Das neue Datenschutzrecht

Die Europäische Datenschutz-Grundverordnung

Die Europäische Datenschutz-Grundverordnung (DS-GVO[1]) wird nach einer zweijährigen Übergangszeit das Bundesdatenschutzgesetz (BDSG) größtenteils ablösen. Ab dem 25.05.2018 gilt die Verordnung europaweit einheitlich und unmittelbar in allen Mitgliedstaaten. Unternehmen in Deutschland müssen daher ihr derzeitiges Datenschutzmanagement anhand der neuen Rechtslage überprüfen und gegebenenfalls anpassen. Diese Prüfung ist Bestandteil des unternehmenseigenen Risikomanagements, denn etwaige Verstöße gegen die Datenschutz-Grundverordnung können für Unternehmen erhebliche Nachteile mit sich bringen. Die möglichen Geldbußen seitens der Aufsichtsbehörden wurden drastisch auf bis zu 20 Millionen EUR oder im Fall eines Unternehmens auf bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs erhöht (Art. 83 Abs. 5). Daneben drohen Schadensersatzansprüche von Betroffenen (Art. 82) und Verbandsklagen (Art. 80). Sollten etwaige Verstöße in der Öffentlichkeit bekannt werden, drohen zudem erhebliche Reputationsschäden. Ziel eines jeden Unternehmens muss es daher sein, diese Risiken zu analysieren und anschließend zu minimieren.

Ausgangspunkt: Verarbeitung personenbezogener Daten

Der Ausgangspunkt des Datenschutzrechts ist das personenbezogene Datum. Nur wenn ein solches verarbeitet wird, ist die Datenschutz-Grundverordnung überhaupt anwendbar (Art. 2 Abs. 1). Hierunter versteht man alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Nr. 1). Eine Person ist identifizierbar, wenn sie direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann. Werden dagegen anonyme Daten verarbeitet, finden die datenschutzrechtlichen Vorschriften keine Anwendung (EwG 26 DS-GVO). Als „Datenverarbeitung“ bezeichnet man jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung (Art. 4 Nr. 2).

Um zu verstehen, ob die Vorschriften der Datenschutz-Grundverordnung für sie gelten, sollten sich Unternehmen einen Überblick über ihre Datenflüsse verschaffen und prüfen, ob sie personenbezogene Daten verarbeiten.

[1] Art sind solche der DS-GVO

DIE FAMILIENUNTERNEHMER e.V.
Charlottenstraße 24
10117 Berlin

Tel. 030 300 65-0
Fax 030 300 65-390
kontakt@familienunternehmer.eu
www.familienunternehmer.eu

Verantwortlichkeit

Werden personenbezogene Daten verarbeitet, sieht die Datenschutz-Grundverordnung diverse Regelungen und Handlungspflichten zum Schutz der betroffenen Personen vor. Um diese Regelungen effektiv umsetzen zu können, muss deutlich sein, wer die daraus folgenden Maßnahmen ergreifen soll. Zunächst ist also zu klären: „Wer ist verantwortlich für was gegenüber wem?“. Der Verantwortliche ist diejenige natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Art. 4 Nr. 7 DS-GVO). Dabei geht es nicht darum, wer formal über die Datenverarbeitung entscheidet, sondern wer sie wirklich veranlasst und maßgeblich beeinflusst. Der danach ermittelte Akteur („Wer?“) ist für die Verarbeitung personenbezogener Daten im Einklang mit der Datenschutz-Grundverordnung („für was?“) gegenüber dem Betroffenen und weiteren Kontrollstellen („gegenüber wem?“) verantwortlich.

Allgemeine Datenverarbeitungsgrundsätze

Wenn ein Unternehmen für die Verarbeitung personenbezogener Daten im Einklang mit der Datenschutz-Grundverordnung verantwortlich ist, erscheint es sinnvoll, sich zunächst einen Überblick über die Systematik und die wesentlichen Ziele der Verordnung zu verschaffen. Eine Hilfestellung hierfür können die allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten in Art. 5 DS-GVO leisten:

- Rechtmäßigkeit
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Datensicherheit bzw. „Integrität und Vertraulichkeit“
- Rechenschaftspflicht

Diese Grundsätze werden an vielen Stellen der Verordnung wieder aufgegriffen und durch detaillierte Regelungen konkretisiert. Im Folgenden sollen sie daher kurz beschrieben werden.

Rechtmäßigkeit

Danach muss sich jede Verarbeitung von personenbezogenen Daten auf eine Rechtsgrundlage stützen können. Ohne Rechtsgrundlage ist die Datenverarbeitung verboten (sog. Verbotsprinzip). Eine solche Rechtsgrundlage kann sich entweder aus der Datenschutz-Grundverordnung oder aus dem sonstigen Unionsrecht oder aus dem Recht der Mitgliedstaaten ergeben. In der Datenschutz-Grundverordnung ist Art. 6 DS-GVO die zentrale Vorschrift zur Zulässigkeit der Datenverarbeitung. Danach ist die Verarbeitung rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- Einwilligung des Betroffenen
- Erforderlichkeit zur Vertragserfüllung oder zum Vertragsabschluss
- Erforderlichkeit zur Erfüllung rechtlicher Verpflichtungen
- Erforderlichkeit zum Schutz lebenswichtiger Interessen
- Erforderlichkeit zur Wahrnehmung öffentlicher Aufgaben
- Erforderlichkeit zur Wahrung berechtigter Interessen

Nachdem Unternehmen sich einen Überblick über ihre Datenflüsse verschafft haben, sollten sie in einem nächsten Schritt prüfen, auf welchen Rechtsgrundlagen ihre Datenverarbeitung derzeit beruht und ob diese über den 25.05.2018 hinaus fortbestehen können. Das gilt insbesondere für Rechtsgrundlagen aus dem nationalen Recht.

Transparenz

Die Datenverarbeitung muss für den Betroffenen nachvollziehbar sein (Art. 5 Abs. 1 a). Der Betroffene soll verstehen, dass ihn betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten derzeit und künftig noch verarbeitet werden (EwG 39 DS-GVO). Dafür sieht die Datenschutz-Grundverordnung Informationspflichten des Verantwortlichen und ein Auskunftsrecht des Betroffenen (Art. 13, 14 und 15) vor. Alle diese Informationen müssen vom Verantwortlichen leicht verständlich, unverzüglich und unentgeltlich bereitgestellt werden (Art. 12 DS-GVO).
Unternehmen sollten daher zunächst feststellen, ob überhaupt Ablaufprozesse zur Erfüllung ihrer Transparenzpflichten bestehen. Falls ja, sollten sie abgleichen, in welchem Umfang und in welcher Form sie derzeit Informationen bereitstellen und ob dies den neuen Anforderungen der Art. 12 ff. DS-GVO entspricht.

Zweckfestlegung und -bindung

Der Verantwortliche muss bestimmte rechtmäßige Zwecke festlegen, für die die personenbezogenen Daten verarbeitet werden sollen (Art. 5 Abs. 1 b). Diese Zwecke müssen vor der erstmaligen Datenerhebung bestimmt werden. Werden sie erst später oder überhaupt nicht bestimmt, liegt eine unzulässige Datenverarbeitung „auf Vorrat“ vor. Werden die personenbezogenen Daten in der Zukunft weiterverarbeitet, so ist der Verantwortliche weiterhin an die ursprünglichen Zwecke gebunden. Die Verarbeitung für andere Zwecke (sog. Zweckänderung) ist nur unter strengen Voraussetzungen (Art. 6 Abs. 4 DS-GVO) möglich.

Unternehmen sollten sich daher vergewissern, dass vor Erhebung der personenbezogenen Daten eine Zweckfestlegung erfolgt und diese (beispielsweise in einem Verarbeitungsverzeichnis nach Art. 30) dokumentiert wird. Sollen die Daten später zu anderen Zwecken weiterverarbeitet werden, muss vorher geprüft werden, ob eine Zweckänderung zulässig ist.

Datenminimierung

Daten dürfen nur insoweit verarbeitet werden, wie es für die Erreichung des Zwecks erforderlich ist. (Art. 5 Abs. 1 c). Dazu muss der Verantwortliche zunächst prüfen, ob zur Erreichung des Zwecks überhaupt personenbezogene Daten erforderlich sind oder ob stattdessen anonymisierte Daten verarbeitet werden können (EwG 39). Sollte ersteres der Fall sein, dann sind die personenbezogenen Daten auf das notwendige Maß zu beschränken. Als Richtschnur hierfür gilt: „So wenig Daten wie möglich, so viele Daten wie nötig.“.

Unternehmen sollten prüfen, inwieweit ihre bisherige Datenverarbeitung mit diesem Grundsatz konform ist und gegebenenfalls Anpassungen vornehmen.

Richtigkeit

Die Verarbeitung von personenbezogenen Daten ist nach nur zulässig, wenn die Daten vollständig, richtig und (soweit erforderlich) aktuell sind (Art. 5 Abs. 1 d). Dies macht es notwendig, dass der Verantwortliche von sich aus die Daten regelmäßig auf ihre Korrektheit hin überprüft. Stellt er hierbei fest, dass Daten unrichtig sind, so müssen sie berichtigt oder gelöscht werden. Das Gleiche gilt für den Fall, dass ein Betroffener einen begründeten Berichtigungs- oder Löschungsanspruch (Art. 16, 17) geltend macht.

Unternehmen müssen daher sicherstellen, dass sie über Strukturen verfügen, die eine regelmäßige Überprüfung der Daten ermöglichen. Für die Reaktion auf Berichtigungs- und Löschungsansprüche sollten sie (wie auch bei den Transparenzpflichten) geeignete Ablaufprozesse implementieren.

Speicherbegrenzung

Personenbezogene Daten dürfen nur so lange gespeichert werden, wie dies für die Erreichung des Zwecks notwendig ist (Art. 5 Abs. 1 e). Danach sind die Daten zu löschen (Art. 17 Abs. 1 a). Eine Ausnahme hiervon gilt, wenn für das Unternehmen gesetzliche Aufbewahrungspflichten, beispielsweise aus dem Handelsgesetzbuch (HGB), bestehen (Art. 17 Abs. 3 b).

Unternehmen müssen prüfen, welche Löschfristen für sie gelten und anschließend ein individuelles Löschkonzept etablieren, das den Vorgaben des Art. 17 DSGVO entspricht.

Datensicherheit

Der Verantwortliche hat eine sichere Verarbeitung der Daten zu gewährleisten („Integrität und Vertraulichkeit“, Art. 5 Abs. 1 f). Datensicherheit bedeutet in diesem Kontext insbesondere Schutz vor Vernichtung, Verlust, Veränderung oder unbefugter Offenlegung der personenbezogenen Daten (Art. 32 Abs. 2). Das erforderliche Schutzniveau ist abhängig von der Risikobewertung. Je höher das Risiko einzuschätzen ist, desto stärkere Schutzmaßnahmen muss der Verantwortliche ergreifen.
Unternehmen sollten zwingend überprüfen, ob die vorliegenden Verarbeitungsstandards diesen Anforderungen entsprechen. Werden dabei Schwachstellen aufgedeckt, sind angemessene Maßnahmen zur Verbesserungen der Datensicherheit zu implementieren.

Rechenschaftspflicht

Die DS-GVO verpflichtet den Verantwortlichen, die rechtmäßige Verarbeitung der Daten entsprechend der zuvor genannten Grundsätze zu dokumentieren und gegebenenfalls nachzuweisen (Art. 5 Abs. 2). Im Streitfall muss der Verantwortliche nachweisen können, dass die Verarbeitung gemäß den Vorgaben der Datenschutz-Grundverordnung erfolgt ist.
Für Unternehmen bedeutet das, dass es zwingend erforderlich ist, ihre Datenverarbeitung vollständig zu dokumentieren, um in Konflikten die Rechtmäßigkeit ihres Handelns nachweisen zu können.

Ausblick

Die ab dem Jahr 2018 geltende Datenschutz-Grundverordnung bringt für Unternehmen einen nicht unerheblichen Mehraufwand mit sich. Abhängig vom Ist-Zustand des Datenschutzmanagements, der Komplexität der Datenverarbeitungsvorgänge und der vorhandenen Ressourcen im Unternehmen kann die zweijährige Übergangsfrist bis zum Stichtag knapp werden. Viele Unternehmen haben daher bereits mit der Umsetzung begonnen. Alle anderen sollten möglichst zeitig prüfen, wo sie jetzt stehen und welche Schritte bis zum 25.05.2018 noch zu gehen sind.

Für eine erste Bestandsaufnahme sollten daher folgende Fragen beantwortet werden:

- Welche Daten werden in Ihrem Unternehmen erhoben?
- Wie werden diese Daten aktuell genutzt?
- Ist die Speicherung und Verarbeitung dieser Daten erforderlich?
- Was ist der aktuelle und zukünftige Zweck der Erhebung und Verarbeitung?
- Darf Ihr Unternehmen die erhobenen Daten zum beabsichtigten Zweck nutzen?
- Hat Ihr Unternehmen überhaupt Zugriff auf die relevanten Daten?

Hierauf sollte Ihr Unternehmen aufbauen und die weiteren notwendigen Maßnahmen zur praktikablen Durchführung und rechtlichen Absicherung eines interessengerechten Datenmanagements treffen.

WHITE PAPER - ein Service von DIE FAMILIENUNTERNEHMER
Kommission Wettbewerbs- und Wirtschaftsrecht

April 2018 | im Auftrag von DIE FAMILIENUNTERNEHMER erstellt von
Ulrich Herfurth, Rechtsanwalt, Herfurth & Partner Rechtsanwaltsgesellschaft mbH, Hannover