DATENSCHUTZ - D01

Stand: Februar 2020

Ihr Ansprechpartner
Ass. iur. Kim Pleines
E-Mail
kim.pleines@saarland.ihk.de
Tel.
(0681) 9520-640
Fax
(0681) 9520-690

EU-Datenschutz-Grundverordnung

I. Hintergrund

Seit dem 25. Mai 2018 gilt die **DSGVO unmittelbar** in allen Mitgliedstaaten der EU. Insgesamt besteht die DSGVO aus 99 Artikeln und annähernd doppelt so vielen Erwägungsgründen, die der Erläuterung dienen sollen.

Ziel der Verordnung ist es, europaweit ein **einheitliches Datenschutzniveau** zu erreichen sowie den Datenschutz an die zwischenzeitliche **technische Weiterentwicklung des Internets** und die **fortschreitende wirtschaftliche Globalisierung** anzupassen.

Obwohl die Staaten von den meisten Regeln aufgrund der Vereinheitlichung nicht mehr abweichen können, lässt die Verordnung für bestimmte Bereiche wie den Beschäftigtendatenschutz oder den betrieblichen Datenschutzbeauftragten - im Rahmen von **Öffnungsklauseln** - den einzelnen Mitgliedstaaten die Möglichkeit nationaler Regelungen. Regelungen zum Datenschutz finden sich neben dem Bundesdatenschutzgesetz (BDSG) auch in zahlreichen Spezialgesetzen.

II. Was sind die Grundsätze der DSGVO?

Beim Datenschutz geht es um den **Schutz personenbezogener Daten.** Davon sind alle Informationen umfasst, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen, wie Name, Geburtsdatum oder IP-Adresse. Der Anwendungsbereich der DSGVO ist sehr weit gefasst. Es geht um den Schutz dieser Daten als Ausfluss des **Persönlichkeitsrechts** einer jeden Person.

Der Datenschutz wird durch die DSGVO nicht neu erfunden. Es bleibt grundsätzlich bei den bisherigen Zielen und Grundsätzen des Datenschutzes. Diese Grundsätze, die bei einer automatisierten Verarbeitung personenbezogener Daten zu beachten sind, werden in Art. 5 DSGVO aufgelistet:

1. Verbot mit Erlaubnisvorbehalt
Grundsätzlich ist eine Datenverarbeitung verboten, da die Verarbeitung in das verfassungsrechtlich geschützte Persönlichkeitsrecht einer jeden Person eingreift. Eine Datenverarbeitung kann nur dann vorgenommen werden, wenn sie erlaubt ist. Die Erlaubnis kann sich durch ein Gesetz ergeben oder auf einem Vertrag oder auf einer Einwilligung der betroffenen Person beruhen.

2. Rechtmäßigkeit
Die Verarbeitung von Daten ist dann rechtmäßig, wenn sie auf einer entsprechenden Grundlage beruht (Rechtsgrundlage, Vertrag, Einwilligung usw.) und der Zwecke der Verarbeitung von der Rechtsgrundlage bzw. der Einwilligung umfasst ist.

3. Transparenz
Die betroffene Person muss wissen, wer welche Daten für welchen Zweck verarbeitet. Daher gibt es umfangreiche Betroffenenrechte (z. B. Informationspflichten, Auskunftsrechte, Recht auf Berichtigung der Daten, Widerspruchsrecht).

4. Zweckbindung
Die DSGVO sieht eine enge Zweckbindung vor. Personenbezogene Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden. Ausnahmen sind vorgesehen für sog. kompatible Zwecke, also Zweckänderungen, die aber mit dem ursprünglichen Zweck eng zusammenhängen.

5. Datenminimierung
Es dürfen nur die personenbezogenen Daten verarbeitet werden, die für die Zweckerreichung notwendig sind.

6. Richtigkeit
Die Daten müssen richtig sein, weshalb alle angemessenen Maßnahmen zu treffen sind, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden.

7. Speicherbegrenzung
Personenbezogene Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist (Datensparsamkeit). Sind sie nicht mehr erforderlich, müssen sie gelöscht werden. Zudem sind alle Möglichkeiten zur Anonymisierung von Daten zu nutzen.

8. Integrität und Vertraulichkeit
Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet. Die DSGVO verknüpft sehr stark den Datenschutz mit der Technik. Die IT-Verfahren müssen somit schon von Anfang an darauf ausgerichtet sein, möglichst wenig personenbezogene Daten verarbeiten zu können (privacy by design).

9. Rechenschaftspflicht
Dies ist der wichtigste Aspekt aller Grundsätze. Die Einhaltung der dargestellten Grundsätze für die Verarbeitung personenbezogener Daten ist durch den Verantwortlichen = Unternehmer nachzuweisen. Auch in kleineren und mittleren Unternehmen muss ein Mindestmaß an Dokumentation vorhanden sein, um die Einhaltung des Datenschutzes nachweisen zu können.

III. Wann dürfen Daten verarbeitet werden?

Prinzipiell gilt bei der Datenverarbeitung der Grundsatz, **dass jegliche Verarbeitung personenbezogener Daten verboten ist, es sei denn, es gibt eine Erlaubnis nach Art. 6 DSGVO dafür.** Obwohl dieser Grundsatz mit Blick auf die fortschreitende Digitalisierung manch einem befremdlich erscheinen mag, ist er die Konsequenz des **Grundrechts auf informationelle Selbstbestimmung** und Bestandteil der Europäischen Menschenrechtskonvention.

1. Einwilligung

Die Datenverarbeitung ist rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben hat.

➔**D02** „Einwilligung nach der DSGVO“, **Kennzahl 2158**

2. Vertrag

Daten, die zur Erfüllung eines Vertrags oder einer vorvertraglichen Maßnahme benötigt werden, dürfen zulässig erhoben werden.

3. Rechtliche Verpflichtung

Sofern ein anderes Gesetz die Erhebung und Verarbeitung von personenbezogenen Daten vorsieht, liegt eine rechtliche Verpflichtung für den Verantwortlichen vor. Eine Verarbeitung der Daten zur Erfüllung dieser Pflicht ist dann in dem gesetzlich vorgegebenen Rahmen zulässig.

4. Wahrung berechtigter Interessen

Die Verarbeitung ist rechtmäßig, wenn sie für die Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, und die Interessen der betroffenen Person diese Interessen nicht überwiegen.

5. Weiterverarbeitung

Unter bestimmten Voraussetzungen können personenbezogene Daten auch weiterverarbeitet werden, wenn die Verarbeitung nicht mehr dem ursprünglichen Zweck entspricht. Hierfür muss der neue Zweck mit dem alten kompatibel, darf also für die betroffene Person nicht überraschend sein. Die Prüfung umfasst insbesondere folgende Punkte:

- jede **Verbindung zwischen den Zwecken**
- der **Zusammenhang der Erhebung der Daten,** insbesondere hinsichtlich des Verhältnisses zwischen der betroffenen Person und dem Verantwortlichen
- die **Art der personenbezogenen Daten** (z. B. besonders sensible Daten)
- die **möglichen Folgen** der beabsichtigten Weiterverarbeitung für die betroffenen Personen
- Vorhandensein geeigneter Garantien wie **Verschlüsselungen oder Pseudonymisierungen** der Daten.

Ergibt die vom Verantwortlichen durchgeführte Prüfung, dass der Zweck nicht kompatibel ist, ist eine darauf gestützte Verarbeitung unzulässig, es sei denn, es wird für den neuen Zweck wiederum eine Einwilligung eingeholt.

IV. Was gilt seit 2018?

1. Die wichtigsten Neuerungen der DSGVO für Unternehmen sind:

- **Wegfall des Schriftformerfordernisses bei Einwilligungen:**

  Die DSGVO sieht keine bestimmte Form für die Erteilung einer Einwilligung vor. Sie kann **schriftlich, elektronisch oder mündlich** erfolgen.

- **Erweiterung der Informationspflichten:**

  In Art. 13 und Art. 14 DSGVO wurden die Informationspflichten gegenüber den Betroffenen erheblich **erweitert,** um für eine bessere **Nachvollziehbarkeit der Datenverwendung** zu sorgen.

  ➔**D05** „Informationspflichten nach der DSGVO“, **Kennzahl 2158**

- **Erweiterung der Dokumentationspflichten:**

  Eine zentrale Änderung durch die DSGVO ist die Einführung der „Rechenschaftspflicht“, welche gem. Art. 5 Abs. 2 DSGVO von den Verantwortlichen fordert, dass sie „die Einhaltung des Gesetzes nachweisen können“. Es reicht nicht mehr aus, sich nur an die Regelungen der Verordnung zu halten. Vielmehr müssen Unternehmen jederzeit die Rechtmäßigkeit der Datenverarbeitung nachweisen können.

  Allein der **fehlende Nachweis** kann **hohe Bußgelder** zur Folge haben, auch wenn die Datenverarbeitung rechtmäßig erfolgte.

  Im Zusammenhang mit der Rechenschaftspflicht steht das **Verzeichnis aller Datenverarbeitungsvorgänge.** Art. 30 DSGVO ordnet an, dass Verantwortliche und Auftragsdatenverarbeiter ein Verzeichnis über alle Verarbeitungstätigkeiten unter der Angabe der im Artikel genannten Punkte führen müssen.

  ➔**D11** „Verzeichnis von Verarbeitungstätigkeiten“, **Kennzahl 2158**

- **Einführung der Datenschutzfolgenabschätzung:**

  Die DSGVO führt für die Verarbeitung von personenbezogenen Daten einen **risikobasierten Ansatz** ein. Ähnlich der bisherigen Vorabkontrolle sollen auf der Grundlage einer Risikoanalyse die Folgen der Verarbeitung abgeschätzt werden, um frühzeitig Schutzmaßnahmen ergreifen zu können. Es gilt: Je risikoreicher und schadensgeneigter eine Verarbeitung von Daten für Betroffene sein kann, umso höhere Anforderungen stellt die Verordnung an die Anwendung. Die DSGVO nennt in Art. 35 Abs. 3 bestimmte **Fallgruppen,** bei denen eine **Folgenabschätzung stets durchzuführen** ist.

  Dazu gehören:

  - das **Profiling**
  - die **Verarbeitung besonders sensibler Daten** (Art. 9 Abs. 1 und Art. 10 DS-GV0)
  - die **umfangreiche Videoüberwachung** öffentlich zugänglicher Bereiche

  Eine Blacklist für Verarbeitungen, bei denen eine Datenschutzfolgeabschätzung durchzuführen ist, können Sie hier nachlesen.

- **Erhöhung der Bußgelder:**

  Seit Inkrafttreten der DSGVO ist die Haftung erheblich verschärft. Bei Verstößen gegen die Grundprinzipien der Verordnung drohen Geldbußen von bis zu 20 Mio. EUR oder bis zu vier Prozent des weltweiten letztjährigen Jahresumsatzes. 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.

2. Weitere wesentliche Neuerungen der DSGVO sind:

- **Räumlicher Anwendungsbereich (Marktortprinzip):**

  Das Europäische Datenschutzrecht gilt nach der Verordnung nicht nur für die in der EU niedergelassenen Unternehmen. Voraussetzung ist nach Art. 3 Abs. 2 DSGVO lediglich, dass sich ein Angebot an einen bestimmten nationalen **Markt in der EU** richtet oder dass die Datenverarbeitung der Beobachtung des Verhaltens von **Personen in der EU** dient. Der Anwendungsbereich erstreckt sich damit auch auf außereuropäische Unternehmen, die auf dem europäischen Markt tätig sind (Marktortprinzip).

- **Betroffenenrechte**

  Die Rechte des Betroffenen gegenüber der Verantwortlichen Stelle werden erweitert. Neben dem bislang bereits eingeräumten Recht auf Auskuft, Berichtigung und Löschung, hat der Betroffene auch ein Recht auf Einschränkung der Verarbeitung, ein Recht auf Datenübertragung, ein Beschwerderecht und ein Widerspruchsrecht.

  ➔**D05** „Informationspflichten nach der DSGVO“, **Kennzahl 2158**

  Personenbezogene Daten von Kindern:

  Zum ersten Mal ausdrücklich geregelt ist, dass eine Einwilligung in die Verarbeitung personenbezogener Daten erst im Alter von **16 Jahren** möglich ist. Zuvor bedarf es der elterlichen Einwilligung. Dabei ist wichtig, dass eine nachträgliche Genehmigung ausdrücklich ausgeschlossen ist.

- **Prinzip des "One-Stop-Shop":**

  Durch die DSGVO wird die Zuständigkeit der Aufsichtsbehörden vereinheitlicht. Mit dem Prinzip des „One-Stop-Shop“, zu Deutsch: das Prinzip der einheitlichen Anlaufstelle, wird festgehalten, dass künftig für grenzüberschreitende Datenvereinbarungen innerhalb der EU grundsätzlich die **Aufsichtsbehörde am Sitz der Hauptniederlassung** federführend zuständig sein wird.

- **Meldepflichten 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. Beim Unabhängigen Datenschutzzentrum Saarland kann eine Meldung auch elektronisch erfolgen.