Die Rechenschaftspflicht der DSGVO

Einleitung

Die datenschutzrechtliche Dokumentation hat unter der Datenschutz-Grundverordnung (DSGVO) an Bedeutung gewonnen. Nach Art. 5 Abs. 2 DSGVO muss die verantwortliche Stelle die Einhaltung der Grundsätze der Datenverarbeitung nachweisen können. Dieses Prinzip der „Rechenschaftspflicht" führt dazu, dass sich Unternehmen unter der DSGVO bei dem Vorwurf eines Datenschutzverstoßes selbst entlasten müssen und nicht umgekehrt der Datenschutzverstoß dem Unternehmen nachgewiesen werden muss. Der Nachweis der Einhaltung von datenschutzrechtlichen Vorgaben wird ohne eine umfangreiche datenschutzrechtliche Dokumentation nicht möglich sein.

Es ist deshalb jedem Unternehmen zu empfehlen, eine strukturierte Dokumentation der eigenen datenschutzrechtlichen Aktivitäten zu erarbeiten. Um einen Überblick über die Rechenschaftspflicht zu geben, haben wir das Thema in unserem Newsletter vertieft für Sie aufbereitet. Wir beschreiben im Folgenden Dokumentationspflichten, die in der DSGVO geregelt werden, und benennen darüber hinaus weitere mögliche Dokumentationen, die den Nachweis datenschutzrechtlicher Aktivitäten im Unternehmen erleichtern können. An geeigneter Stelle geben wir Tipps für die praktische Umsetzung. Zudem geben wir einen Überblick über die möglichen Konsequenzen bei Nichterfüllung der Rechenschaftspflicht.

Dokumentationspflichten in der DSGVO

Verzeichnis der Verarbeitungstätigkeiten

Die Erstellung und Pflege des Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 DSGVO ist eine der zentralen Grundpflichten für Unternehmen unter der DSGVO. Ein Verzeichnis der Verarbeitungstätigkeiten ist die Dokumentation von Prozessen in einem Unternehmen, bei denen personenbezogene Daten verarbeitet werden. Das Verzeichnis dient unter der DSGVO vornehmlich dem Nachweis datenschutzrechtlicher Aktivitäten und ist den Aufsichtsbehörden auf Anfrage zur Verfügung zu stellen, damit diese die datenverarbeitenden Prozesse überprüfen können. Gleichzeitig bietet die Erstellung des Verzeichnisses den Unternehmen eine Möglichkeit zur kritischen Auseinandersetzung mit der eigenen Datenverarbeitung.

Bei der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten kann beispielsweise so vorgegangen werden, dass zunächst die zu dokumentierenden Prozesse im Unternehmen, bei denen personenbezogene Daten verarbeitet werden, identifiziert werden. In einem zweiten Schritt erfolgt die schriftliche Dokumentation der Datenverarbeitungsvorgänge, wobei die Mindestanforderungen an die Dokumentation von Art. 30 DSGVO vorgegeben werden. Für die Dokumentation gibt es spezielle Softwarelösungen, häufig kommen aber auch Excel-Tabellen oder Word-Vorlagen zum Einsatz. Es ist zu beachten, dass das Verzeichnis der Verarbeitungstätigkeiten fortlaufend zu pflegen ist. Bei der Einführung neuer Verarbeitungsvorgänge sind deshalb neue Dokumentationen zu erstellen. Die existierenden Verfahrensdokumentationen sollten außerdem regelmäßig hinsichtlich eines etwaigen Änderungs- oder Verbesserungsbedarfs überprüft werden, beispielsweise durch Nutzung eines Wiedervorlagensystems.

Datenschutz-Folgenabschätzung

Für Datenverarbeitungsvorgänge, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, ist nach Art. 35 DSGVO zusätzlich die Durchführung einer Datenschutz-Folgenabschätzung erforderlich. Bei der Datenschutz-Folgenabschätzung handelt es sich um eine vertiefte datenschutzrechtliche Prüfung, die dabei helfen soll, die Rechtmäßigkeit von Datenverarbeitungsvorgängen im Vorhinein zu überprüfen und die Einhaltung der datenschutzrechtlichen Vorgaben sicherzustellen. Bei der Erstellung der Datenschutz-Folgenabschätzung bietet es sich häufig an, die Überprüfung der einzelnen Datenverarbeitungsprozesse auf Basis der Beschreibungen der Prozesse in dem Verzeichnis der Verarbeitungstätigkieten vorzunehmen. Die Aufsichtsbehörden haben sowohl Vorgaben veröffentlicht, wann eine Datenschutz-Folgenabschätzung zwingend erforderlich ist als auch wie sie strukturiert werden kann.

Weitere mögliche Dokumentationen

Weitergehende datenschutzrechtliche Dokumentationen sind nach der aktuellen Rechtslage nicht zwingend vorgeschrieben, sondern optional. Ratsam sind weitergehende Dokumentationen gleichwohl, um die Einhaltung der datenschutzrechtlichen Vorgaben der DSGVO nachweisen zu können. Mögliche weitere Dokumentationen werden im Folgenden dargestellt.

Berichtspflichten des Datenschutzbeauftragten

Der Datenschutzbeauftragte berichtet nach Art. 38 Abs. 3 S. 3 DSGVO unmittelbar der höchsten Managementebene des Unternehmens. Es sollte deshalb darauf geachtet werden, dass der Datenschutzbeauftragte in regelmäßigen Abständen über seine

Aktivitäten Bericht erstattet. Dies kann beispielsweise in Form von jährlichen Tätigkeitsberichten erfolgen. Die Berichte sollten ein wahrheitsgemäßes Bild der Aktivitäten des Datenschutzbeauftragten geben. Im Falle einer konkreten Überprüfung können sie aber auch der Aufsichtsbehörde als Nachweis für datenschutzrechtliche Aktivitäten vorgelegt werden.

Übersicht der technischen und organisatorischen Maßnahmen

Verantwortliche Stellen haben nach Art. 32 Abs. 1 DSGVO geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko der Datenverarbeitung für die Rechte und Freiheiten natürlicher Personen angemessenes Schutzniveau zu gewährleisten. Es ist zu empfehlen, die im Unternehmen getroffenen technischen und organisatorischen Maßnahmen zu dokumentieren und dahingehend zu überprüfen, ob sie einem angemessenen Schutzniveau entsprechen.

Unternehmen sollen nach Erwägungsgrund 81 zudem nur Auftragsverarbeiter heranziehen, die hinreichende Garantien dafür bieten, dass ausreichende technische und organisatorische Maßnahmen getroffen werden. Zum Nachweis der Einhaltung dieser Pflicht hat der Auftragsverarbeiter alle erforderlichen Informationen dem Verantwortlichen zur Verfügung zu stellen (Art. 28 Abs. 3 S. 2 lit. h) DSGVO). Die Übersicht der technischen und organisatorischen Maßnahmen dient insofern ebenfalls als Nachweis.

Verpflichtungserklärung für Mitarbeiter

Während unter der alten Rechtslage alle Mitarbeiter, die mit der Verarbeitung personenbezogener Daten befasst waren, zwingend auf das sogenannte Datengeheimnis verpflichtet werden mussten, sehen die Regelungen der DSGVO nicht mehr ausdrücklich eine solche Verpflichtung auf das Datengeheimnis vor. Um die Vertraulichkeit im Zusammenhang mit der Datenverarbeitung sicherzustellen, ist es allerdings weiterhin empfehlenswert, die Mitarbeiter des Unternehmens auf das Datengeheimnis zu verpflichten. Die schriftlichen Verpflichtungserklärungen dienen gleichzeitig als Nachweis der Maßnahme.

Datenschutzkonzept

Empfehlenswert ist ein Datenschutzkonzept, das allgemein zusammenfasst, welche Maßnahmen in einem Unternehmen zur Einhaltung der datenschutzrechtlichen Bestimmungen getroffen werden. In dem Konzept können gleichzeitig die Ziele des Unternehmens im Datenschutz beschrieben und die allgemeinen datenschutzrechtlichen Anforderungen für das Unternehmen konkretisiert werden. Das Datenschutzkonzept dient damit vor allem der internen Dokumentation für die Geschäftsleitung und mit dem Thema betraute Personen sowie als Arbeitsgrundlage für den Datenschutzbeauftragten. Darauf aufbauend können zusätzlich die einzelnen Aktivitäten in bestimmten Bereichen separat dokumentiert werden.

Konzept zum Vorgehen bei Datenschutzverletzungen

Verletzungen des Schutzes personenbezogener Daten müssen nach Art. 33, 34 DSGVO unter bestimmten Voraussetzungen der Aufsichtsbehörde und dem Betroffenen gemeldet werden. Die Meldung an die Aufsichtsbehörde hat unverzüglich, möglichst innerhalb einer Frist von 72 Stunden, zu erfolgen. Die Aufsichtsbehörden vertreten hierzu teilweise die Auffassung, dass eine solche fristgerechte Meldung nur dann sichergestellt werden kann, wenn es im Unternehmen dafür klare Abläufe gibt, die auch nachgewiesen werden müssen. Es ist deshalb ratsam, in einer Dokumentation festzuhalten, wie in Fällen von Datenschutzverstößen oder bei Datenverlust vorgegangen wird. Indem ein klares Vorgehen definiert, schriftlich festgehalten und im Unternehmen bekannt gemacht wird, können die Vorbereitungen nachgewiesen und im Ernstfall die knappen Fristen einfacher eingehalten werden. Den Mitarbeitern des Unternehmens ist anhand strukturierter vorgegebener Arbeitsabläufe eine schnelle Reaktion auf Datenschutzverletzungen möglich.

Die internen Berichts- und Dokumentationspflichten sollten dabei großzügiger ausgestaltet werden. Jede verantwortliche Stelle sollte also auch solche Datenschutzvorfälle dokumentieren, die nicht zu einer Meldepflicht geführt haben. Auf diese Weise kann auch im Nachhinein noch begründet werden, warum ein konkreter Vorfall nicht gemeldet wurde.

Umgang mit Betroffenenanfragen

Bezüglich der Verarbeitung von personenbezogenen Daten stehen betroffenen Personen nach Art. 12 bis 23 DSGVO umfangreiche Rechte zu. Unternehmen sollten in diesem Kontext darauf achten, Betroffenenanfragen ordnungsgemäß und zeitnah nachzukommen. Um die Einhaltung des datenschutzkonformen Umgangs mit Betroffenenanfragen nachzuweisen, ist es empfehlenswert, die Korrespondenz zu Betroffenenanfragen für eine gewisse Zeit aufzubewahren. Von der Datenschutzaufsichtsbehörde in NRW wird etwa eine Aufbewahrungsfrist von drei Jahren für den Fall empfohlen, in dem die Verfolgungsverjährungsfrist drei Jahre beträgt. Während der Aufbewahrungsdauer sollten die betroffenen Daten vor unbefugtem Zugriff besonders geschützt werden, indem etwa ihre Verarbeitung eingeschränkt wird.

Vorgaben zur Löschung und Archivierung von Daten

Unter der DSGVO gilt nach Art. 5 Abs. 1 lit. c) DSGVO der Grundsatz der Datenminimierung, nach dem die Datenverarbeitung auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein muss. Personenbezogene Daten sind danach zu löschen, wenn der Zweck der ursprünglichen Datenverarbeitung entfallen ist. Dafür sind Löschfristen zu definieren und regelmäßig zu prüfen.

Die Vorgaben zur Aufbewahrung und Löschung von Daten können in einem Archivierungs- und Löschkonzept festgehalten werden. Bereits in dem Verzeichnis der Verarbeitungstätigkeiten sind nach Art. 30 Abs. 1 S. 2 lit. f) DSGVO die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien möglichst anzugeben. Neben der Festlegung von einzelnen Fristen in den Verfahrensdokumentationen kann dort zusätzlich auf ein gesondertes Löschkonzept verwiesen werden, das allgemein beschreibt, welche Vorgaben zur Speicherung und Löschung von Daten in einem Unternehmen gelten.

Schulungskonzept

Die Vermittlung von datenschutzrechtlichem Wissen ist für die Einhaltung der datenschutzrechtlichen Vorschriften in einem Unternehmen von essentieller Bedeutung. Nur wenn Mitarbeiter im Rahmen ihrer täglichen Arbeit die datenschutzrechtlichen Problemfelder erkennen, können Sie diesbezüglich Rücksprache mit der Geschäftsführung oder dem Datenschutzbeauftragten halten.

Um Mitarbeiter zu datenschutzrechtlichen Themen zu sensibilisieren, ist die regelmäßige Durchführung von Datenschutzschu-

lungen zu empfehlen. In einem Schulungskonzept kann dargestellt werden, in welchen Abständen und in welchem Umfang Datenschutzschulungen vorgesehen sind und wie diese ausgestaltet sind.

Datenschutzhandbuch

Ergänzend kann außerdem über die Erstellung eines Datenschutzhandbuches nachgedacht werden. Hierbei handelt es sich zumeist um eine Sammlung aller Vorgaben, Regelwerke und Empfehlungen zum Umgang mit personenbezogenen Daten. Ein Datenschutzhandbuch kann insoweit als Übersicht über die verschiedenen Einzeldokumente gesehen werden. Die Mitarbeiter können sich dadurch schnell über datenschutzrechtliche Themen informieren.

Konsequenzen bei Nichterfüllung der Rechenschaftspflicht

Einige Verstöße gegen Dokumentationspflichten, etwa Verstöße gegen Art. 30 DSGVO (Führung eines Verzeichnisses der Verarbeitungstätigkeiten) oder Art. 35 DSGVO (Durchführung von Datenschutz-Folgenabschätzungen), sind nach der DSGVO ausdrücklich bußgeldbewährt. Bei Verletzungen dieser Vorschriften sind nach Art. 83 Abs. 4 lit. a) DSGVO Geldbußen von bis zu 10 Mio. Euro oder 2 % des weltweit erzielten Jahresumsatzes eines Unternehmens möglich. Kann in einem Verfahren der Nachweis der Datenschutzkonformität nicht erbracht werden, wirkt sich dies ebenfalls auf mögliche Bußgelder aus.

Verantwortliche und Auftragsverarbeiter sind verpflichtet, auf Anfrage der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammenzuarbeiten und alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Gut gepflegte datenschutzrechtliche Dokumentationen können im Falle eines aufsichtsbehördlichen Verfahrens einen guten Eindruck hinterlassen und die Zusammenarbeit mit der Aufsichtsbehörde erleichtern. Dies kann sich gemäß Art. 83 Abs. 2 S. 2 lit. f) DSGVO mindernd auf die Verhängung von Bußgeldern auswirken.

Fazit

Unter der DSGVO sollten Unternehmen einen gesteigerten Wert auf datenschutzrechtliche Dokumentationen legen. Ein wichtiger Bestandteil der Erfüllung der Rechenschaftspflicht ist die Dokumentation in einem Verzeichnis der Verarbeitungstätigkeiten. Darüber hinaus ist eine großzügige Ausgestaltung der internen Dokumentationspflichten empfehlenswert, um im Zweifel die Einhaltung von datenschutzrechtlichen Vorgaben nachweisen zu können. Gleichzeitig bietet die Dokumentation den Unternehmen die Möglichkeit, sich selbst kritisch mit der eigenen Datenverarbeitung auseinanderzusetzen. Bei der Erstellung und Pflege der Dokumentationen handelt es sich um laufende Aufgaben, weshalb in regelmäßigen Abständen eine Überprüfung und Aktualisierung erfolgen sollte. Soweit die vorstehend aufgeführten Unterlagen in einem Unternehmen vorhanden sind, besteht regelmäßig ein angemessener Grundbestand für eine datenschutzrechtliche Dokumentation, wobei zusätzlich immer noch konkrete Aspekte und Themen dokumentiert werden müssen.

Johanna Schmale

Kontakt:

BRANDI Rechtsanwälte
Partnerschaft mbB
Adenauerplatz 1
33602 Bielefeld

Johanna Schmale
Wissenschaftliche Mitarbeiterin
T +49 521 96535 - 890
F +49 521 96535 - 114
M johanna.schmale@brandi.net
www.brandi.net