Die Datenschutz-Folgenabschätzung

Einleitung

Die Datenschutz-Grundverordnung (DSGVO) ist ab dem 25. Mai 2018 anwendbares Recht innerhalb der EU. Mit der DSGVO wird das Konzept der Datenschutz-Folgenabschätzung in das europäische Datenschutzrecht integriert. Die Datenschutz-Folgenabschätzung ist eine vertiefte datenschutzrechtliche Prüfung, die gemäß Art. 35 DSGVO in bestimmten Fällen durchgeführt werden muss. Sie soll helfen, die Rechtmäßigkeit von Datenverarbeitungsvorgängen zu überprüfen und die Einhaltung der datenschutzrechtlichen Vorgaben sicherstellen.

Wann ist eine Datenschutz-Folgenabschätzung durchzuführen?

Eine Datenschutz-Folgenabschätzung ist für solche Datenverarbeitungsvorgänge zwingend durchzuführen, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben (Art. 35 Abs. 1 DSGVO). Die Datenschutz-Folgenabschätzung ist insoweit vergleichbar mit der aus dem bisherigen deutschen Datenschutzrecht bekannten Vorabkontrolle gemäß § 4 d Abs. 5 BDSG, bei der es sich um eine Prüfung besonders risikogeneigter Verarbeitungsvorgänge handelt.

Ein hohes Risiko für die Betroffenen liegt gemäß Art. 35 Abs. 3 DSGVO insbesondere dann vor, wenn eine systematische und umfassende Bewertung persönlicher Aspekte der Betroffenen vorgenommen wird („Profiling“), bei der umfangreichen Verarbeitung von besonderen personenbezogenen Daten im Sinne des Art. 9 DSGVO sowie bei der systematischen Überwachung öffentlich zugänglicher Bereiche. In diesen Fällen ist somit immer eine Datenschutz-Folgenabschätzung durchzuführen.

Aber auch bei anderen Datenverarbeitungsvorgängen, die ein entsprechend hohes Risiko für die Betroffenen aufweisen, ist eine Datenschutz-Folgenabschätzung erforderlich. Entscheidende Kriterien für die diesbezügliche Risikobewertung sind gemäß Art. 35 Abs. 1 DSGVO Art, Umfang, Umstände und Zwecke der Verarbeitung.

Ein hohes Risiko für die Betroffenen kann unter anderem auch vorliegen, wenn im Rahmen der Datenverarbeitungsprozesse neuartige Technologien verwendet werden, sodass auch dann eine Datenschutz-Folgenabschätzung erforderlich werden kann (Art. 35 Abs. 1 DSGVO i.V.m. ErwG 89, 91 DSGVO).

Die Aufsichtsbehörden werden gemäß Art. 35 Abs. 4, 5 DSGVO ermächtigt, Listen von Verarbeitungsvorgängen zu erstellen, für die zwingend eine Datenschutz-Folgenabschätzung durchzuführen ist („Blacklist“). Wann die erste Blacklist veröffentlicht wird ist noch unklar, da sich die europäischen Aufsichtsbehörden bezüglich dieser Liste zunächst miteinander abstimmen müssen. Parallel können die Aufsichtsbehörden auch eine Liste von Verfahren beschließen, für die gerade keine Datenschutz-Folgenabschätzung erforderlich ist („Whitelist“). Da auch die diesbezügliche Einigung der Aufsichtsbehörden einige Zeit in Anspruch nehmen wird, ist nicht sichergestellt, dass die ersten Black- bzw. Whitelists noch vor Mai 2018 veröffentlicht werden.

Gibt es konkrete Beispiele zur Ermittlung der Erforderlichkeit?

Als erste Orientierung zur Bewertung der Erforderlichkeit einer Datenschutz-Folgenabschätzung können die Empfehlungen der Artikel-29-Arbeitsgruppe zur Datenschutz-Folgenabschätzung dienen (Art. 29 Working Party, WP 248 17/EN v. 04.04.2017). Die Empfehlungen beinhalten dabei sowohl Beispiele für Verfahren, bei denen eine Datenschutz-Folgenabschätzung erforderlich sein soll, als auch Vorschläge zur Dokumentation der erforderlichen Prüfung.

Die Arbeitsgruppe sieht beispielsweise eine Datenschutz-Folgenabschätzung für Gesundheitsinformationssysteme

oder die automatische Analyse von Nutzerverhalten auf Social Media-Kanälen grundsätzlich als erforderlich an. Bei der Videoüberwachung soll es auf die konkrete Ausgestaltung ankommen, „intelligente Systeme“ mit Erkennungs- oder Verfolgungsfunktion sollen etwa eine Datenschutz-Folgenabschätzung erforderlich werden lassen. Auch die Überwachung von Mitarbeitern im Hinblick auf das Nutzungsverhalten von IT-Systemen soll in den Anwendungsbereich der Datenschutz-Folgenabschätzung fallen.

Nicht erforderlich ist nach der Einschätzung der Arbeitsgruppe dagegen eine Datenschutz-Folgenabschätzung bei typischen Werbeaktivitäten wie dem Versand von Newslettern an Kunden oder die Nutzung von Werbeanzeigen entsprechend der Vorlieben der Kunden. Für das letztgenannte Beispiel nimmt die Arbeitsgruppe aber eine Beschränkung dahingehend vor, dass nur eine „limitierte Profilbildung“ erfolgen darf.

Wie ist die Datenschutz-Folgenabschätzung durchzuführen?

Die Datenschutz-Folgenabschätzung ist gemäß Art. 35 Abs. 1 DSGVO „vorab“, also vor der Durchführung der Datenverarbeitungsprozesse, durchzuführen. Die Mindestinhalte der Datenschutz-Folgenabschätzung ergeben sich aus Art. 35 Abs. 7 DSGVO. Danach hat die Datenschutz-Folgenabschätzung zumindest eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitung sowie eine Bewertung der Risiken für die Betroffenen und eine Darstellung der zur Bewältigung dieser Risiken getroffenen Abhilfemaßnahmen zu enthalten.

Anders als die Vorabkontrolle ist die Datenschutz-Folgenabschätzung nicht Aufgabe des Datenschutzbeauftragten, sondern ist von dem für die Verarbeitung Verantwortlichen durchzuführen. Der Datenschutzbeauftragte, sofern ein solcher bestellt wurde, ist vielmehr gemäß Art. 35 Abs. 2 DSGVO beratend in die Datenschutz-Folgenabschätzung einzubeziehen. Tatsächlich werden die für die Verarbeitung Verantwortlichen im Rahmen der Durchführung einer Datenschutz-Folgenabschätzung vermutlich umfangreich auf die Praxiserfahrung des Datenschutzbeauftragten zurückgreifen.

Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einheitliche Datenschutz-Folgenabschätzung vorgenommen werden (Art. 35 Abs. 1 S. 2 DSGVO). Soweit wesentliche Teile eines Verarbeitungsvorgangs an einen Auftragsverarbeiter ausgegliedert wurden, hat dieser den für die Verarbeitung Verantwortlichen bei der Erstellung der Datenschutz-Folgenabschätzung zu unterstützen und die benötigten Informationen beizusteuern.

Bemerkenswert ist die Regelung des Art. 35 Abs. 9 DSGVO, nach der der Verantwortliche im Rahmen der Datenschutz-Folgenabschätzung gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung einzuholen hat. Eine Konkretisierung, auf welche Art der Standpunkt der Betroffenen in der Praxis eingeholt werden soll, fehlt in der DSGVO. Die bisher diskutierten Möglichkeiten, namentlich die Durchführung von Studien und die Befragung von (zukünftigen) Kunden, sind wohl nur den wenigsten Unternehmen zuzumuten. Die Befragung von Mitarbeitern könnte unterdessen im Rahmen des Mitarbeiterdatenschutzes ein geeignetes Konzept sein, den Standpunkt der Beschäftigten einzuholen.

Soweit sich ein geprüftes Verfahren später in wesentlichen Punkten verändert, muss die Datenschutz-Folgenabschätzung diesbezüglich überprüft werden, Art. 35 Abs. 11 DSGVO. Soweit neuartige Systeme oder Technologien eingesetzt werden, kann unter Umständen ein völlig neues Verfahren entstehen, das gesondert zu prüfen und zu bewerten ist. Die Artikel-29-Arbeitsgruppe, ein Zusammenschluss der europäischen Aufsichtsbehörden, empfiehlt bisher eine Revision von durchgeführten Datenschutz-Folgenabschätzungen im Abstand von jeweils drei Jahren.

In welchen Fällen müssen die Aufsichtsbehörden konsultiert werden?

Wenn aus der Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko für die Betroffenen zur Folge hätte, hat der für die Verarbeitung Verantwortliche die Aufsichtsbehörden zu kontaktieren, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft (Art. 36 Abs. 1 DSGVO). Soweit die Aufsichtsbehörde im Rahmen der Konsultation zu dem Ergebnis kommt, dass die geplante Verarbeitung nicht die Vorgaben der DSGVO erfüllt, hat sie dem Verantwortlichen gemäß Art. 36 Abs. 2 DSGVO innerhalb von bis zu acht Wochen nach Erhalt des Ersuchens um Konsultation eine schriftliche Empfehlung zu unterbreiten. Andere Befugnisse der Aufsichtsbehörde sind dadurch nicht beschränkt, sodass die Aufsichtsbehörde auch Datenschutzüberprüfungen durchführen, auf vermeintliche Datenschutzverstöße hinweisen und ein Verbot des Verarbeitungsvorgangs erlassen kann.

Was sollten Unternehmen mit Hinblick auf die Rechtsänderung veranlassen?

Unternehmen sollten die Rechtsänderungen zum Anlass nehmen, ihre Datenverarbeitungsvorgänge mit Hinblick auf die neuen Anforderungen der DSGVO zu überprüfen. Zur Beantwortung der Frage, ob jeweils eine Datenschutz-Folgenabschätzung durchgeführt werden muss, sollten alle Verfahren einer Risikobewertung unterzogen werden. Im Rahmen der Risikobewertung sind dabei sowohl das Ausmaß bei Verwirklichung des Risikos als auch die Eintrittswahrscheinlichkeit zu berücksichtigen. Dabei ist auch zu beachten, dass die Durchführung einer Datenschutz-Folgenabschätzung insbesondere für solche Verfahren erforderlich sein kann, die bereits einer Vorabentscheidung gemäß § 4 d Abs. 5 BDSG unterlagen.

Was droht Unternehmen bei Verstößen gegen die Pflicht zur Bestellung eines Datenschutzbeauftragten?

Unter der DSGVO kann gem. Art. 83 Abs. 4 lit. a DSGVO ein Bußgeld verhängt werden, dessen Höhe bis zu 10 Mio. Euro oder bis zu 2 % des gesamten weltweit erzielten Jahresumsatzes betragen kann, wenn einer Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung nicht oder nicht richtig nachgekommen wird.

Fazit

Die Datenschutz-Folgenabschätzung ist ein wichtiger Bestandteil bei der Planung von Verarbeitungsprozessen, die ein hohes Risiko für die Rechte der Betroffenen aufweisen. Insgesamt scheint sich der datenschutzrechtliche Prüfungsaufwand für Unternehmen durch die neue Datenschutz-Folgenabschätzung zu erhöhen. Strukturell muss zukünftig jedes Verfahren hinsichtlich seiner Risiken für die Betroffenen überprüft werden, damit jeweils dokumentiert werden kann, aus welchen Gründen sich der Verantwortliche für oder gegen die Durchführung einer Datenschutz-Folgenabschätzung entschieden hat.

Tatsächlich muss eine derartige Risikobewertung aber ohnehin bereits im Rahmen der Erstellung des Verfahrensverzeichnisses von den für die Verarbeitung Verantwortlichen erarbeitet und dokumentiert werden. Auch die getroffenen Abhilfemaßnahmen und die Zwecksetzung werden bereits im Verfahrensverzeichnis dokumentiert. Mit Hinblick darauf, dass die Datenschutz-Folgenabschätzung „vorab“, also vor der Durchführung der Verarbeitungsprozesse durchzuführen ist, dürfte zumindest die zumeist nachgelagerte Erstellung einer Verfahrensdokumentation mit vergleichsweise geringem Aufwand möglich sein.

Die Durchführung einer Datenschutz-Folgenabschätzung kann für Unternehmen auch einen großen Mehrwert haben. Potenzielle Risiken und Sicherheitslücken können frühzeitig aufgedeckt werden, ebenso wie strukturelle Probleme der Verarbeitung. Dies dürfte dazu beitragen, dass Unternehmen die Voraussetzungen der DSGVO besser erfüllen und die empfindlichen Bußgelder vermieden werden können.

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

Kontakt:

BRANDI Rechtsanwälte Partnerschaft mbB
Adenauerplatz 1
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

www.brandi.net