung niedergelegt. Es handelt sich insofern nicht um ein Recht auf Vergessen, als dass der Betroffene selbst die Löschung verlangen muss. Dann allerdings ist der Verantwortliche verpflichtet die Löschung unter den im Artikel genannten Voraussetzungen unverzüglich vorzunehmen. Wurden die personenbezogenen Daten über einen Betroffenen öffentlich (gerade bei Internetveröffentlichungen) gemacht, ist der Verantwortliche künftig zusätzlich dazu verpflichtet, angemessene Maßnahmen zu treffen und andere verantwortliche Stellen darüber zu informieren, dass der Betroffene die Löschung aller Links zu diesen Daten sowie von Kopien verlangt.

6. Personenbezogene Daten von Kindern

Erstmals wird ausdrücklich festgelegt, dass eine Einwilligung in die Datenverarbeitung personenbezogener Daten erst mit 16 Jahren möglich ist. Zuvor bedarf es der elterlichen Einwilligung. Dabei ist wichtig, dass eine nachträgliche Genehmigung ausdrücklich ausgeschlossen ist.

7. Datenschutzfolgenabschätzung

Die EU-DSGVO verlangt 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 die EU-DSGVO in Art. 35 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 Whitelist festgelegt.

8. Prinzip des „One-Stop-Shop“

Das Prinzip des „One-Stop-Shop“, zu Deutsch das Prinzip 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.

9. Meldepflicht von „Datenpannen“

Die Verletzung des Schutzes personenbezogener Daten muss der Verantwortliche, bspw. 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 EU-DSGVO).

10. Haftung

Durch die EU-DSGVO wird die Haftung erheblich verschärft. So wird bei Verstößen gegen die Grundprinzipien der EU-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 EU-DSGVO ist ein Bußgeld von maximal zehn Mio. EUR oder von zwei Prozent des weltweiten letztjährigen Jahresumsatzes vorgesehen.