Verzeichnis der Verarbeitungstätigkeiten

Einleitung

Die Erstellung und Pflege des Verzeichnisses der Verarbeitungstätigkeiten ist eine der zentralen Grundpflichten für Unternehmen unter der Datenschutz-Grundverordnung (DSGVO). Unternehmen müssen ab dem 25. Mai 2018 die Einhaltung der datenschutzrechtlichen Grundsätze bei der Verarbeitung von personenbezogenen Daten nachweisen können, Art. 5 Abs. 2 DSGVO („Rechenschaftspflicht“). In Erwägungsgrund 82 der DSGVO heißt es ausdrücklich, Verantwortliche und Auftragsverarbeiter sollen ein Verzeichnis der Verarbeitungstätigkeiten führen, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis muss den Aufsichtsbehörden auf Anfrage zur Verfügung gestellt werden, damit diese anhand des Verzeichnisses die Verarbeitungstätigkeiten überprüfen können (Art. 30 Abs. 4 DSGVO, Erwägungsgrund 82 DSGVO).

Das Verzeichnis der Verarbeitungstätigkeiten entspricht inhaltlich weitgehend dem bisherigen Verarbeitungsverzeichnis, weist aber teilweise auch Unterschiede auf. Anders als im aktuellen BDSG gliedert sich das Verzeichnis der Verarbeitungstätigkeiten nicht in einen öffentlichen und einen internen Teil. Vielmehr gibt es zukünftig nur noch ein Verzeichnis der Verarbeitungstätigkeiten für den internen Gebrauch; das sogenannte „öffentliche Verfahrensverzeichnis“ gemäß § 4e BDSG entfällt ersatzlos. Tatsächlich hatte das öffentliche Verfahrensverzeichnis auch nur einen sehr begrenzten Informationsgehalt, da es zumeist äußerst generisch formuliert war. Im Gegenzug werden aber die Informationspflichten für das interne Verzeichnis der Verarbeitungstätigkeit ausgeweitet.

Welche Inhalte sind in dem Verzeichnis der Verarbeitungstätigkeiten zu dokumentieren?

Große Unternehmen müssen sämtliche Verarbeitungstätigkeiten dokumentieren, die ihrer Zuständigkeit unterliegen und im Rahmen derer personenbezogene Daten verarbeitet werden (Art. 30 DSGVO). In der Regel wird für jede Verarbeitungstätigkeit eine eigene kurze Dokumentation erforderlich sein, die bestimmte Mindestanforderungen zu erfüllen hat. Erforderlich sind danach unter anderem die nachfolgend aufgeführten Informationen:

- Name und Kontaktdaten des für die Verarbeitung verantwortlichen Unternehmens
- Zwecke der Verarbeitung
- Betroffene Personengruppen
- Beschreibung der Kategorien der verarbeiteten Daten
- Informationen über eine etwaige Datenübermittlung in Drittländer
- Beschreibung der technischen und organisatorischen Maßnahmen zur Einhaltung von Datenschutz und Datensicherheit
- Regelfristen zur Löschung der Daten

Die inhaltlichen Vorgaben entsprechen im Wesentlichen denen aus dem bisherigen BDSG. Der Detailgrad des Verzeichnisses der Verarbeitungstätigkeiten dürfte auch weiterhin von der Art der verarbeiteten Daten und dem Umfang der Datenverarbeitung abhängen. Die Summe der Einzeldokumentationen bildet dann das Verzeichnis der Verarbeitungstätigkeiten.

Gibt es Ausnahmen von der Pflicht zur Führung des Verzeichnisses der Verarbeitungstätigkeiten für kleinere Unternehmen?

Unternehmen mit weniger als 250 Mitarbeitern müssen – anders als größere Unternehmen – nicht jede Datenverarbeitungstätigkeit dokumentieren. Gemäß Art. 30 Abs. 5 DSGVO

müssen lediglich solche Verfahren erfasst werden, im Rahmen derer besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO, also beispielsweise Gesundheitsdaten, verarbeitet werden.

Zudem müssen allerdings auch solche Verarbeitungen dokumentiert werden, die „nicht nur gelegentlich“ erfolgen, Art. 30 Abs. 5 DSGVO. Diese Rückausnahme dürfte dazu führen, dass letztlich auch Unternehmen mit weniger als 250 Mitarbeitern eine Vielzahl von Verfahrensdokumentationen erstellen müssen. „Nicht nur gelegentlich“ im Sinne der DSGVO dürfte beispielsweise die Verarbeitung von Mitarbeiterdaten im Rahmen der Personalakten, aber auch die Verarbeitung von Kundenstammdaten sein. Im Ergebnis bleiben letztlich nur solche Verarbeitungstätigkeiten ausgenommen, die einmalig aus einem bestimmten Anlass erfolgen und bei denen nicht von einer Regelmäßigkeit auszugehen ist.

Ist eine besondere Form für das Verzeichnis der Verarbeitungstätigkeiten vorgeschrieben?

Durch Art. 30 DSGVO ist vorgegeben, dass das Verzeichnis der Verarbeitungstätigkeiten schriftlich zu führen ist, wobei auch ein elektronisches Format genutzt werden kann. Weitergehende Vorgaben finden sich in der DSGVO nicht; Sinn und Zweck der Regelung führen ebenfalls nicht zu zusätzlichen Anforderungen. Für kleinere Unternehmen kann es daher zweckmäßig sein, für jede Verarbeitungstätigkeit ein Formular (etwa auf Basis eines Word-Dokumentes) auszufüllen und die ausgefüllten Formulare ausgedruckt und/oder als Datei zu verwahren. Bei einer größeren Anzahl von Verarbeitungstätigkeiten kann sich dagegen der Einsatz einer Datenbank oder die Nutzung einer besonderen Software empfehlen.

Muss das Verzeichnis der Verarbeitungstätigkeiten nur ein einziges Mal erstellt werden?

Im Rahmen einer vollständigen Erfassung aller Verfahren kann ein erster Ist-Bestand der datenschutzrechtlichen Verarbeitungen dokumentiert werden. Sobald ein solches Verzeichnis der Verarbeitungstätigkeiten besteht, muss dieses Verzeichnis auch aktuell gehalten werden. Zwar findet sich in der finalen Fassung der DSGVO anders als in den Vorentwürfen keine ausdrückliche Aktualisierungspflicht, diese kann aber aus dem Sinn und Zweck der Regelung abgeleitet werden (Paal/Pauly-Martini, DSGVO, 2. Aufl., Art. 30 Rn. 5b).

Bei der Einführung neuer Verarbeitungsvorgänge sind daher die neuen Verfahrensdokumentationen in das Verzeichnis aufzunehmen. Außerdem sollten die existierenden Verfahrensdokumentationen regelmäßig hinsichtlich eines etwaigen Änderungs- oder Verbesserungsbedarfs überprüft werden. Empfehlenswert ist dabei die Nutzung eines Wiedervorlagesystems, bei dem die Häufigkeit der Prüfung und Aktualisierung abhängig von der Relevanz der Verarbeitungstätigkeit definiert werden kann. Ohne eine regelmäßige Überprüfung und Anpassung des Verzeichnisses der Verarbeitungstätigkeiten besteht die Gefahr, dass die mühsam erstellte Übersicht schon nach kurzer Zeit überholt und damit wertlos ist.

Wer ist für die Führung des Verzeichnisses zuständig?

Die Pflicht zur Führung des Verzeichnisses der Verarbeitungstätigkeiten liegt gem. Art. 30 Abs. 1 DSGVO bei dem Verantwortlichen, also dem jeweiligen Unternehmen. Innerhalb des Unternehmens kann die Aufgabe durch die Geschäftsleitung delegiert werden, gegebenenfalls auch auf den Datenschutzbeauftragten. Die Führung des Verzeichnisses ist jedoch keine originäre Aufgabe des Datenschutzbeauftragten im Rahmen des Aufgabenkatalogs gem. Art. 39 DSGVO. Je nach Umfang der zu dokumentierenden Verarbeitungstätigkeiten ist es aber sinnvoll, zumindest die Konzeption des Verzeichnisses dem Datenschutzbeauftragten zu überlassen und ihn auch in die Dokumentation der einzelnen Verarbeitungstätigkeiten einzubinden. Denkbar ist etwa ein zweistufiger Prozess, bei dem die Verarbeitungstätigkeiten im ersten Schritt in der jeweiligen Fachabteilung auf Basis eines bereitgestellten Formulars dokumentiert werden und im zweiten Schritt eine Prüfung der dokumentierten Verarbeitungstätigkeiten erfolgt. Bei dieser Gestaltung kann der Datenschutzbeauftragte zugleich prüfen, ob sich im Hinblick auf die neuen Anforderungen durch die DSGVO noch ein Anpassungsbedarf bei der Verarbeitungstätigkeit ergibt.

Welche Konsequenzen drohen bei nicht ordnungsgemäßer Führung des Verzeichnisses der Verarbeitungstätigkeiten?

Liegt auf Anfrage der Aufsichtsbehörden kein ordnungsgemäßes Verzeichnis der Verarbeitungstätigkeiten im Unternehmen vor, kann dies Bußgelder zur Folge haben. Deren Höhe kann gemäß Art. 83 Abs. 4 DSGVO bis zu 20 Mio. Euro oder bis zu 2 % des gesamten weltweiten Jahresumsatzes betragen. Umgekehrt kann ein gut gepflegtes Verzeichnis der Verarbeitungstätigkeiten im Falle eines aufsichtsbehördlichen Verfahrens einen guten Eindruck hinterlassen und die Zusammenarbeit mit der Aufsichtsbehörde erleichtern, was sich gemäß Art. 83 Abs. 2 S. 2 lit. f DSGVO mindernd auf die festgelegten Bußgelder auswirken kann.

Fehlt ein Verzeichnis der Verarbeitungstätigkeiten oder sind wesentliche Verarbeitungstätigkeiten nicht dokumentiert, besteht außerdem die Gefahr, dass das Unternehmen den ordnungsgemäßen Umgang mit den personenbezogenen Daten nicht nachweisen kann. Selbst wenn die Datenverarbeitung in der Sache ordnungsgemäß war, wird der entsprechende Nachweis rückwirkend ohne Dokumentation aufgrund der Rechenschaftspflicht nur sehr schwer möglich sein.

Fazit

Für Unternehmen besteht unter der DSGVO die Pflicht zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten. Ein entsprechendes Verzeichnis ist von jedem Unternehmen, das personenbezogene Daten verarbeitet, zu erstellen und zu pflegen. Bei der Erstellung der umfangreichen Dokumentationen, die Bestandteil eines solchen Verzeichnisses sind, müssen die Datenverarbeitungsvorgänge kleinteilig analysiert und genau dokumentiert werden. Unternehmen bietet die Erstellung des Verzeichnisses der Verarbeitungstätigkeiten damit aber auch eine Möglichkeit zur kritischen Auseinandersetzung mit der eigenen Datenverarbeitung. Ein gut gepflegtes Verzeichnis der Verarbeitungstätigkeiten dient insoweit auch als Nachweis einer durchdachten und selbstkritischen Auseinandersetzung mit dem Thema Datenschutz. So kann die Pflicht zur Dokumentation der Verarbeitungstätigkeiten einen zusätzlichen Mehrwert haben.

Robert Bommel, LL.M. / Dr. Sebastian Meyer, LL.M.

Kontakt:

BRANDI Rechtsanwälte Partnerschaft mbB
Adenauerplatz 1 I 33602 Bielefeld

Dr. Sebastian Meyer, LL.M.
Rechtsanwalt
Fachanwalt für Informationstechnologierecht (IT-Recht)
Datenschutzauditor (TÜV)

T +49 521 96535 - 812
F +49 521 96535 - 115
E sebastian.meyer@brandi.net