Der Datenschutzbeauftragte als Tausendsassa?

Rollen und Verantwortlichkeiten in der Datenschutzorganisation: Im Datenschutzbereich fallen zahlreiche strategische und operative Aufgaben an. Eine Aufgabenverteilung hilft dabei, die einer jeden Datenschutzorganisation innewohnenden Risiken zu reduzieren.

Die Datenschutz-Grundverordnung (DSGVO) überträgt Verantwortlichen und Auftragsverarbeitern die Pflicht, ihre innerbetriebliche Datenschutzorganisation derart zu gestalten, dass die Datenverarbeitungen jederzeit im Einklang mit den Anforderungen erfolgen. Werden dabei lediglich die gesetzlichen Mindestanforderungen umgesetzt, geraten Datenschutzorganisationen in der betrieblichen Realität schnell an ihre Grenzen: Sie halten den komplexen regulatorischen und aufsichtsbehördlichen Anforderungen sowie den veränderten Kundenerwartungen nicht stand. Unternehmen, die lediglich einen Datenschutzbeauftragten benennen (egal ob intern oder extern) und damit die Erwartung verbinden, alle ihre Verpflichtungen aus der DSGVO umgesetzt und eine fortlaufende Compliance sichergestellt zu haben, werden für diesen Irrtum häufig abgestraft.

Überforderung und Interessenkollision

Ein durchschnittlich informierter Beschäftigter ist mit den komplexen datenschutzrechtlichen Bestimmungen üblicherweise nicht im Einzelnen vertraut. In zahlreichen Fällen (beispielsweise bei Vertragserstellung, Änderungen von Geschäftsprozessen, Produkteinführungen, Kundenbeschwerden oder im Falle von Datenschutzverletzungen) besteht daher das Bedürfnis nach Beratung und Unterstützung. In Ermangelung einer speziellen Stelle im Unternehmen wird in all diesen Fällen häufig der Datenschutzbeauftragte konsultiert. Dabei wird nicht selten der gesetzliche Beratungsauftrag falsch verstanden und als Unterstützungsauftrag ausgelegt. Es wird erwartet, dass der Datenschutzbeauftragte die Aufgaben in Gänze übernimmt. Aus naheliegenden Gründen können diese Aufgaben aber nicht in vollem Maße an ihn delegiert werden. Der Hauptgrund für diese Limitierung besteht in der gesetzlich geforderten Unabhängigkeit des Datenschutzbeauftragten und der damit zusammenhängenden Problematik von latenten Interessenkonflikten.

Die zwischen der notwendigen Bestellung eines Datenschutzbeauftragten und der Erfüllung operativer Compliance-Pflichten bestehende Lücke muss durch weitere Maßnahmen geschlossen werden. Hierzu sind organisatorische und personelle Aspekte festzulegen. Im Folgenden soll aufgezeigt werden, welche Bereiche, Stellen und Funktionen in eine risikoadäquate Datenschutzorganisation eingebunden werden sollten.

Unternehmensleitung und Supportbereiche

Gesamtverantwortung für den Datenschutz trägt die Unternehmensleitung (Vorstand, Geschäftsführung). Dies umfasst die Verantwortung für die wirksame Umsetzung und regelmäßige Kontrolle aller datenschutzrechtlichen Vorgaben. Sofern die Aufgaben zur Umsetzung der Vorgaben an Mitarbeiter delegiert werden, muss dies in geeigneter Weise dokumentiert werden. Dazu gehört es, dass mittels Anweisungen wie Leitlinien, Richtlinien, Arbeitsanweisungen die einzelnen Stellen und deren Aufgaben in

der Aufbau- und Ablauforganisation festgelegt werden. Die Leitung trägt die Verantwortung für die Bereitstellung der erforderlichen finanziellen, sachlichen wie personellen Ressourcen und muss durch Etablierung eines Reportingsystems sicherstellen, dass sie trotz Delegation von Aufgaben und Zuständigkeiten stets über den Zustand des Datenschutzes im Unternehmen informiert bleibt. Eine regelmäßige (auch unterjährige) Berichterstattung ist daher zwingend erforderlich. Es bietet sich zudem an, dem Datenschutzbeauftragten eine Teilnahme an Vorstandssitzungen zu ermöglichen, soweit dort datenschutzrechtliche Themen vorgestellt und besprochen werden.

Auch einzelnen Supportbereichen (also speziellen Fachbereichen mit Management- und Servicefunktionen, z. B. Organisation, Recht, Informationssicherheit und Revision) können Aufgaben aus der Datenschutzorganisation zugewiesen werden. In Betracht kommen hier etwa die Bearbeitung von Beschwerden mit Datenschutzbezug, Betroffeneneingaben zu Einwilligungen, Widersprüchen, Auskunftsersuchen und Löschersuchen. Häufig werden in Supportbereichen bereits ticketbasierte Lösungen eingesetzt, die für die Bearbeitung von Betroffenenrechten mitgenutzt werden können. Darüber hinaus können sie mit spezifischem Know-how Aufgaben z. B. in der Beschaffung und dem Lieferantenmanagement übernehmen, Vertragsprüfungen durchführen und Sicherheitsmaßnahmen prüfen und bewerten (Informationssicherheit).

Operative Organisationseinheiten

Für die Umsetzung der restlichen datenschutzrechtlichen Vorgaben sind grundsätzlich die operativen Organisationseinheiten (Fachbereiche/Geschäftsbereiche) zuständig. Als Prozess- und Verarbeitungsverantwortliche tragen sie für einen angemessenen Schutz der verarbeiteten personenbezogenen Daten bei der Gestaltung und Durchführung ihrer Datenverarbeitungen Sorge. Dies umfasst insbesondere die Vornahme datenschutzrechtlicher Risikobewertungen, Erstellung von Löschkonzepten und bedarfsweise Durchführung von Datenschutz-Folgenabschätzungen. Um eine Nachweisbarkeit der Maßnahmen zu gewährleisten, haben die Organisationseinheiten eine angemessene Dokumentation anzufertigen und grundsätzlich auch die fortlaufende Pflege des Verzeichnisses der Verarbeitungstätigkeiten zu übernehmen. Ab einer gewissen Größe und Innovationsfreudigkeit sollten Organisationseinheiten als Schnittstelle zum Datenschutzbeauftragten einen eigenen Koordinator benennen.

Möglichkeiten und Grenzen der Aufgabenzuweisung an den Datenschutzbeauftragten

Die Aufgaben des Datenschutzbeauftragten ergeben sich zunächst aus den Artikeln 38 und 39 DSGVO. Danach fungiert er u. a. als Anlaufstelle für betroffene Personen. Ihm obliegt die Unterrichtung und allgemeine Beratung der Organisationseinheiten und die spezielle Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung. Er hat entsprechend im Unternehmen adressatengerecht zu kommunizieren und der höchsten Managementebene zu berichten. Seine Hauptaufgabe liegt jedoch in der Überwachung der Einhaltung der Datenschutzvorschriften im Unternehmen. Die Stelle des Datenschutzbeauftragten ist daher als unabhängiges Überwachungsorgan auszugestalten. Das verantwortliche Unternehmen muss ihm die dazu notwendige Unabhängigkeit gewähren. Führt er Aufgaben bzw. operative Tätigkeiten aus, die er im Rahmen seiner Überwachungstätigkeit kontrollieren sollte, treten schnell Interessenkonflikte zutage.

Es existieren zahlreiche mögliche Fallkonstellationen, in denen es zu einer „kritischen Nähe“ verschiedener Tätigkeiten kommen kann. Für die Frage nach der Zulässigkeit des Tätigwerdens sind oft Details ausschlaggebend. In welchen Fällen der Verantwortliche den Datenschutzbeauftragten als Erfüllungsgehilfen heranziehen kann, soll nachfolgend anhand ausgewählter Pflichten erläutert werden:

1. **Beantwortung von Betroffenenanfragen einschließlich Datenschutzbeschwerden**
   Die Beantwortung von Betroffenenanfragen sollte nach Möglichkeit durch zentrale Servicebereiche erfolgen, da diese ohnehin regelmäßig Kundenkorrespondenz führen. Der Datenschutzbeauftragte kann hier zuarbeiten. Soll die Bearbeitung vollständig an den Datenschutzbeauftragten delegiert werden, ist dies als wesentlicher Faktor bei seiner regelmäßigen Aufwandsabschätzung (Umfang der nötigen Aufwände) zu berücksichtigen.

2. **Erstellung und Pflege des Verzeichnisses von Verarbeitungstätigkeiten**
   Nach Art. 30 DSGVO ist der Verantwortliche (also die Unternehmensleitung oder die Fachbereiche) für die Erstellung und Pflege eines Verarbeitungsverzeichnisses zuständig. In der Praxis kann trotzdem häufig beobachtet werden, dass diese Aufgabe durch den Datenschutzbeauftragten wahrgenommen wird. Dies ist dann pro-

blematisch, wenn der Datenschutzbeauftragte damit nicht ausdrücklich von seiner Unternehmensleitung beauftragt wurde. Es ist zudem sicherzustellen, dass die jeweiligen Prozess- und Verarbeitungsverantwortlichen zur fortlaufenden Bereitstellung der erforderlichen Informationen verpflichtet werden und die Vollständigkeit und Aktualität des Verzeichnisses im Rahmen des Internen Kontrollsystems (IKS) überwacht wird.

3. **Entscheidung über die Meldung von Datenschutzverletzungen**
   Eine Beteiligung des Datenschutzbeauftragten bei Bewertungs- und Dokumentationsvorgängen im Rahmen von Datenschutzverletzungen sollte nach Möglichkeit vermieden werden. Die Vorfälle können durch den Datenschutzbeauftragten begleitet und bedarfsweise nachträglich durch ihn geprüft werden. Entsprechende Prüfungen würden durch eine zu aktive Rolle in den zu prüfenden Vorgängen jedoch entwertet. In keinem Fall darf ihm die Kompetenz zur Entscheidung von Meldungen nach Art. 33 bzw. Benachrichtigungen gemäß Art. 34 DSGVO übertragen werden.

4. **Durchführung einer Datenschutz-Folgenabschätzung**
   Der Datenschutzbeauftragte ist verpflichtet, die Durchführung der Datenschutz-Folgenabschätzung zu überwachen. Daraus folgt, dass er sie nicht selbst durchführen, sondern lediglich eine beratende Funktion einnehmen darf. Folgenabschätzungen sind mitunter komplex und zeitaufwändig. Es bietet sich daher regelmäßig an, einen Dienstleister hinzuzuziehen.

Nicht nur die Zuweisung einzelner operativer Datenschutztätigkeiten, auch die gleichzeitige Wahrnehmung artfremder Aufgaben durch den Datenschutzbeauftragten kann zu Interessenkonflikten führen. Positionen, bei denen über Zwecke und Mittel einer Datenverarbeitung entschieden wird, dürfen Datenschutzbeauftragte nicht innehaben. Mitglieder der Geschäftsführung oder des Vorstandes sowie Beschäftigte mit ausgewählter Leitungsfunktion (Leitung der Personalabteilung, Leitung der IT-Abteilung, Leitung der Rechtsabteilung, Leitung der Marketing- oder Vertriebsabteilung) können daher nicht wirksam als Datenschutzbeauftragte benannt werden.

Unzulässig ist eine Benennung zum Datenschutzbeauftragten laut dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit regelmäßig auch für hierarchisch nachgeordnete Positionen, wie etwa Beschäftigte in der IT oder Personalabteilung sowie für Gesellschafter und Familienangehörige der Geschäftsleitung.

Die Übernahme der Funktion des Datenschutzbeauftragten in Personalunion mit der Tätigkeit des Informationssicherheitsbeauftragten oder Compliance-Beauftragten ist laut dem Hessischen Beauftragten für Datenschutz und Informationsfreiheit ebenfalls in einigen Fällen unzulässig. Ähnlich kritisch äußerten sich dazu in der Vergangenheit bereits die Datenschutz-Aufsicht in Bremen sowie der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit.

Sehr bedenklich ist auch die Wahrnehmung in Personalunion mit dem Amt des Betriebsratsvorsitzenden oder des Revisionsleiters, da es dem Datenschutzbeauftragten auch hier an der notwendigen Unabhängigkeit fehlen könnte. Unternehmen sollten zudem stets einen Vertreter benennen, für den die gleichen Anforderungen gelten. Sofern dies intern nicht abgebildet werden kann, bietet sich eine externe Beauftragtenvertretung an.

Maximilian Schmidt
Beauftragter Informationssicherheit und Datenschutz,
E-Mail: maximilian.schmidt@dz-cp.de

Datenschutzteam

Egal ob sich Verantwortliche dafür entscheiden, dem Datenschutzbeauftragten zur Vermeidung von Interessenkonflikten keine operativen Datenschutzaufgaben zu übertragen oder ob sie ihm in zulässiger Weise begrenzte operative Tätigkeiten delegieren: Es bedarf in jedem Fall einer oder mehrerer weiterer Stellen, die im Rahmen der Datenschutzorganisation die verbleibenden Pflichten übernehmen und insbesondere die Fachbereiche unterstützen. Hierzu sind entsprechende Stellen mit den erforderlichen Kompetenzen einzurichten. Um zu gewährleisten, dass Ausrichtung und Umsetzung des Datenschutzes im gesamten Unternehmen einheitlich erfolgen, können die entsprechenden Stellen in einem Datenschutzteam institutionalisiert werden. Abhängig von der Unternehmenskultur und dem vorherrschenden Management-Commitment bietet es sich an, auch die Unternehmensleitung im Rahmen ihrer Möglichkeiten ins Datenschutzteam einzubinden.

Es handelt sich hierbei um ein Modell, das im Hinblick auf unterschiedliche Einflüsse anzupassen ist, insbesondere Größe der Organisationseinheit, Umfang und Kritikalität der Datenverarbeitung. Gerade in kleineren Unternehmen können mehrere Rollen zusammenfallen oder sind extern zu besetzen.

Es haben sich verschiedene Bezeichnungen für entsprechende Stellen/Rollen etabliert (z. B. Datenschutzmanager, Datenschutzkoordinator, Datenschutzreferent). Wie die Stelle bezeichnet wird und welche Aufgaben ihr letztlich zugewiesen werden, kann jedes Unternehmen selbst entscheiden. Am geläufigsten dürfte der Datenschutzkoordinator sein, der insbesondere bei einer Auslagerung des Datenschutzbeauftragten als dessen Ansprechpartner fungiert, aber nicht zwangsläufig operative Datenschutzaufgaben ausführt. Gerade bei externen Datenschutzbeauftragten ist eine Zuarbeit durch eine operative Einheit jedoch sinnvoll. Entsprechend sollten Aufgabenverteilungen, klare Abgrenzungen zwischen den operativen Datenschutzrollen sowie dem Datenschutzbeauftragten und Fragen der Zusammenarbeit organisatorisch geregelt werden.

Fazit

Wird die Bedeutung einer arbeitsteiligen Datenschutzorganisation verkannt, drohen erhebliche Compliance-Risiken. Die strategische und operative Umsetzung des Datenschutzes muss durch geeignete strukturelle Maßnahmen und Prozesse sichergestellt werden. Der Datenschutzbeauftragte kann wie gezeigt nur in einigen Fällen herangezogen werden, da er laut Gesetz eine Beratungs- und Überwachungsfunktion innehat und insoweit nicht die Rolle eines „Datenschutz-Sachbearbeiters“ für die Fachbereiche übernehmen darf. Mithin verbleiben einige Aufgaben und Pflichten, die entweder geeigneten internen Bereichen oder neu zu schaffenden (internen oder externen) Stellen übertragen werden müssen. ▬