

information oktober 2017

4. Überblick Datenschutz-Grundverordnung im Unternehmen (DS-GVO)

Die neue DS-GVO ist ab dem 25. Mai 2018 als unmittelbar geltendes Recht in Deutschland anzuwenden. Sie tritt dann an die Stelle des aktuell gültigen Bundesdatenschutzgesetz (BDSG) und wird zukünftig von einem neuen Bundesdatenschutzgesetz (BDSG n. F.) flankiert.

Nach einer durch das IT-Unternehmen Veritas in Auftrag gegebenen Umfrage bei weltweit über 900 Unternehmen bestehen noch erhebliche Mängel bei der Umsetzung der DS-GVO. Was müssen Unternehmen nun konkret veranlassen, um auch nach Inkrafttreten der DS-GVO noch gesetzeskonform zu handeln? Die unabhängige Datenschutzkonferenz des Bundes und der Länder empfiehlt dazu folgende Maßnahmen in ihrem aktuellen „Kurzpapier Nr. 8“:

a. Information der Geschäftsleitung - Die betrieblichen Datenschutzbeauftragten und/oder IT-Verantwortlichen müssen die Geschäftsleitung informieren, damit sich alle Entscheidungsträger der Auswirkungen der DS-GVO bewusst sind.

b. Start eines Projekts - Da verschiedene Personen bzw. Abteilungen im Unternehmen Verfahren zur Verarbeitung personenbezogener anwenden, müssen die Maßnahmen untereinander koordiniert werden. Es bietet sich daher an, ein eigenes Projekt mit dem Ziel zu initiieren, die Datenschutzkonzeption anhand eines Soll-Ist-Abgleichs zu aktualisieren.

aa. Bestandsaufnahme (Ist-Zustand) - Um ein genaues Verständnis davon zu bekommen, wie derzeit im Unternehmen mit personenbezogenen Daten umgegangen wird, sollten die aktuell vorhandenen Prozesse, Rechtsgrundlagen und die Datenschutzorganisation im Detail analysiert werden.

bb. Ermittlung Handlungsbedarf - Nunmehr ist der Soll-Zustand nach der DS-GVO zu ermitteln und im Anschluss daran eine Lückenanalyse zwischen dem Ist-Zustand und dem künftigen Soll-Zustand durchzuführen:

- *Verbot mit Erlaubnisvorbehalt*: Auch zukünftig ist für jede Verarbeitung personenbezogener Daten eine Legitimationsgrundlage erforderlich. Für alle Prozesse ist daher eine Rechtsgrundlage erforderlich. Sofern sich die Verarbeitung auf eine Einwilligung stützt, sind die Anforderungen des Art. 7 DS-GVO einzuhalten.

- *Betroffenenrechte*: Den betroffenen Personen stehen umfangreichere Rechte zu, die das Unternehmen zu beachten hat (z. B. Informationspflichten gegenüber den betroffenen Personen, Art. 13 und Art. 14; Auskunftsrecht, Art. 15; Recht auf Berichtigung, Art. 16; Recht auf Löschung Art. 17; neu: Recht auf Datenübertragbarkeit Art. 20; Widerspruchsrecht, Art. 21 DS-GVO).

- *Schutz durch Gestaltung und Voreinstellungen*: Die DS-GVO gibt spezifische Rahmenbedingungen vor, wie Datenschutzvorgaben schon bei der Prozessgestaltung und bei den Voreinstellungen umzusetzen sind (sog. „Data Protection by design“ und „Data Protection by default“ Art. 25 DS-GVO).

- *Dienstleistungsbeziehungen*: Die bestehenden Verträge zur Auftragsdatenverarbeitung bedürfen der Prüfung anhand der Vorgaben aus Art. 28 und 29 DS-GVO.

- *Dokumentationspflichten*: Die DS-GVO enthält weit reichende Pflichten zum Nachweis und an die Dokumentation, dass personenbezogene Daten rechtmäßig verarbeitet werden (Rechenschaftspflicht, Art. 5 Abs. 2; Verarbeitungsverzeichnis, Art. 30; Dokumentation von Datenschutzvorfällen, Art. 33 Abs. 5 und von Weisungen bei Auftragsdatenverarbeitung, Art. 28 Abs. 3 lit. a DS-GVO).

- *Datenschutz-Folgenabschätzung*: Die aus dem BDSG bekannte Vorabkontrolle wird durch eine Datenschutz-Folgenabschätzung mit Dokumentationspflicht abgelöst (Art. 35 DS-GVO). Diese kann durch die Aufsichtsbehörde überprüft werden (Art. 36 DS-GVO).

- *Meldepflichten*: Meldepflichten an die zuständige Aufsichtsbehörde bestehen sowohl bei einer Verletzung des Schutzes personenbezogener Daten (Art. 33 Abs. 1 DS-GVO) als auch hinsichtlich der Kontaktdaten des Datenschutzbeauftragten (Art. 37 Abs. 7 DS-GVO).

- *Datensicherheit*: Unternehmen müssen ein angemessenes Schutzniveau in Bezug auf Datensicherheit gewährleisten und die dazu implementierten Sicherungsmaßnahmen einer regelmäßigen Überprüfung unterziehen (Art. 24 und 32 DS-GVO).

- *Zertifizierung*: Im Rahmen eines Zertifizierungsverfahrens besteht die Möglichkeit, den Nachweis zu erbringen, dass die Datenverarbeitung im Einklang mit der DS-GVO erfolgt.

c. Umsetzung

Bei der Umsetzung sind dann die im Rahmen des Soll-Ist Abgleichs festgestellten Lücken entweder durch Anpassung oder erstmalige Einrichtung notwendiger Prozesse und Strukturen fristgerecht bis zum 25. Mai 2018 zu beseitigen.

Dr. Tilo Jung

+49 6221 4340230

tilo.jung@adjuga.com

Die Beiträge sind urheberrechtlich geschützt. Gerne dürfen Sie die „information oktober 2017“ an weitere Interessierte weiterleiten. Jede andere Verwendung ist nur nach Zustimmung durch die adjuga Rechtsanwaltsgesellschaft mbH unter Nennung der Quelle zulässig. Diese Information ersetzt nicht die rechtliche Beratung. Trotz sorgfältiger Erstellung übernimmt die adjuga Rechtsanwaltsgesellschaft mbH für die Richtigkeit keine Haftung.