

Von Steuerberater Thomas Meister, Wolfgang Sievert Steuerberatungsgesellschaft mbH

Die neue EU-Datenschutz-Grundverordnung (DSGVO)

In diesem Jahr ergeben sich grundlegende Änderungen im Datenschutzrecht. Ab dem 25. Mai 2018 gilt die EU-Datenschutz-Grundverordnung (DSGVO). Damit soll ein einheitlicher Datenschutzstandard in Europa geschaffen werden. Die bislang unterschiedlichen nationalen Bestimmungen werden im Sinne einer Vollharmonisierung abgelöst und in wesentlichen Punkten durch neue Vorschriften ersetzt.

Der deutsche Gesetzgeber hat parallel dazu ein neues Datenschutzgesetz (BDSG n.F.) verabschiedet, das ebenfalls zum 25. Mai 2018 in Kraft tritt und an die Stelle des aktuell noch gültigen Datenschutzgesetzes (BDSG) tritt.

Der wesentliche strukturelle Unterschied zur bisherigen Rechtslage besteht darin, dass die DSGVO unmittelbare Wirkung in allen EU-Mitgliedsstaaten entfaltet und nationale Regelungen nur noch dann zulässig sind, wenn die DSGVO ausdrücklich eine entsprechende Öffnungsklausel enthält.

Anbei werden exemplarisch vier umzusetzende Maßnahmen aufgelistet. Diese Auflistung ist nicht vollständig und stellt nur eine Auswahl dar:

Benennung eines Datenschutzbeauftragten

Neu ist mit der DSGVO die verpflichtende Benennung eines Datenschutzbeauftragten an die zuständigen Behörden. Diese Meldung hat zwingend bis zum 25. Mai 2018 zu erfolgen.

Gemäß § 38 BDSG n.F. ist ein Datenschutzbeauftragter zu benennen, soweit in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten im Unternehmen beschäftigt sind. Aber selbst, wenn kein Datenschutzbeauftragter zu benennen ist, sind die datenschutzrechtlichen Vorgaben selbstverständlich trotzdem einzuhalten.



Meldung von Datenpannen

Neu ist ebenfalls die Verpflichtung, Datenpannen innerhalb von 72 Stunden nach Bekanntwerden der Datenpanne an die zuständige Aufsichtsbehörde zu melden. Hier ist es vor allem wichtig, dass die Mitarbeiter hierfür sensibilisiert werden und diese auch wissen, wie die Meldungen zu erfolgen haben.

Interessant wird hier sein, wie die Aufsichtsbehörden mit den Meldungen umgehen werden. Eine Datenpanne liegt bereits vor, wenn eine E-Mail an einen Kunden versehentlich an einen falschen E-Mail-Empfänger versendet wird. Geht man davon aus, dass jede Datenpanne ge-

meldet wird, fragt sich, wie die Prüfung und Priorisierung der Fälle vorgenommen werden soll. Die Meldungen lassen Individualtexte zu und können somit nicht automatisiert gefiltert werden. Ich wage zu bezweifeln, dass genügend Mitarbeiter für die Prüfung der Datenpannen vorhanden sind.

Auftragsdatenverarbeitung regeln

Wenn Sie über einen externen Dienstleister automatisiert Daten verarbeiten lassen (z. B. Aktenvernichter, Entsorgung Hardware, Online-Datensicherung, Web-Hosting, Online-Visitenkartendruck) ist bei der Auftragsdatenverarbeitung nach Art. 28, 29 DSGVO weiterhin ein Auftragsverarbeitungsvertrag nötig. Dieser muss schriftlich oder in einem elektronischen Format vorliegen. Den Auftragsverarbeiter treffen zahlreiche neue Pflichten, wie z. B. die Pflicht zur Einrichtung eines Verfahrensverzeichnis (§ 30 Abs. 2 DSGVO) oder die Pflicht zur Durchführung technischer und organisatorischer Maßnahmen und zur Bestellung eines Datenschutzbeauftragten (Art. 32, 37 DSGVO). Ohne diesen Vertrag dürfen Sie keine personenbezogenen Daten zur Auftragsverarbeitung überlassen.

Verzeichnis der Verarbeitungstätigkeiten

Jedes Unternehmen, das „nicht nur gelegentlich“ Daten verarbeitet, muss nach Art. 30 Abs. 1, 3 DSGVO ein sogenanntes schriftliches oder elektronisches Verzeichnis führen; das



Steuerberater Thomas Meister, Wolfgang Sievert Steuerberatungsgesellschaft mbH

ist nicht neu. Neu ist, dass diese Pflicht nicht dem Datenschutzbeauftragten obliegt, sondern dem „Verantwortlichen“ i. S. des Art. 4 Abs. 1 Nr. 7 DSGVO, weshalb diese Pflicht künftig dem Vorstand oder Geschäftsführer (also dem Vertretungsorgan) zufällt. Erst wenn bekannt ist, in welche Prozesse personenbezogene Daten eingebunden sind (Datenerhebung), warum das passiert (Datensparsamkeit) und wer darauf Zugriff hat (Datenzugriff), können die Anforderungen der DSGVO an diese Verarbeitungsprozesse sowie die Rechte der Betroffenen zielführend umgesetzt werden.

Anhand dieser kleinen Auswahl wird deutlich, wie tief die neue DSGVO in die täglichen Prozesse eines jeden Unternehmens eingreift. Sofern noch nicht geschehen, machen Sie sich bitte schnellstmöglich mit dieser Thematik vertraut. Denn auch die Bußgelder bei Verstößen sind mit bis zu 20 Mio. EUR oder 4 Prozent des Jahresumsatzes deutlich erhöht worden. ■