MAYER·BROWN

Legal Update
1. Februar 2011

Auf betriebliche Datenschutzbeauftragte kommen neue Anforderungen zu

Am 24./25. November 2010 hat der Düsseldorfer Kreis hohe Mindestanforderungen im Hinblick darauf beschlossen, welche Fachkunde betriebliche Datenschutzbeauftragte vorweisen müssen und welche Rahmenbedingungen für ihre Arbeit gelten. Der Düsseldorfer Kreis ist das gemeinsame Abstimmungsgremium der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich. Seine Beschlüsse haben erhebliche Auswirkungen für die Unternehmen: Die auf Landesebene zuständigen Aufsichtsbehörden koordinieren ihr Vorgehen im Rahmen des Düsseldorfer Kreises und setzen dessen Beschlüsse in aller Regel konsequent um.

Gesetzliche Anforderungen an betriebliche Datenschutzbeauftragte und die Rahmenbedingungen ihrer Arbeit

Unternehmen müssen gemäß § 4f Abs. 1 Bundesdatenschutzgesetz (BDSG) unter anderem dann einen betrieblichen Datenschutzbeauftragten schriftlich bestellen, wenn sie zehn oder mehr Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen oder Datenverarbeitungen vornehmen, die einer Vorabkontrolle unterliegen. Der Datenschutzbeauftragte, so das Gesetz „wirkt darauf hin“, dass das BDSG und andere Vorschriften über den Datenschutz eingehalten werden. Zu seinen Aufgaben gehört es also beispielsweise, die Unternehmensführung auf mögliche Verstöße oder entstehenden Nachbesserungsbedarf hinzuweisen. Um diese Aufgaben ordnungsgemäß erfüllen zu können, muss er nach § 4f Abs. 2 BDSG über ein bestimmtes Maß an Fachkunde und Zuverlässigkeit verfügen. Die erforderlichen rechtlichen, technischen sowie organisatorischen Mindestkenntnisse müssen bereits vorliegen, wenn der Datenschutzbeauftragte bestellt wird.

Mindestanforderungen und Folgen von Verstößen

Bei Kontrollen haben die obersten Aufsichtsbehörden nun festgestellt, dass Fachkunde und Rahmenbedingungen für die Arbeit der Datenschutzbeauftragten nicht durchgängig den Anforderungen des BDSG genügen. Das haben sie zum Anlass genommen, um die Mindestanforderungen an die Fachkunde und Unabhängigkeit der betrieblichen Datenschutzbeauftragten näher festzulegen.

Diese Vorgaben können für Unternehmen direkte Konsequenzen haben: Die Bestellung eines Datenschutzbeauftragten, dessen Fachkunde, Zuverlässigkeit oder Stellung im Unternehmen nicht den gesetzlichen Anforderungen entspricht, kann gemäß § 43 Abs. 1 Nr. 2 BDSG mit einem Bußgeld von bis zu 50.000 Euro bestraft werden. Würde das bekannt, wären darüber hinaus Rufschäden die Folge, möglicherweise auch weitere Ermittlungen.

Erforderliche Fachkunde des Datenschutzbeauftragten

Datenschutzbeauftragte müssen über die für die Erfüllung ihrer Aufgaben notwendige Fachkunde verfügen. Das Gesetz bestimmt nicht näher, was genau darunter zu verstehen ist. Vor dem Hintergrund, dass die Anforderungen an die Funktion des Datenschutzbeauftragten aber generell gestiegen sind, fordern die Aufsichtsbehörden als Mindestmaß nun Folgendes:

Umfassende allgemeine Kenntnisse im Datenschutzrecht

Unabhängig von der Branche und der Größe des Unternehmens muss jeder Datenschutzbeauftragte über nicht unerhebliches Wissen im Datenschutzrecht verfügen. Das umfasst unter anderem Grundkenntnisse zu den verfassungsrechtlich garantierten Persönlichkeitsrechten der von Datenverarbeitungen Betroffenen und der Mitarbeiter des Unternehmens. Zudem muss der Datenschutzbeauftragte die für Unternehmen einschlägige Regelungen des BDSG kennen. Dies betrifft auch technische und organisatorische Bestimmungen zum Datenschutz, wie etwa § 9 BDSG.

Zudem muss der Datenschutzbeauftragte mit den tragenden Prinzipien des Datenschutzes gut vertraut sein. Diese Forderung der Aufsichtsbehörden bezieht sich vor allem auf die anerkannten Grundsätze zum Datenschutz. Hier sind etwa der datenschutzrechtliche Verhältnismäßigkeitsgrundsatz (etwa in Form der Verpflichtung zur Datenvermeidung und Datensparsamkeit gemäß § 3a BDSG) zu nennen sowie das Prinzip des Verbots der Datenverarbeitung mit Erlaubnisvorbehalt nach § 4 Abs. 1 BDSG, der Zweckbindungsgrundsatz und das Transparenzgebot.

Branchenspezifische Kenntnisse

Abhängig von der Branche, Größe oder IT-Infrastruktur des jeweiligen Unternehmens und der Sensibilität der zu verarbeitenden Daten können nach Auffassung der Aufsichtsbehörden noch weitere Mindestanforderungen hinzukommen.

Erforderlich sind umfassende Kenntnisse spezialgesetzlicher datenschutzrelevanter Vorschriften, die für das jeweilige Unternehmen wichtig sind. So wird etwa der Datenschutzbeauftragte einer Bank § 25c KWG im Detail kennen müssen, der Datenschutzbeauftragte einer Versicherung § 80d VAG.

Zudem fordern die Aufsichtsbehörden Kenntnisse der Informations- und Telekommunikationstechnologie und der Datensicherheit. Dies soll unter anderem die physische Sicherheit von Datenverarbeitungsanlagen, Kryptographie, Netzwerksicherheit, Schadsoftware und Schutzmaßnahmen betreffen. Auch Kenntnisse im praktischen Datenschutzmanagement des Unternehmens sollen je nach Unternehmen und Branche notwendig sein. Der Beschluss des Düsseldorfer Kreises nennt als Beispiele für solche praktischen Fähigkeiten etwa die zur Durchführung von Kontrollen, die Beratung der Unternehmensführung und der Mitarbeiter, die Strategieentwicklung, die Dokumentation von datenschutzrelevanten Vorgängen, die Erstellung von Verfahrensverzeichnissen sowie Kenntnisse zur Logfile-Auswertung, zum Risikomanagement, zur Analyse von Sicherheitskonzepten, über Betriebsvereinbarungen, Videoüberwachungen und die Zusammenarbeit mit dem Betriebsrat.

Gegebenenfalls muss der Datenschutzbeauftragte auch eine betriebswirtschaftliche Grundkompetenz vorweisen. Dies kann nach den Vorgaben des Düsseldorfer Kreises etwa Personalwirtschaft, Controlling, Finanzwesen, Vertrieb, Management oder Marketing umfassen. Ferner fordern die Aufsichtsbehörden Kenntnisse der technischen und organisatorischen Struktur des Unternehmens. Der Datenschutzbeauftragte sollte sich daher mit Aufbau- und Ablaufstrukturen sowie der Organisation des Unternehmens auskennen.

Anforderungen an die Unabhängigkeit des Datenschutzbeauftragten

Der betriebliche Datenschutzbeauftragte nimmt in Unternehmen eine Sonderrolle ein. Um ihm die unabhängige Ausübung seiner Kontroll- und Beratungsfunktionen zu ermöglichen, muss ihn das Unternehmen direkt der Unternehmensleitung unterstellen (§ 4f Abs. 3 Satz 1 BDSG). Bezüglich Fragen des Datenschutzes ist er weisungsfrei (§ 4f Abs. 3 Satz 2 BDSG), er genießt zudem einen gesetzlichen Sonderkündigungsschutz.

Der Datenschutzbeauftragte muss seine Aufgaben und Verpflichtungen ohne Interessenkonflikte erfüllen können. Das müssen Unternehmen durch entsprechende organisatorische und vertragliche Regelungen sicherstellen und dies sowohl innerhalb des Unternehmens als auch nach außen hin publik machen. Dies dürfte in der Praxis dazu führen, dass Unternehmen verpflichtet sind, die Öffentlichkeit nicht nur über die Kontaktdaten des Datenschutzbeauftragten zu informieren, sondern darüber hinaus bekannt zu geben, mit welchen Mitteln das Unternehmen die Unabhängigkeit des Datenschutzbeauftragten sicherstellt.

Ein Unternehmen darf einen angestellten (internen) Datenschutzbeauftragten wegen der Erfüllung seiner Aufgaben in Hinblick auf sein Beschäftigungsverhältnis gemäß § 4f Abs. 3 Satz 3 ff. BDSG nicht benachteiligen. Hieraus folgern die Aufsichtsbehörden, dass auch bei der Bestellung eines externen (also unternehmensfremden) Datenschutzbeauftragten der Dienstvertrag so ausgestaltet sein muss, dass grundsätzlich eine unabhängige Erfüllung der gesetzlichen Aufgaben gewährleistet wird. Dies soll durch entsprechende Kündigungsfristen, Zahlungsmodalitäten, Haftungsfreistellungen und Dokumentationspflichten gewährleistet werden. § 4f Abs. 3 BDSG schränke insoweit die grundsätzliche Vertragsfreiheit ein.

Der Düsseldorfer Kreis empfiehlt grundsätzlich eine Vertragslaufzeit von mindestens vier Jahren, bei Erstverträgen eine Laufzeit von ein bis zwei Jahren wegen der Notwendigkeit, die Eignung zu überprüfen. Bei Bestellung eines externen Datenschutzbeauftragten müssen Unternehmen eine bedarfsgerechte Leistungserbringung sicherstellen. Auch externe Datenschutzbeauftragte müssen ihre Leistungen in angemessenem Umfang in der beauftragenden verantwortlichen Stelle selbst erbringen. Hierfür sollen Unternehmen und externe Datenschutzbeauftragte ein angemessenes Zeitbudget konkret vereinbaren und vertraglich festgelegen.

Bei der Bestellung von externen Datenschutzbeauftragten kann die gesetzlich vorgeschriebene Fortbildung nach Auffassung des Düsseldorfer Kreises Bestandteil der vereinbarten Vergütung sein und muss nicht zusätzlich erbracht werden.

In der Praxis dürften die hohen Anforderungen der Aufsichtsbehörden wahrscheinlich dazu führen, dass die Fälle erheblich zunehmen, in denen externe Datenschutzbeauftragte bestellt werden.

Rahmenbedingungen innerhalb des Unternehmens

Die Aufsichtsbehörden machen zudem eine Reihe von Vorgaben, welche internen Strukturen zur Sicherstellung der gesetzlichen Anforderungen notwendig sind.

Das Unternehmen muss dem Datenschutzbeauftragten zur Erfüllung seiner Pflichten gemäß § 4g BDSG die erforderlichen Zutritts- und Einsichtsrechte in alle betrieblichen Bereiche einräumen. Er muss zudem in alle relevanten betrieblichen Planungs- und Entscheidungsabläufe eingebunden werden. In der Praxis kann dies in vielen Unternehmen dazu führen, dass die Bedeutung des Datenschutzbeauftragten deutlich aufgewertet und er an wesentlichen Entscheidungsprozessen beteiligt wird.

Ergebnis und Handlungsempfehlungen

Die Forderungen der Aufsichtsbehörden gehen sehr weit. Vor allem die von den Aufsichtsbehörden verlangten Fachkenntnisse erfordern ausgesprochen umfangreiche Vorkenntnisse und ein hohes Maß an Spezialisierung. Da der Unternehmensführung bei der Bestellung eines nicht hinreichend fachkundigen Datenschutzbeauftragten hohe Bußgelder drohen, ist Vorsicht geboten. Andererseits stellen die Aufsichtsbehörden auch klar, dass die Belastung des Datenschutzbeauftragten durch die Größe des Unternehmens beeinflusst wird, wie auch durch die Anzahl der vom einzelnen Datenschutzbeauftragten betreuten Unternehmen, die Besonderheiten branchenspezifischer Datenverarbeitungen und dem Grad der Schutzwürdigkeit der verarbeiteten personenbezogenen Daten. Richtigerweise sind an große Unternehmen oder solche Unternehmen, die besonders viele oder sensible Datenverarbeitungen vornehmen, höhere Anforderungen zu richten.

Die Aufsichtsbehörden empfehlen den Besuch von Fortbildungsveranstaltungen, um eventuell bestehende Informationsdefizite auszugleichen. Ob das in der Praxis ausreichen wird, um den umfassenden Forderungskatalog des Düsseldorfer Kreises zu erfüllen, bleibt abzuwarten. Unternehmen sollten jedenfalls möglichst zeitnah sicherstellen, dass ihr Datenschutzbeauftragter die beschriebenen hohen Anforderungen an Fachkunde und Stellung im Unternehmen erfüllt. Falls notwendig lässt sich die erforderliche Fachkunde auch durch die vertraglich dokumentierte Zusammenarbeit mit externen Datenschutzexperten sicherstellen.

Sollten Sie zu dieser Publikation noch mehr Informationen wünschen, wenden Sie sich bitte an einen der folgenden Ansprechpartner:

Tim Wybitul
T: +49 69 79 41 2271
twybitul@mayerbrown.com

Dr. Guido Zeppenfeld, LL.M.
T: +49 69 79 41 1701
gzeppenfeld@mayerbrown.com