DATENSCHUTZRECHT

MÄRZ 2018

Die Datenschutz-Grundverordnung – Das neue Datenschutzrecht ab dem 25.05.2018 (Teil 2)

Im ersten Teil der relevanten Änderungen zur DSGVO wurde bereits näher auf den begrifflichen und räumlichen Anwendungsbereich der DSGVO sowie die Möglichkeit der Datenverarbeitung aufgrund von Einwilligungen oder berechtigter Interessen, eingegangen. Im Folgenden soll nun aufgezeigt werden was sich hinsichtlich der Verfahrensverzeichnisse und der zu ergreifenden technischen und organisatorischen Maßnahmen geändert hat.

Dabei ergeben sich äußerst relevante Änderungen bei der Datenverarbeitung, die sich wie folgt auswirken.

3. Verfahrensverzeichnisse

Bereits das BDSG sieht Verfahrensverzeichnisse im Rahmen der Datenverarbeitung vor. Dabei regeln § 4g Abs. 2 und § 4e BDSG, dass der Verantwortliche zwei unterschiedliche Verzeichnisse zu erstellen hat. Eines der Verzeichnisse ist der Öffentlichkeit zugänglich zu machen und enthält lediglich die Angaben im Sinne des § 4e Nr. 1 - 8 BDSG, wohingegen das interne Verzeichnis darüber hinaus eine Übersicht enthalten muss, die geeignet ist zu beurteilen, ob die ergriffenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit angemessen sind. Dieses interne Verzeichnis ist der Öffentlichkeit nicht zugänglich zu machen, da die technischen und organisatorischen Maßnahmen jeweils geheim zu halten sind, um deren Wirkung nicht zu untergraben.

a) Verzeichnispflicht

Eine solche Unterscheidung in ein internes und ein öffentliches Verzeichnis gibt es unter Geltung der DSGVO nicht mehr, da eine Pflicht zur Öffentlichmachung des Verzeichnisses nicht mehr vorgesehen ist. Allerdings sieht die DSGVO einige deutliche Neuerungen hinsichtlich der Verzeichnisse vor, die bei Nichteinhaltung zu massiven Problemen führen können.

Zum einen erlegt die DSGVO nicht mehr nur noch dem Verantwortlichen auf, ein Verfahrensverzeichnis zu erstellen, sondern nunmehr auch dem Auftragsverarbeiter, Art. 30 Abs. 1, 2 DSGVO.

Darüber hinaus ist zu beachten, dass mit der Einführung der DSGVO der Verstoß gegen die Pflicht, ein Verfahrensverzeichnis zu führen, nach Art. 83 Abs. 4 lit. a DSGVO bußgeldbewehrt ist.

Eine Befreiung von der Verzeichnispflicht kommt für Unternehmen oder Einrichtungen mit weniger als 250 Mitarbeitern nach Art. 30 Abs. 5 DSGVO in Betracht.

Voraussetzung dafür ist jedoch, dass die Verarbeitung kein Risiko für die Rechte und Freiheiten betroffener Personen birgt, sie nur gelegentlich erfolgt und keine besonderen Daten nach Art. 9 Abs. 1 DSGVO oder personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten nach Art. 10 DSGVO verarbeitet werden.

b) Verfahrensverzeichnis des Verantwortlichen

Der Verantwortliche hat nach wie vor ein Verfahrensverzeichnis zur Datenverarbeitung anzufertigen. Dieses muss entsprechend des Art. 30 Abs. 1 DSGVO die folgenden Punkte beinhalten:

- Name oder Firma der verantwortlichen Stelle,
- Inhaber, Vorstände, Geschäftsführer oder sonstige Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
- den Namen und die Kontaktdaten der Verantwortlichen, ihrer Vertreter sowie eines etwaigen Datenschutzbeauftragten,
- die Zwecke der Verarbeitung,
- eine Beschreibung der Kategorien personenbezogener Daten und betroffener Personen,
- die Kategorien von Empfängern, gegenüber denen die Daten offengelegt werden oder wurden, einschließlich Empfänger in Drittländern oder internationalen Organisationen,
- Übermittlungen von Daten an ein Drittland oder an eine internationale Organisation, einschließlich deren Angabe,
- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien,
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Die Pflichtinhalte des Verfahrensverzeichnisses des Verantwortlichen entsprechen abgesehen von einigen wenigen Änderungen der bisherigen Norm des § 4e BDSG.

c) Verfahrensverzeichnis des Auftragverarbeiters

Die Erforderlichkeit eines solchen Verzeichnisses sieht Art. 30 Abs. 2 DSGVO neu vor. Bei diesem handelt es

sich um eine verkürzte Form des unter 3. b) genannten Verzeichnisses.

Die Pflichtvorgaben, die das Verzeichnis beinhalten muss, betreffen:

- den Namen und die Kontaktdaten der Auftragsverarbeiter und aller Verantwortlichen, in deren Auftrag sie tätig sind, sowie deren Vertreter und eines etwaigen Datenschutzbeauftragten,
- die Kategorien von Verarbeitungen,
- Übermittlungen von Daten an ein Drittland oder an eine internationale Organisation, einschließlich deren Angabe,
- eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Die beiden - schriftlich (dazu zählt auch elektronisch) zu führenden - Verzeichnisse sind auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen.

Bei Verstößen hiergegen werden entsprechend Art. 83 Abs. 4 lit. a DSGVO Geldbußen von bis zu 10 Mio. € oder von bis zu 2% des gesamten weltweit von diesem Unternehmen erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

4. Technische und organisatorische Maßnahmen (TOMs)

TOMs werden getroffen, um zu gewährleisten, dass die Schutz- und Sicherheitsanforderungen bei Datenverarbeitungen erfüllt werden. Unter technischen Maßnahmen sind Schutzmaßnahmen zu verstehen, die physisch umsetzbar sind, wohingegen organisatorische Maßnahmen durch Anweisungen durchsetzbar sind.

a) Gleichbleibende Maßnahmen

Bislang listete § 9 BDSG in Verbindung mit der Anlage zu § 9 BDSG diejenigen Maßnahmen auf, die zu ergreifen waren. Dazu gehörten die

- grundsätzliche Verschlüsselungspflicht,
- Zutrittskontrolle,
- Zugangskontrolle,
- Zugriffskontrolle,
- Weitergabekontrolle,
- Eingabekontrolle,
- Auftragskontrolle,
- Verfügbarkeitskontrolle und
- das Trennungsprinzip.

Mit Einführung der DSGVO kommen noch einige weitere Maßnahmen hinzu, die es zu beachten und zu dokumentieren gilt.

b) Neue Maßnahmen nach DSGVO

Die vorherigen Maßnahmen gilt es weiterhin einzuhalten. Darüber hinaus legt Art. 32 DSGVO nunmehr fest, dass zusätzlich unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte Betroffener weitere Maßnahmen durch den Verantwortlichen und den Auftragsverarbeiter zu treffen sind.

Bereits im Vorfeld der Verarbeitung werden zwei neue Datenschutzkonzepte wichtig, die Art. 25 DSGVO festlegt:

Einerseits bestimmt „Privacy by design“, dass Datenschutz und -sicherheit bereits in der Planung und Entwicklung von IT-Systemen einkalkuliert werden müssen, um zu verhindern, dass der Datenschutz erst nach Bereitstellen eines Systems durch teure zusätzliche Programmierungsarbeiten umgesetzt wird.

Andererseits bestimmt „Privacy by default“, dass IT-Systeme bereits datenschutzfreundlich voreingestellt sein sollen, sodass nur die Daten verarbeitet werden, die auch für den verfolgten Zweck erforderlich sind.

Um ein angemessenes Schutzniveau zu gewährleisten, sind bei der Verarbeitung die Daten dann zu pseudonymisieren und gegen Verlust zu sichern.

In die Verfügbarkeitskontrolle ist ferner nunmehr herein zu lesen, dass die Daten zu dem Zeitpunkt zur Verfügung gestellt werden können müssen, zu dem sie gebraucht werden. Darüber hinaus sind die Systeme und Dienste dahingehend zu überprüfen, dass sie belastbar und widerstandsfähig sind.

Es muss ein Verfahren durch regelmäßige Prüfung, Bewertung und Evaluierung der Datensicherheit ausgearbeitet werden (z.B. QM), das alle TOMs bewertet und dieses im Geschäftsablauf etabliert.

Die getroffenen Maßnahmen sind zu dokumentieren.

Carsten Ullrich
Rechtsanwalt | Fachanwalt für Arbeitsrecht

Telefon +49 (0)351 424 73 9-11
Telefax +49 (0)351 424 73 9-60

E-Mail ullrich@ullrich-rechtsanwaelte.de
Internet www.ullrich-rechtsanwaelte.de