Der Datenschutzbeauftragte unter der DSGVO und dem BDSG-neu

Das deutsche Datenschutzrecht hat seit Einführung des Datenschutzbeauftragten im Jahr 1977 an dem Prinzip festgehalten, dass der internen (Vorab-)Kontrolle durch den Datenschutzbeauftragten der Vorrang vor der Fremdkontrolle durch die Aufsichtsbehörden zu geben ist. Seither hat sich der Datenschutzbeauftragte in Deutschland als internes Kontrollorgan in Unternehmen etabliert, wobei die konkrete Ausgestaltung der Regelungen zur Funktion des Datenschutzbeauftragten im Laufe der Zeit regelmäßig angepasst wurde.

Mit der Datenschutzrichtlinie aus dem Jahr 1995 fand die Idee des Datenschutzbeauftragten auch erstmalig Einzug in einen europäischen Rechtsakt, allerdings nicht als verpflichtende Vorgabe, sondern als eine von mehreren Kontrollalternativen. Diese freiwillige Möglichkeit zur Schaffung eines Datenschutzbeauftragten wurde seinerzeit außerhalb von Deutschland kaum genutzt.

Mit Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) und der Anwendung ihrer Regelungen im Mai 2018 wird das Datenschutzrecht europaweit vereinheitlicht. Durch diese Vereinheitlichung ergeben sich auch zahlreiche Änderungen in Bezug auf die Funktion des Datenschutzbeauftragten.

Wie ist die bisherige Rechtslage?

Unter dem geltenden deutschen Recht muss jede verantwortliche Stelle einen Datenschutzbeauftragten gemäß § 4f Abs. 1 S. 1 BDSG bestellen. Eine Ausnahmevorschrift lässt diese Pflicht nur dann entfallen, wenn bei einer nicht-öffentlichen Stelle, also insbesondere Unternehmen, nicht mehr als neun Personen mit der automatisierten Verarbeitung personenbezogener Daten gem. § 4 f Abs. 1 S. 4 BDSG befasst sind. Zusätzlich ist eine Ausnahmeregelung für den Fall vorgesehen, dass keine automatisierte Datenverarbeitung erfolgt. In diesen Fällen ist ein Datenschutzbeauftragter erst dann verpflichtend, wenn mindestens 20 Personen in dem Unternehmen beschäftigt sind. Diese Alternative ist aber ohne praktische Relevanz, da fast in allen Unternehmen mittlerweile IT-Systeme zur automatisierten Datenverarbeitung zum Einsatz kommen dürften.

Es darf gemäß § 4 f Abs. 2 S. 1 BDSG nur eine solche Person zum Datenschutzbeauftragten bestellt werden, die über die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit verfügt. Das Maß der erforderlichen Sachkunde hängt insbesondere auch von dem Umfang der Datenverarbeitung und dem Schutzbedarf der von der verantwortlichen Stelle verarbeiteten Daten ab, § 4 f Abs. 2 S. 2 BDSG.

Organisatorisch ist der Datenschutzbeauftragte gemäß § 4 f Abs. 3 S. 1 BDSG dem Leiter der verantwortlichen Stelle in einem Unternehmen, also der Geschäftsführung, unmittelbar unterstellt. Bei Ausübung seiner Tätigkeit ist der Datenschutzbeauftragte gemäß § 4f Abs. 3 S. 2 BDSG weisungsfrei. Zur Sicherstellung der Weisungsfreiheit und Unabhängigkeit genießt der interne Datenschutzbeauftragte einen besonderen Kündigungsschutz, für externe Datenschutzbeauftragte soll eine hinreichend lange Mindestdauer für die Zusammenarbeit definiert werden.

Inhaltlich hat der Datenschutzbeauftragte gemäß § 4 g BDSG im Rahmen seiner Tätigkeit auf die Einhaltung des Datenschutzes „hinzuwirken“. Diese Formulierung wird dabei so interpretiert, dass der Datenschutzbeauftragte im Ergebnis nicht für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich ist, also die Compliance des Unternehmens nicht sicherzustellen hat. Die Aufgabe des Datenschutzbeauftragten ist vielmehr die Beratung des Unternehmens und die Schulung der Mitarbeiter hinsichtlich der bestehenden datenschutzrechtlichen Pflichten sowie die Unterstützung bei der datenschutzkonformen Umsetzung von Projekten. Auf erkannte Rechtsverstöße oder drohende Risiken ist aber gleichwohl hinzuweisen.

Soweit nicht ohnehin eine Pflicht zur Bestellung eines Datenschutzbeauftragten besteht, kommt auch eine freiwillige Bestellung eines Datenschutzbeauftragten in Betracht, um überobligatorisch einen zentralen Ansprechpartner für Datenschutzfragen zu etablieren.

Was ändert sich unter der DSGVO und dem BDSG-neu?

Mit dem Inkrafttreten der Datenschutz-Grundverordnung werden neue datenschutzrechtliche Anforderungen in materieller und formeller Hinsicht eingeführt, die zukünftig in den Verantwortungsbereich des Datenschutzbeauftragten fallen. Zugleich entfallen einzelne Aufgaben, die dem Datenschutzbeauftragten bisher gesetzlich zugewiesen worden waren.

In der Datenschutz-Grundverordnung ist ein Katalog mit Pflichtaufgaben vorgesehen, die dem Datenschutzbeauftragten gemäß Art. 38 Abs. 1 DSGVO „zumindest“ obliegen. Im Umkehrschluss lässt sich daraus ableiten, dass weitere Aufgaben zwischen dem für die Verarbeitung Verantwortlichen und dem Datenschutzbeauftragten abgestimmt und vereinbart werden müssen.

Standardaufgaben des Datenschutzbeauftragten sind auch zukünftig die Unterrichtung und Beratung des Verantwortlichen, des Auftragsverarbeiters und der Beschäftigten, die Überwachung der Einhaltung der datenschutzrechtlichen Anforderungen sowie die Zusammenarbeit mit den Datenschutzaufsichtsbehörden.

Anders als die Vorabkontrolle nach dem BDSG ist die Durchführung der Datenschutz-Folgenabschätzung nicht Aufgabe des Datenschutzbeauftragten; zuständig ist stattdessen der für die Verarbeitung Verantwortliche. Der Datenschutzbeauftragte hat aber gemäß Art. 39 Abs. 1 lit. c) DSGVO die Durchführung der Datenschutz-Folgenabschätzung zu überwachen und auf Anfrage bei der Durchführung zu beraten. Eine Pflicht der für die Verarbeitung Verantwortlichen, den Rat des Datenschutzbeauftragten im Rahmen der Datenschutz-Folgenabschätzung einzuholen, ergibt sich aus Art. 35 Abs. 2 DSGVO. Faktisch ist der Datenschutzbeauftragte damit in alle Datenschutz-Folgenabschätzungen einzubeziehen, außerdem dürfte es regelmäßig wegen der besonderen Fachkenntnisse sinnvoll sein, über die Mindestanforderungen hinaus den Datenschutzbeauftragten mit der Steuerung der Dokumentationstätigkeiten zu betrauen.

Die Pflicht des Datenschutzbeauftragten zur Bereitstellung des Verfahrensverzeichnisses „für jedermann“ aus § 4g Abs. 2 S. 2 BDSG entfällt zukünftig. Grundsätzlich sind aber weiter alle Verarbeitungstätigkeiten mit Bezug zu personenbezogenen Daten zu dokumentieren. Das bisherige Verfahrensverzeichnis ist um zusätzliche Angaben zu ergänzen und heißt zukünftig „Verzeichnis von Verarbeitungstätigkeiten“ gem. Art. 30 DSGVO.

Zusätzlich hat der Datenschutzbeauftragte gemäß Art. 39 Abs. 1 lit. b) DSGVO zukünftig die Strategie des Verantwortlichen für den Schutz personenbezogener Daten zu überwachen. Weiter hat der Datenschutzbeauftragte im Rahmen seiner Tätigkeit gemäß Art. 39 Abs. 2 DSGVO den mit den Verarbeitungsvorgängen verbunden Risiken gebührend Rechnung zu tragen, wobei Art, Umfang, Umstände und Zweck der Verarbeitung zu berücksichtigen sind. Dieser risikobasierte Ansatz ist neu und führt dazu, dass besonders risikoträchtige Themen genauer geprüft werden müssen, während im Gegenzug bei unkritischen Themen eine vereinfachte Prüfung genügen kann. Die konkrete Priorisierung der Aufgaben ist dem Datenschutzbeauftragten, dem ohnehin gemäß Art. 38 Abs. 3 DSGVO Unabhängigkeit garantiert ist, dabei selbst überlassen.

In Deutschland ist wie bisher ein Datenschutzbeauftragter gemäß § 38 Abs. 1 S. 1 BDSG-neu zu bestellen, wenn in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Insoweit hat der deutsche Gesetzgeber – anders als die meisten anderen Mitgliedstaaten – die entsprechende Öffnungsklausel der DSGVO genutzt, wonach auf nationaler Ebene Fälle vorgesehen werden können, die zu einer Bestellpflicht führen. Europaweit einheitlich besteht zudem eine Bestellpflicht gemäß Art. 37 DSGVO für Behörden und staatliche Stellen sowie Unternehmen, die besonders sensible Daten im Sinne von Art. 9 DSGVO verarbeiten. Darüber hinaus müssen auch Unternehmen, deren Kerntätigkeit die Durchführung von Verarbeitungsvorgängen ist, einen Datenschutzbeauftragten bestellen, soweit Art, Umfang und Zweck der Datenverarbeitung eine regelmäßige und systematische Überwachung von Personen erforderlich machen. Letztgenannte Alternative dürfte insbesondere für Auskunfteien, Detekteien, unter Umständen aber auch für Versicherungen und Online-Händler gelten.

Was sollten Unternehmen mit Hinblick auf die Rechtsänderung veranlassen?

Mit Hinblick auf die gestiegenen Anforderungen an Datenschutzbeauftragte und deren Tätigkeit ist Unternehmen zu empfehlen, den Bereich der datenschutzrechtlichen Beratung zu professionalisieren. Dies gilt insbesondere vor dem Hintergrund steigender Haftungsrisiken bei Datenschutzverstößen.

Die Bestellung eines Datenschutzbeauftragten dürfte vielfach auch für solche Unternehmen sinnvoll sein, die nicht der Bestellpflicht unterfallen. Mit der Datenschutz-Grundverordnung werden eine Vielzahl neuer datenschutzrechtlicher Verpflichtungen eingeführt, deren interne Verantwortlichkeit ohnehin bei allen für die Verarbeitung Verantwortlichen geklärt werden muss. Der Schritt zur förmlichen Bestellung ist dann ohnehin nicht mehr weit und kann beispielsweise für Unternehmen auch in der Außendarstellung Vorteile haben.

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

Bei fehlender Bestellung eines Datenschutzbeauftragten trotz bestehender Bestellpflicht droht nach geltendem Recht gemäß § 43 Abs. 1 Nr. 2 BDSG ein Bußgeld von bis zu 50.000

Euro. Nach dem zukünftigen Recht kann in derartigen Fällen 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.

Der Datenschutzbeauftragte haftet auch zukünftig nicht im Außenverhältnis für die Einhaltung der datenschutzrechtlichen Pflichten durch das Unternehmen. Im Innenverhältnis zum Unternehmen kann sich jedoch eine Haftung ergeben, wenn der Datenschutzbeauftragte seine Aufgabe nicht ordnungsgemäß ausführt. Für Unternehmen hat die Bestellung eines Datenschutzbeauftragten oftmals den Vorteil, dass die Verhängung von ansonsten drohenden Geldbußen vermieden werden kann, wenn der Datenschutzbeauftragte geschickt einbezogen wird. Umgekehrt hat der Datenschutzbeauftragte darauf zu achten, die Haftung durch vertragliche Regelungen zu begrenzen oder sich auf andere Art abzusichern.

Fazit

Mit der DSGVO wird erstmals europaweit eine Verpflichtung zur Bestellung eines Datenschutzbeauftragten eingeführt, wenn auch nur in einem relativ engen Anwendungsbereich. In Deutschland müssen, von wenigen Ausnahmen abgesehen, alle Unternehmen einen Datenschutzbeauftragten bestellen.

Im Kern bleibt der Datenschutzbeauftragte eine interne Kontrollinstanz im Unternehmen. Zwar übernimmt der Datenschutzbeauftragte im Außenverhältnis nicht die Verantwortung für die Einhaltung aller datenschutzrechtlicher Vorschriften, dennoch kann sich im Innenverhältnis aus der Verletzung der Pflichten eine Haftung des Datenschutzbeauftragten ergeben. Unternehmen sollten deswegen auch unter Haftungsgesichtspunkten sorgfältig prüfen, wer als Datenschutzbeauftragter in Betracht kommt.

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