Industrie- und Handelskammer Dresden

Merkblatt

Datenschutzgrundverordnung (DS-GVO)

Neue Anforderung für Unternehmen

Ansprechpartner: Referat Recht

Eric Dreuse
Telefon: 0351 2802-194
Fax: 0351 2802-7194
dreuse.eric@dresden.ihk.de

Stand: 2022

Hinweis:

Neue Anforderungen für Unternehmen durch die DS-GVO

Die europäische Union hat mit der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Europäischen Rates am 27. April 2016 das Datenschutzrecht innerhalb der Europäischen Union auf eine neue Basis gestellt. Die Datenschutz-Grundverordnung (DS-GVO) löst die bisherige Datenschutzrichtlinie aus dem Jahr 1995 ab und regelt den Datenschutz innerhalb der EU weitgehend einheitlich und verbindlich. Darum können die EU-Mitgliedsstaaten von den meisten Regeln nicht mehr durch nationale Gesetze abweichen. Für eigene Regelungen sieht die Verordnung jedoch sog. Öffnungsklauseln vor, durch welche die Mitgliedsstaaten eigene, abweichende Gesetze erlassen können. Diese beziehen sich aber oftmals nicht auf den Datenschutzstandard als solches, sondern lassen nur Raum zur Interpretation. Unmittelbar anwendbar ist die Verordnung ab dem 25. Mai 2018.

Welche Auswirkungen hat dies auf Deutschland?

Das bisherige Bundesdatenschutzgesetz (BDSG) kann aufgrund des für EU-Verordnungen geltenden Anwendungsvorrangs soweit es der DS-GVO widerspricht, nicht mehr angewendet werden. Der Bundesgesetzgeber plant daher eine Änderung des BDSG unter vielfacher Ausnutzung der Öffnungsklauseln. Aufgrund des schon bisher hohen Datenschutzniveaus in Deutschland, sind die Auswirkungen der DS-GVO nicht ganz so gravierend wie für andere EU-Länder. Nichtdestotrotz werden gerade an Unternehmen zukünftig verschärfte Datenschutzanforderungen gestellt.

1. Wesentliche Neuerungen:
Räumlicher Anwendungsbereich – das Marktortprinzip
Die DS-GVO 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 personengezogene Daten von in der EU befindlichen Personen verarbeitet. Diese Erweiterung dient dem Verbraucherschutz und stellt gleiche Anforderungen für alle Marktteilnehmer auf. Daneben ist die DS-GVO auch dann anzuwenden, wenn die Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU dient. Letzteres fällt die Analyse des Surfverhaltens im Internet und auch die Speicherung von Cookies, egal zu welchem Zweck (Art. 3 Abs. 2 DS-GVO).

2. Grundsätze der Datenverarbeitung
An den Grundsätzen der Datenverarbeitung wurde im Kern nichts geändert. In Art. 5 DS-GVO 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 von 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 DS-GVO ordnet an, dass Verantwortliche und Auftragsdatenverarbeiter ein Verzeichnis über alle Verarbeitungstätigkeiten und 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. 13 und 14 DS-GVO erheblich erweitert. Der Betroffene ist von der Erhebung von personenbezogenen Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfacher Sprache über die in den Artikeln genannten Verwendungsgesichtspunkten zu informieren. Im Einzelnen sind dies:

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

Daneben ist der Betroffene auch über

- die voraussichtliche Dauer der Datennutzung
- die betroffenen Rechte auf Auskunft, Vernichtung, 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 DS-GVO 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. Datenschutzfolgeabschätzung

Die DS-GVO verlangt nicht bei jeder Datenverarbeitung eine Meldung an die Aufsichtsbehörde, sondern fordert von den Verpflichteten eine sog. Datenschutzfolgeabschätzung. Diese muss durchgeführt werden, wenn durch die Datenverarbeitung voraussichtlich ein hohes Risiko für Rechte und Freiheiten natürlicher Personen besteht. Unabhängig vom Risiko ordnet die DS-GVO in Art. 35 für besonders sensible Fälle die zwingende Durchführung der Folgeabschätzung an. Dies sind die automatische Verarbeitung von Daten, Profilbildmaßnahmen 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 Datenverarbeitung 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 für „Datenpannen“

Die Verletzung des Schutzes personenbezogener Daten muss der Verantwortliche, bzw. 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 DS-GVO).

10. Haftung

Durch die DS_GVO wird die Haftung erheblich verschärft. So wird bei Verstößen gegen die Grundprinzipien der DS-GVO 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 DS-GVO ist ein Bußgeld von maximal 10 Mio. EUR oder von zwei Prozent des weltweiten letztjährigen Jahresumsatzes vorgesehen.

(Quelle: IHK Münster)

Auf dem Weg zur EU-Datenschutz-Grundverordnung – Checkliste für Unternehmen –

1. Sensibilisierung

Geschäftsführungen, Datenschutzbeauftragte und andere für das Thema Datenschutz Zuständige sollten innerhalb des Unternehmens dafür sensibilisieren, dass sich ab dem 25. Mai 2018 nicht nur der Name der wichtigsten Datenschutzvorschriften ändern wird. Die DS-GVO wird in vielen Bereichen direkte Auswirkungen auf jedes 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: Bis zum 24. Mai 2018 (einschließlich) gilt das Bundesdatenschutzgesetz!

2. Risikoanalyse

Vor allem aufgrund der steigenden Bußgeld- und Reputationsverlustrisiken sowie künftig drohender Schadenersatzforderungen betroffener Personen ist eine auf das gesamte Unternehmen und die einzelnen Geschäftsbereiche bezogene Risikoanalyse empfehlenswert. Denkbare Risiken sind beispielsweise:

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

3. Bestandsaufnahme

Um Änderungsbedarf identifizieren zu können, sollte eine Bestandsaufnahme sämtlicher Prozesse und Verfahren durchgeführt werden, in denen personenbezogene Daten verarbeitet werden. Ein möglichst aktuelles Verfahrensverzeichnis nach § 4 d Bundesdatenschutzgesetz (BDSG) kann ein wertvoller Ausgangspunkt zur Identifizierung sein. Wegen des gegenüber dem BDSG deutlich stärker risikobasierten Ansatzes der DS-GVO kommen neben der Nutzung bereits bestehender Datenschutzstrukturen auch die Adaption von Prozessen und Strukturen eines bestehenden Compliancemanagements oder Qualitätsmanagementsystems in Betracht.

4. Gap-Analyse

Das Unternehmen sollte für die erfolgreiche Umsetzung der Vorgaben der DS-GVO einen strukturierten Abgleich des Ist-Zustandes mit dem künftigen Soll-Zustand vornehmen. Auf dieser Grundlage lassen sich dann alle weiteren Schritte planen. Die Gap-Analyse ist ein wichtiger Baustein jeglicher Projektplanung zum Thema Datenschutz, insbesondere bei der Umsetzung vorgeschriebener Transparenz- und Dokumentationspflichten. In einem ersten Schritt der Gap-Analyse sollten alle von der Umsetzung der DS-GVO betroffenen Organisationseinheiten und Prozesse und rechtlichen Einheiten identifiziert werden. Unternehmen sollten außerdem insbesondere ihre bestehenden Verträge mit Auftragsdatenverarbeitern (ADV) überprüfen und überarbeiten.

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 DS-GVO entsprechenden Weise dokumentieren. Der Datenschutzbeauftragte ist gleichzeitig 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 für das Unternehmen und dessen Entscheidungsträger zu vermeiden.

6. Datenschutzkommunikation

Viele Unternehmen werden dem Datenschutz aufgrund der Vorgaben der DS-GVO 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 entsprechende 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 und den vielfältigen Anforderungen der DS-GVO sollten von den Änderungen betroffene Mitarbeiter gründlich im Umgang mit den Neuregelungen geschult werden. Der Datenschutzbeauftragte ist nach Art. 39 Abs. 1 lit. b der DS-GVO ausdrücklich zur „Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter“ angehalten.

8. Betriebsrat und Betriebsvereinbarungen

Die DS-GVO zählt zu den Schutzvorschriften, über die der Betriebsrat zum Schutz der Arbeitnehmer zu wachen hat. Aus Unternehmersicht empfiehlt es sich deshalb zu Fragen der Umsetzung der DS-GVO frühzeitig den Betriebsrat in die Umsetzungsprozesse mit einzubeziehen. Aufgrund der DS-GVO werden außerdem teilweise erhebliche Anpassungen bei bestehenden Betriebsvereinbarungen notwendig. Zudem kann auch der Abschluss neuer Betriebsvereinbarungen Sinn machen.

9. Rechtzeitige Planung neuer Prozesse und Strukturen

Nach der DS-GVO werden zahlreiche neue Prozesse und Strukturen vorausgesetzt, die die Unternehmen bis Ende Mai 2018 umsetzen müssen. Dabei sollten insbesondere folgende Anforderungen besonders berücksichtigt werden:

a) Datenschutzdokumentation

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

b) Privacy by design, privacy by default

Unternehmen sind in Zukunft nach Art. 25 DS-GVO 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) Transparenz

Eines der wichtigsten Gebote der DS-GVO 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 BDSG deutlich erweiterten Mitteilungs- und Hinweispflichten (Art. 13 u. 14 DS-GVO). 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 DS-GVO) 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 DS-GVO 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 DS-GVO, das deutlich umfangreicher ist als das bisher nach § 34 BDSG bestehende. Außerdem sieht die DS-GVO u. a. ein Recht auf Berichtigung (Art. 16 DS-GVO), das „Recht auf Vergessen-werden“ (Art. 17 Abs. 2 DS-GVO), ein Recht auf Datenübertragbarkeit (Art. 20 DS-GVO), das Recht auf Einschränkung der Verarbeitung (Art. 18 Abs. 1 DS-GVO) sowie ein Widerspruchsrecht (Art. 21 DS-GVO) vor. Die Umsetzung dieser Betroffenenrechte legt nahe, dass Unternehmen ein entsprechendes Beschwerdemanagement einrichten sollten, um die Geltendmachung der genannten Ansprüche umsetzen zu können, andernfalls droht eine Haftung.

f) Vertragsmanagement

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

g) Einwilligungsmanagement
Die DS-GVO 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 DS-GVO umzustellen. Nach dem Beschluss des Düsseldorfer Kreises vom 14. September 2016 gelten bisher erteilte Einwilligungen fort, sofern sie der Art nach den Bedingungen der Datenschutz-Grundverordnung entsprechen (Erwägungsgrund 171, Satz 3 DS-GVO). Bereits rechtswirksam erteilte Einwilligungen erfüllen grundsätzlich diese Bedingungen. Informationspflichten nach Art. 13 DS-GVO müssen dafür nicht erfüllt sein, da sie keine Bedingungen im Sinne des genannten Erwägungsgrundes sind.

Weitere Informationen zu den einzelnen Punkten finden Sie in den weiteren Merkblättern zur Datenschutzgrundverordnung