Die neue EU-DSGVO.

Das müssen Sie beim Führen eines Verzeichnisses aller Verabeitungstätigkeiten beachten.

Nicht alle Regelungen der Datenschutz-Grundverordnung und der ab 25. Mai geltenden Fassung des Bundesdatenschutzgesetzes sind komplett neu.

Einiges ist schon – zumindest in ähnlicher Art und Weise – bekannt.

VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN DES VERANTWORTLICHEN

Mussten Firmen früher ein so genanntes Verfahrensverzeichnis führen, in dem alle Prozesse dokumentiert wurden, die personenbezogene Daten betrafen, so gibt es auch nach der Datenschutzgrundverordnung eine entsprechende Verpflichtung. Unternehmen müssen für jeden Prozess, der personenbezogene Daten verarbeitet, erfassen welchen Zweck dieser verfolgt, welche Personen bzw. Personengruppen davon betroffen sind und welche Art (Kategorien) personenbezogener Daten verarbeitet werden. Gemeint ist dabei die allgemeine Angabe, also zum Beispiel Name Anschrift, E-Mail-Adresse, Telefonnummer usw. der betroffenen Person.

OFFENLEGUNG VON DATEN

Wenn die Daten weitergegeben werden sollen – die DSGVO bezeichnet das als Offenlegung – dann müssen Angaben zu den Empfängern gemacht werden. Hier muss nicht jede Firma oder Behörde konkret benannt werden. Es ist ausreichend, wenn Gruppen gebildet werden, wie etwa Krankenkassen, Finanzämter, Lohnbüro, o.ä. Angaben zu einer geplanten Übermittlung in Länder außerhalb der EU oder an internationale Organisationen sowie welchen Regelungen die Übermittlung (sogenannte geeignete Garantien) unterliegt, müssen ebenfalls enthalten sein.

WEITERE ANGABEN IM VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Dazu kommen – sofern möglich – noch Angaben, wie lange die im Prozess verwendeten personenbezogenen Daten benötigt bzw. zu welchem Zeitpunkt diese gelöscht werden und wie die Daten und auch der Prozess abgesichert sind – die sogenannten technischen und organisatorischen Maßnahmen.Diese Angaben werden noch mit einigen allgemeinen Angaben, die in der Regel für die meisten Prozesse fast gleich sind, ergänzt: Angaben zur Firma, wie etwa Kontaktdaten oder eventuell mitverantwortliche Firmen, oder aber auch den Kontaktdaten des Datenschutzverantwortlichen.

VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN BEIM AUFTRAGSVERARBEITER

Etwas anders sieht es aus, wenn ein Unternehmen Dienstleistungen im Bereich der Verarbeitung personenbezogener Daten für andere Firmen erbringt – hier spricht man von einer sogenannten Auftragsverarbeitung. Aufgrund der DSGVO sind nun auch Auftragsverarbeiter zum Führen eines solchen Verzeichnisses verpflichtet. Im Gegensatz zu Verantwortlichen muss das Verzeichnis des Auftragsverarbeiters nur die folgenden Angaben enthalten: Name und Kontaktdaten des oder der Auftragsverarbeiter, die jedes Verantwortlichen in deren Auftrag die Verarbeitungen durchgeführt werden sowie die eines vorhandenen Datenschutzbeauftragten. Darüber hinaus sollten die Kategorien der Verarbeitungen, die im Auftrag der Verantwortlichen durchgeführt werden, angegeben werden. Hier empfiehlt es sich (auch wenn der Gesetzestext dies nicht ausdrücklich vorschreibt) eine klare Zuordnung der Verarbeitungen zu den jeweiligen Verantwortlichen vorzunehmen. Auch Angaben zu einer möglichen Übermittlung in Länder

pb-030_05/18

außerhalb der EU oder an internationale Organisationen müssen gemacht werden – inklusive der dafür geltenden Regelungen. Der Auftragsverarbeiter hat darüber hinaus, ebenso wie ein Verantwortlicher, Angaben darüber zu machen, wie die personenbezogenen Daten und die Verarbeitungsprozesse abgesichert sind.

AUSNAHME UND ÄNDERUNGEN GEGENÜBER DEM BISHERIGEN DATENSCHUTZRECHT

Auch wenn die DSGVO eine Ausnahme von der Pflicht zur Führung des Verzeichnisses für Unternehmen mit weniger als 250 Mitarbeitern unter bestimmten Voraussetzungen vorsieht, so sind die Bedingungen, die an diese Ausnahme geknüpft sind jedoch so streng, dass die Regelung in der Praxis nur sehr wenige Unternehmen betrifft und faktisch kaum ein Unternehmen umhin kommt, das Verzeichnis zu führen. Da diese Pflicht jedoch schon vor der neuen EU-DSGVO bestand, sollte sich bei Unternehmen, die sich bisher gesetzeskonform in Sachen Datenschutz verhalten haben, kein allzu großer Aufwand ergeben. Wegfallen wird mit der Anwendung der DSGVO allerdings die Pflicht den öffentlichen Teil des Verzeichnisses durch den Datenschutzbeauftragten jedem bereitzustellen. Zukünftig wird es keine Unterscheidung mehr zwischen öffentlichen und nichtöffentlichen Angaben geben. Auch die bisherige Meldepflicht des Verzeichnisses an die Aufsichtsbehörde für bestimmte Unternehmen fällt weg. Ab dem 25. Mai ist das Verzeichnis nur noch auf Anfrage den Aufsichtsbehörden zur Verfügung zu stellen.

ZUSAMMENARBEIT MIT DER AUFSICHTSBEHÖRDE

Eine relativ knappe Formulierung der DSGVO verpflichtet Unternehmen – egal ob Verantwortliche oder Auftragsverarbeiter – dazu, mit der Aufsichtsbehörde zusammenzuarbeiten. Dies dient vor allem dazu, den Aufsichtsbehörden ihre Arbeit als Kontrollstelle zu ermöglichen und Unternehmen dazu zu verpflichten, sich an Vorgaben der Aufsichtsbehörde zu halten oder auf entsprechende Nachfragen Auskunft zu erteilen. Eine besondere Rolle spielt dabei der Datenschutzbeauftragte, denn er fungiert als Ansprechpartner im Unternehmen für die Aufsichtsbehörde.

DATENSCHUTZ-FOLGENABSCHÄTZUNG UND VORHERIGE KONSULTATION

Für besondere Verarbeitungen sieht die Datenschutz-Grundverordnung eine so genannte Datenschutz-Folgenabschätzung vor. Dieses Werkzeug tritt die Nachfolge der bisherigen sogenannten Vorabkontrolle an – auch wenn die Aufsichtsbehörden betonen, dass sie nicht gleichgesetzt werden sollen. Bei der Datenschutz-Folgenabschätzung handelt es sich um einen Prozess der zwingend im Vorfeld der Verarbeitung durchgeführt wird und der eine Risikoabschätzung darstellt mit deren Hilfe entsprechende Maßnahmen oder Alternativen identifiziert werden sollen, die die Auswirkung auf die von der Verarbeitung betroffenen Personen verringern sollen. Da hierbei der Datenschutzbeauftragte einzubeziehen ist, führt die Pflicht einiger Unternehmen die Datenschutz-Folgenabschätzung durchzuführen häufig auch zur Pflicht diesen zu benennen. Der Datenschutzbeauftragte hat bei der Durchführung eine beratende und überwachende Funktion. Um sinnvoll beraten zu können, sollte er dabei auch den Standpunkt der betroffenen Personen nachvollziehen, um zu verhindern, dass bei der Datenschutz-Folgenabschätzung nur Risiken aus Unternehmersicht betrachtet werden. Der komplette Durchführungsprozess ist zusammen mit seinen Ergebnissen zu dokumentieren und auch regelmäßig fortzuschreiben, um die Aktualität der Maßnahmen in Hinblick auf neu hinzukommenden Herausforderungen und Risiken zu gewährleisten. Sofern sich keine Möglichkeit findet, die Risiken für die betroffenen Personen wirksam zu verringern, besteht für Unternehmen die Verpflichtung, die Aufsichtsbehörde zu konsultieren, sodass diese über die Durchführbarkeit des Verarbeitungsprozesses entscheidet. Bevor hohe Risiken nicht ausgeschlossen werden können, darf die betreffende Verarbeitung nicht begonnen werden, Unternehmen sollten daher im Vorfeld ausreichend Zeit einplanen, um entsprechend sorgsam die Datenschutz-Folgenabschätzung durchzuführen. Auch benötigen die Aufsichtsbehörden aufgrund der aktuellen Umstellungen auf die DSGVO Zeit, um die Konsultationsanfrage zu bearbeiten. Es handelt sich daher also in der Regel nicht um einen Prozess, der in zwei bis drei Wochen abgeschlossen sein wird.

pb-030_05/18

ÜBER DEN AUTOR

Thomas Schwenski ist externer Datenschutzbeauftragter und zertifizierter Information Security Officer. Mit über 15 Jahren Erfahrung im IT-Bereich berät er Firmen und Einzelunternehmer zur Umsetzung der neuen Datenschutzrichtlinien und unterstützt bei der Vorbereitung von Systemzertifizierungen nach ISO 27001.

Übrigens: Ob Ausbildung zum Datenschutzbeauftragten oder Auffrischung des Fachwissens – wir bieten für jeden Anspruch die passende Weiterbildung.

Weitere Informationen finden Sie hier:

www.tuv.com/datenschutz

pb-030_05/18

TÜV Rheinland Akademie
Am Grauen Stein
51105 Köln
akademie.tuv.com

TÜVRheinland®
Genau. Richtig.