MERKBLATT Recht und Steuern

EU-Datenschutz-Grundverordnung

Datenschutz ist nichts Neues. In Deutschland gibt es ihn schon seit Jahrzehnten, und auch auf EU-Ebene war er bereits seit 1995 geregelt. Die EU-Datenschutz-Grundverordnung (DS-GVO), schafft aber ein weit umfangreicheres Rechtsregime, an das sich alle Unternehmen halten müssen.

Der Grundsatz lautet schlicht: Jegliche Verarbeitung personenbezogener Daten ist verboten, es sei denn, es gibt einen Erlaubnistatbestand dafür. Dieser Satz scheint angesichts einer fortschreitenden Digitalisierung befremdlich, aber er ist Konsequenz des Grundrechtschutzes der personenbezogenen Daten, wie er vom Bundesverfassungsgericht festgeschrieben wurde („informationelle Selbstbestimmung"), und er ist Inhalt der Europäischen Menschenrechtskonvention.

Die EU-Datenschutz-Grundverordnung (DS-GVO) verlangt von den Unternehmen die Erfüllung der Rechenschaftspflicht. Damit ist die verantwortliche Stelle, also das Unternehmen oder die Institution, verantwortlich für den Datenschutz und seine Beachtung. Dazu ist ein Datenschutzmanagement notwendig. Auch in kleineren und mittleren Unternehmen muss ein Mindestmaß an Dokumentation vorhanden sein, um die Einhaltung des Datenschutzes nachweisen zu können. Denn die Verletzung der Datenschutzpflichten zieht empfindliche Bußgelder nach sich: bis zu 20 Mio. Euro oder 4 % des weltweiten Umsatzes können von den Aufsichtsbehörden verhängt werden.

Inhalt

Ihre Ansprechpartner:
Fachbereich Recht und Steuern
Tel: 0331-2786 203 / Fax: 0331-2842 914
E-Mail: recht@ihk-potsdam.de
www.ihk-potsdam.de

Stand: 03.2022

1. Was regelt die DS-GVO?

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 DS-GVO ist sehr weit gefasst. Es geht um den Schutz dieser Daten als Ausfluss des Persönlichkeitsrechts einer jeden Person.
In Artikel 6 DS-GVO sind die verschiedenen Zulässigkeitsgründe für eine Verarbeitung aufgelistet:

a. Einwilligung

Die betroffene Person muss über den Umfang der Daten, die verarbeitet werden sollen, sowie den Zweck, zu dem sie verarbeitet werden, ausreichend informiert werden. Die Einwilligung muss nicht mehr schriftlich erteilt werden. Ihre Erteilung muss aber nachweisbar sein. Insofern ist eine Protokollierung elektronischer Einwilligungen sinnvoll.
Die Einwilligungserklärung muss in leicht zugänglicher und verständlicher Form und in einer klaren und einfachen Sprache vorhanden sein. Bei der Einholung einer Einwilligung muss die betroffene Person darauf hingewiesen werden, dass sie ihre Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Eine Gegenleistung darf nicht an die Einwilligung in die Verarbeitung von Daten gekoppelt werden, die für die Verarbeitung der Daten nicht erforderlich sind.
Eine auf der Website voreingestellte Einwilligung in Form eines Häkchens („Ich willige in die Verarbeitung meiner Daten ein") ist keine Einwilligung. Die betroffene Person muss handeln und aktiv ihr Einverständnis ausdrücken. Wenn die Einwilligung zusammen mit anderen Erklärungen verlangt wird, muss sie besonders hervorgehoben sein (z. B. drucktechnisch oder als Kasten).

Beachte: Bei Kindern, die das 16. Lebensjahr noch nicht vollendet haben, müssen die Erziehungsberechtigten einwilligen, Art. 8 Abs. 1 DS-GVO.

b. Vertrag

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

c. Rechtliche Verpflichtung

Sofern der Verantwortliche eine rechtliche Verpflichtung erfüllen muss und dafür Daten benötigt (z. B. Erhebung der Religionszugehörigkeit im Beschäftigungsverhältnis wegen der Kirchensteuer), dürfen diese ebenfalls erhoben werden.

d. Berechtigte Interessen

Kann vorliegen, wenn die Verarbeitung für die Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, und die Interessen der betroffenen Person diese Interessen nicht überwiegen. Erforderlich ist hier immer eine Abwägung der jeweiligen Interessen

Hierunter kann z. B. die Verarbeitung personenbezogener Daten für die Direktwerbung fallen (siehe insbesondere Erwägungsgrund 47 der DS-GVO).

e. Weiterverarbeitung

Unter bestimmten Voraussetzungen können personenbezogene Daten auch dann weiterverarbeitet werden, wenn die Verarbeitung nicht mehr dem ursprünglichen Zweck entspricht. Erforderlich ist hier, dass der neue Zweck mit dem alten kompatibel, also für die betroffene Person nicht überraschend ist. Hierfür muss der Verantwortliche eine genaue – dokumentierte – Prüfung anhand der in Art. 6 Abs. 4 DS-GVO festgelegten Kriterien durchführen. Zu prüfen ist:

- 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,
- vorhandene Verschlüsselungen oder Pseudonymisierungen der Daten.

Ergibt die Prüfung, dass der Zweck nicht kompatibel ist, ist eine darauf gestützte Verarbeitung unzulässig, es sei denn, der Verantwortliche holt für den neuen Zweck wiederum die Einwilligung der betroffenen Person ein.

f. Rechtsgrundlagen

Die DS-GVO, aber auch das Bundesdatenschutzgesetz (BDSG) und die Landesdatenschutzgesetze (LDSG) enthalten selbst Erlaubnistatbestände, nach denen eine Datenverarbeitung zulässig ist. Hierzu gehören insbesondere Regelungen zur Videoüberwachung und zum Beschäftigtendatenschutz.

2. Was sind die Grundsätze der DS-GVO?

Art. 5 DS-GVO beinhaltet die Grundsätze, die bei einer Verarbeitung personenbezogener Daten zu beachten sind:

- Verbot mit Erlaubnisvorbehalt

Da die Verarbeitung personenbezogener Daten in das verfassungsrechtlich geschützte Persönlichkeitsrecht eingreift, ist eine Datenverarbeitung grundsätzlich verboten. Nur, wenn sie z. B. gesetzlich erlaubt oder auf der Einwilligung der betroffenen Person beruht, ist sie erlaubt.

- Rechtmäßigkeit

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

- 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).

- Zweckbindung

Die Daten dürfen nur für die genannten Zwecke verarbeitet werden. Ausnahmen sind vorgesehen für sog. kompatible Zwecke, also Zweckänderungen, die aber mit dem ursprünglichen Zweck eng zusammenhängen.

- Datenminimierung

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

- Richtigkeit

Die Daten müssen richtig sein, anderenfalls müssen sie berichtigt oder gelöscht werden.

- Speicherbegrenzung

Die Datensparsamkeit ist hierbei zu beachten. Es geht um die Frage, wann Daten nicht mehr benötigt werden und daher zu löschen sind. Zudem sind alle Möglichkeiten zur Anonymisierung von Daten zu nutzen.

- Integrität und Vertraulichkeit

Die DS-GVO verknüpft sehr stark den Datenschutz mit der Technik. IT-Verfahren müssen schon von Anfang an darauf ausgerichtet sein, möglichst wenig personenbezogene Daten verarbeiten zu können (privacy by design).

- Rechenschaftspflicht

Die verantwortliche Stelle, also das Unternehmen oder die Institution ist verantwortlich für den Datenschutz und seine Beachtung. Dazu ist ein Datenschutzmanagement notwendig – natürlich abhängig von der Größe des Unternehmens, der personenbezogenen Daten, die verarbeitet werden und der Menge und der Qualität der Daten.
Zumindest muss aber auch in kleineren und mittleren Unternehmen ein Mindestmaß an Dokumentation vorhanden sein, um die Einhaltung des Datenschutzes nachweisen zu können.

3. Datenschutzmanagement

a. Planung und Konzeption

Die Risiken, die sich aus der Datenverarbeitung in dem Unternehmen ergeben, müssen hinsichtlich Art, Umfang, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit von Verletzungen und Schäden beachtet werden. Insbesondere geht es um die Risiken für die persönlichen Rechte und Freiheiten der betroffenen Personen.

Das Unternehmen muss also seine „Datenschutzpolitik" beschreiben und damit festlegen:

- die Zuständigkeiten für den Datenschutz im Unternehmen, hierzu gehört auch (wenn erforderlich) die Einbindung und Aufgabenstellung eines betrieblichen Datenschutzbeauftragten;

- die Sensibilisierung und Schulung der Mitarbeiter;

- Verpflichtung der Mitarbeiter und ggf. Dritter auf das Datengeheimnis (dies ist zwar gesetzlich nicht mehr ausdrücklich vorgeschrieben, aber anzuraten; alternativ ist sicherzustellen, dass die Mitarbeiter, die personenbezogenen Daten verarbeiten, dies nur entsprechend ihrer Aufgabenerfüllung tun. Auch für Auftragsverarbeiter ist vorgeschrieben, dass diese ihre Mitarbeiter auf die Vertraulichkeit verpflichten müssen.

- die Durchführung von Kontrollen, dass die getroffenen Regelungen/Anweisungen eingehalten werden;

- den Einsatz datenschutzfreundlicher Technologien;

- den Stand der Technik als Anforderung an die IT-Sicherheit;

- die Führung des Verzeichnisses von Verarbeitungstätigkeiten;

- den Prozess zum Abschluss von Auftragsverarbeitungen oder – bei gemeinsamer Verantwortlichkeit – zum Abschluss entsprechender Vereinbarungen;

- den Prozess zur Umsetzung der Betroffenenrechte und der Transparenz der Datenverarbeitung;

- den Prozess zur Durchführung einer Risikobewertung;

- den Prozess zur Durchführung von Datenschutz-Folgenabschätzungen und einer eventuellen Meldung an die Aufsichtsbehörde;

- den Prozess zur Meldung von Verletzungen des Datenschutzes (Datenpannen).

Es sollte geprüft werden, ob es im Unternehmen Anknüpfungspunkte für ein Datenschutzmanagement gibt. Hierfür bieten sich z. B. bereits bestehende Compliance-Richtlinien oder ein Qualitätsmanagement sowie ein IT-Sicherheits- oder ein Risikomanagement an.

b. Umsetzung

Hiervon umfasst ist die Konkretisierung der genannten Maßnahmen in der Praxis. Dazu gehört eine ausreichende Dokumentation sowie geeignete technisch-organisatorische Maßnahmen.

c. Erfolgskontrolle und Überwachung

Die Planung und Konzeption sowie ihre Umsetzung müssen stetig auf ihre Wirksamkeit hin kontrolliert werden.

d. Optimierung und Verbesserung

Wird unter c. festgestellt, dass Anpassungen notwendig sind, müssen sie vorgenommen werden. Hierzu gehört auch die Erfüllung des angemessenen Stands der Technik bei den technischen IT-Sicherheitsmaßnahmen, denn die DS-GVO verlangt die Anpassung an entsprechende technische Entwicklungen.

Ergebnis muss sein, dass die Rechtskonformität der Verarbeitung personenbezogener Daten in rechtlicher, technischer und organisatorischer Hinsicht jederzeit nachweisbar ist.

Hinweis: Dieses Merkblatt richtet sich an Mitgliedsunternehmen der IHK Potsdam und an Personen, die eine Unternehmensgründung im Kammerbezirk Potsdam anstreben. Es soll - als Service Ihrer IHK Potsdam - nur erste Hinweise geben und erhebt keinen Anspruch auf Vollständigkeit. Obwohl es mit größtmöglicher Sorgfalt erstellt wurde, kann eine Haftung für die inhaltliche Richtigkeit nicht übernommen werden.

Ihre Ansprechpartner:

Fachbereich Recht und Steuern
Tel: 0331-2786 203 / Fax: 0331-2842 914
E-Mail: recht@ihk-potsdam.de
www.ihk-potsdam.de