



Datenschutzrecht

Allgemeines zur Datenschutzgrundverordnung EU

Datenschutz ist nichts Neues. In Deutschland gibt es ihn schon seit Jahrzehnten, und auch auf EU-Ebene war er bereits seit 1995 geregelt. Die neue gesetzliche Vorschrift, die EU-Datenschutz-Grundverordnung (DSGVO), schafft aber ein neues und weit umfangreicheres Rechtsregime. Daran müssen sich alle Unternehmen halten.

Was ändert sich im Datenschutz?

Am 14. April 2016 verabschiedete das Europäische Parlament die EU-Datenschutz-Grundverordnung. Sie ist am 25. Mai 2016 in Kraft getreten, gilt aber erst nach einer zweijährigen Übergangsfrist. Dieser Zeitraum dient den nationalen Gesetzgebern, die bisher geltenden Gesetze wie das Bundesdatenschutzgesetz (BDSG) anzupassen. Unternehmen sind angehalten, die Übergangszeit bis zum Gültigwerden der Verordnung zu nutzen, um die internen Datenverarbeitungsprozesse auf Anpassungsbedarf zu überprüfen. Außerdem sollte bei Neuanschaffungen von Datensystemen darauf geachtet werden, dass diese, soweit zum jetzigen Zeitpunkt möglich, die neuen Datenschutzregelungen bereits berücksichtigen.

Jedenfalls ab dem 25. Mai 2018 wird die DSGVO die bisherige EG-Datenschutzrichtlinie 95/46 und die nationalen Vorschriften wie das BDSG in weiten Teilen ablösen bzw. ersetzen. Sie gilt direkt, d. h. Unternehmen müssen sowohl den Text der VO als auch das Nachfolgegesetz zum BDSG als Rechtsgrundlagen für den Datenschutz verwenden.

Was regelt die Datenschutzgrundverordnung?

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.

Was sind die Grundsätze der DSGVO?

Art. 5 DSGVO 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 Zweck 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, also die Frage, wann Daten nicht mehr benötigt und daher gelöscht werden können. Zudem sind alle Möglichkeiten zur Anonymisierung von Daten zu nutzen.

- **Integrität und Vertraulichkeit**

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).

- **Rechenschaftspflicht**

Das ist der wichtigste Aspekt der Grundsätze! Die verantwortliche Stelle, also das Unternehmen oder die Institution sind 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. 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.