activeMind.AG

WHITEPAPER

BETRIEBLICHER DATEN-SCHUTZBEAUFTRAGTER NACH DSGVO

VERSION 1.0 // Juli 2017

Vorwort

Ab Mai 2018 gilt in allen Ländern der Europäischen Union (EU) die neue Datenschutz-Grundverordnung (DSGVO). Sie soll vor allem das Datenschutzniveau in Europa angleichen und die Datenschutzvorschriften harmonisieren. Als Verordnung ist die DSGVO deshalb unmittelbar anzuwenden und wird durch nationales Recht lediglich ergänzt bzw. konkretisiert.

Die EU-Datenschutz-Grundverordnung schreibt für viele Unternehmen einen betrieblichen Datenschutzbeauftragten vor. Benennung (Art. 37 DSGVO), Stellung (Art. 38 DSGVO) und Aufgaben (Art. 39 DSGVO) des Datenschutzbeauftragten werden konkretisiert. Dadurch wird der betriebliche Beauftragte für Datenschutz nun in jedem EU-Staat zur Pflicht. Bisher war die Bestellung des Datenschutzbeauftragten vor allem in Deutschland gesetzlich vorgeschrieben.

Doch auch für Unternehmen in Deutschland ändern sich mit der DSGVO einige Regelungen zum Datenschutzbeauftragten im Unternehmen. Die DSGVO formuliert diesbezüglich einige Ausgestaltungsmöglichkeiten für nationale Gesetzgebung. Dieser Möglichkeit kam die Bundesrepublik Deutschland mit der Novelle des bisher geltenden Bundesdatenschutzgesetzes (BDSG) im Frühjahr/Sommer 2017 als erster EU-Staat nach. Das von Bundestag und Bundesrat verabschiedete Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) enthält auch Konkretisierungen

zum Datenschutzbeauftragten für deutsche Unternehmen (insbesondere in § 38 DSAnpUG-EU).

In diesem Whitepaper finden Sie alle wichtigen Regelungen der DSGVO und des DSAnpUG-EU zum betrieblichen Datenschutzbeauftragten. Wir erläutern Ihnen, wer überhaupt einen Beauftragten zu bestellen hat, wie die Ernennung erfolgen muss und über welche Voraussetzungen der Kandidat verfügen sollte. Sie erfahren, welche Stellung der Datenschutzbeauftragte im Unternehmen innehat und welche arbeitsrechtlichen Regelungen zutreffend sind. Schließlich lernen Sie, welche Aufgaben der betriebliche Beauftragte für Datenschutz nach DSGVO wahrnehmen muss und wer in welchem Maße wofür haftet.

Datenschutz ist eines der großen Themen unserer Zeit. Von daher ist es absolut richtig, dass der Gesetzgeber dem Thema eine solche Relevanz beimisst. Für Ihr Unternehmen gilt es dabei nicht nur die in der DSGVO vorgesehenen drastischen Bußgelder oder – noch schlimmer – eine Datenpanne zu vermeiden. Stattdessen sollten Sie den unternehmerischen Datenschutz so implementieren, dass er zu einem echten Qualitätsmerkmal wird. Ein rechtskonform bestellter und tätiger Datenschutzbeauftragter ist einer der wichtigsten Schritte dafür!

Wir wünschen Ihnen eine aufschlussreiche Lektüre!

DAS ERWARTET SIE IN DIESEM WHITEPAPER

BESTELLUNG
Wer benötigt einen Datenschutzbeauftragten?

QUALIFIKATIONEN
Welche Voraussetzungen muss ein Datenschutzbeauftragter erfüllen?

STELLUNG
Welche Position hat der Datenschutzbeauftragte im Unternehmen?

AUFGABEN
Was muss ein Beauftragter für den Datenschutz im Unternehmen tun?

HAFTUNG
Wofür haftet der Datenschutzbeauftragte persönlich?

Inhaltsverzeichnis

1. Bestellung des Datenschutzbeauftragten

Die Funktion des betrieblichen Datenschutzbeauftragten ist in Deutschland seit langem bekannt und viele Unternehmen hierzulande müssen einen solchen bereits bestellen. Europaweit wurde die Bestellung eines Datenschutzbeauftragten bisher lediglich als Alternative für die Meldepflicht gegenüber der Datenschutzaufsichtsbehörde gesehen. Mit der DSGVO wird ab dem 25. Mai 2018 eine Bestellpflicht erstmals EU-weit eingeführt. Neben konkreten Vorgaben für die Bestellung eines Datenschutzbeauftragten, die unbedingt eingehalten werden müssen, enthält die DSGVO einige Regelungsspielräume, die nationale Sonderregelungen für die Bestellung eines betrieblichen Datenschutzbeauftragten schaffen.

1.1. Wer muss einen Datenschutzbeauftragten bestellen?

Mit der DSGVO werden zahlreiche Unternehmen in allen Mitgliedstaaten der Europäischen Union einen betrieblichen Datenschutzbeauftragten bestellen müssen. Diese Pflicht ergibt sich aus Art. 37 Abs. 1 DSGVO oder wenn nationales Recht solch eine Bestellpflicht vorsieht.

Nach Art. 37 Abs. 1 DSGVO muss ein Datenschutzbeauftragter im privatwirtschaftlichen Umfeld unter folgenden Voraussetzungen auf jeden Fall benannt werden:

- Die Kerntätigkeit des Unternehmens (als Verantwortlicher oder als Auftragsverarbeiter) erfordert eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen.

- Die Kerntätigkeit des Unternehmens besteht in der umfangreichen Verarbeitung von besonders sensiblen Daten (z. B. Gesundheitsdaten) oder personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten.

Art. 37 Abs. 1 DSGVO verzichtet auf eine feste Grenze von Mitarbeitern oder betroffenen Personen. Es kommt bei nichtöffentlichen Organisationen darauf an, ob der Verantwortliche bzw. der Auftragsverarbeiter bestimmte „Kerntätigkeiten" vornimmt. Außerhalb dieser Kriterien wird es den Verantwortlichen freigestellt, einen Datenschutzbeauftragten zu benennen oder nicht (Art. 37 Abs. 4 DSGVO).

In Erwägungsgrund 97 der DSGVO wird allgemein erklärt was unter Kerntätigkeit zu verstehen ist: Demnach sind damit die Haupttätigkeiten des Unternehmens gemeint und nicht die bloße Verarbeitung personenbezogener Daten als Nebentätigkeit. Ausschlaggebend ist also, dass die Haupttätigkeit des Unternehmens auf der Verarbeitung personenbezogener Daten beruht.

Auch die Artikel 29 Gruppe hat sich in einem Leitfaden (Working Paper 243 vom 13. Dezember 2016) mit dem Thema auseinandergesetzt. Als Kerntätigkeit sei demnach jede Tätigkeit zu verstehen, die essentiell für die Erreichung der Ziele des Unternehmens ist. Ein Beispiel wäre die fortlaufende Beobachtung des Nutzerverhaltens durch Betreiber von sozialen Netzwerken zur Anpassung von Werbeinhalten. Ein Onlineshop, der Kundendaten analysiert, um Produktvorschläge zu generieren, würde nicht unter die Verpflichtung fallen, da die Haupttätigkeit der Verkauf von Waren ist. Nicht als Kerntätigkeit wer-

den zudem Verarbeitungen im Zusammenhang mit der Verwaltung oder auch der Bezahlung der Mitarbeiter und des IT-Supports eingestuft.

Unklar ist jedoch, was unter einer „umfangreichen regelmäßigen und systematischen Überwachung“ (vgl. Art. 37 DSGVO Abs. 1 lit. b) bzw. „umfangreichen Verarbeitung“ (vgl. Art. 37 DSGVO Abs. 1 lit. c) zu verstehen ist. Hier lassen sich konkrete Zahlen schlecht festlegen.

Unter Berücksichtigung von Erwägungsgrund 24 DSGVO kann man unter dem Merkmal „regelmäßige und systematische Überwachung“ alle Arten des Onlinetrackings und -profilings verstehen. Der Begriff umfasst aber auch Überwachungsmethoden, die nicht im Internet, sondern offline stattfinden.

Die Artikel 29 Gruppe führt in ihrem Leitfaden einige Faktoren auf, die maßgeblich für das Merkmal „umfangreiche Verarbeitung“ sind. Hierzu sollen unter anderem die Zahl der betroffenen Personen, der Umfang der Datensätze oder auch die Dauer der Datenverarbeitung und ihre geographische Ausdehnung Berücksichtigung finden.

1.2. Sonderregelungen zur Bestellpflicht in Deutschland

Für Unternehmen, die nach den obengenannten Vorgaben keinen betrieblichen Datenschutzbeauftragten bestellen müssen, kann der nationale Gesetzgeber trotzdem eine solche Pflicht vorsehen.

In Deutschland wird die bisher im BDSG enthaltene Verpflichtung für die Bestellung eines betrieblichen Datenschutzbeauftragten beibehalten. Somit muss zusätzlich zu den oben genannten Kriterien auch weiterhin ein Datenschutzbeauftragter bestellt werden, wenn

- mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind (vgl. § 38 Abs. 1 S. 1 DSAnpUG-EU).

Darüber hinaus müssen Unternehmen, unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen, einen Datenschutzbeauftragten bestellen, wenn

- die Verarbeitung personenbezogener Daten einer Datenschutz-Folgeabschätzung nach Art. 35 DSGVO unterliegt oder

- „personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung“ verarbeitet werden.

Zusammenfassend lässt sich also festhalten, dass sich für Unternehmen in Deutschland die Vorgaben dazu, wann ein Datenschutzbeauftragter zu bestellen ist, zukünftig nicht grundlegend ändern (vgl. § 38 Abs. 1 S. 2 DSAnpUG-EU).

1.3. Neuregelung: Konzerndatenschutzbeauftragter

Eine Neuregelung der DSGVO ist die ausdrückliche Nennung eines Konzerndatenschutzbeauftragten. Gemäß Art. 37 Abs. 2 DSGVO darf eine „Unternehmensgruppe [...] einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann.“ Eine persönliche Präsenz ist demnach nicht erforderlich.

Laut Artikel 29 Datenschutzgruppe bezieht sich die Anforderung „leicht erreichbar“ auf die Aufgabe des Datenschutzbeauftragten, als Anlaufstelle für Mitarbeiter innerhalb des Konzerns, vor allem aber

auch als Anlaufstelle für Betroffene und die Aufsichtsbehörden zu fungieren.

Für Konzerne mit Gesellschaften außerhalb der EU sollte der Datenschutzbeauftragte seinen Sitz in einer konzernangehörigen Gesellschaft in der EU haben, um die leichte Erreichbarkeit zu gewährleisten. Der Datenschutzbeauftragte muss zudem in der Lage sein, sowohl mit den Betroffenen zu kommunizieren als auch mit den zuständigen Aufsichtsbehörden zusammenzuarbeiten. Daraus ergibt sich indirekt, dass der Datenschutzbeauftragte über ausreichende Sprachkenntnisse der Landessprache der Niederlassung verfügen muss.

Die rechtlichen Entwicklungen zur Benennung von Konzerndatenschutzbeauftragten sind abzuwarten. Im Gegensatz zu den Regelungen des BDSG, welche die Einzelbestellung durch jedes Unternehmen verlangt hat, dürfte es jedoch erheblich einfacher werden, einen Konzerndatenschutzbeauftragten zu bestellen.

1.4. Form der Bestellung

Nach dem BDSG musste ein betrieblicher Datenschutzbeauftragter schriftlich bestellt werden (vgl. § 4f Abs. 1 S. 1 BDSG). In der DSGVO ist jedoch lediglich von der „Benennung" eines Datenschutzbeauftragten die Rede. Eine schriftliche Benennung ist demnach nicht zwingend erforderlich.

Allerdings wird in Art. 37 Abs. 7 DSGVO vorgeschrieben, dass der „Verantwortliche oder der Auftragsverarbeiter [...] die Kontaktdaten des Datenschutzbeauftragten [veröffentlicht] und [...] diese Daten der Aufsichtsbehörde mit[teilt]." Mit anderen Worten: Sofern eine Bestellpflicht besteht, muss der Datenschutzbeauftragte zukünftig nicht nur benannt, sondern auch bei der Datenschutzbehörde

gemeldet werden. Ziel dieser Anforderungen ist es, sowohl den Betroffenen (innerhalb und außerhalb des Unternehmens!) als auch der Aufsichtsbehörde eine leichte Kommunikation mit dem Datenschutzbeauftragten zu ermöglichen.

Laut der Artikel 29 Gruppe ist es ausreichend, Kontaktinformationen wie Anschrift, Telefonnummer und E-Mail zu melden. Es wird jedoch zusätzlich empfohlen, der Aufsichtsbehörde und den Mitarbeitern eines Unternehmens die konkreten Kontaktdaten des Datenschutzbeauftragten mitzuteilen. Auf der Webseite eines Unternehmens sei es jedoch ausreichend, wenn beispielsweise eine Hotline oder spezifische Kontaktdaten veröffentlicht werden. Die Artikel 29 Gruppe erwähnt ausdrücklich, dass die Veröffentlichung des Namens des Datenschutzbeauftragten nicht erforderlich ist.

1.5. Sanktionen bei fehlender Bestellung

Bisher wurde die vorsätzliche oder fahrlässige Versäumnis einen betrieblichen Datenschutzbeauftragten zu bestellen in Deutschland als Ordnungswidrigkeit bestraft. Dafür konnte ein Bußgeld in Höhe von bis zu 50.000 Euro verhängt werden (vgl. § 43 Abs. 1 Nr. 2 BDSG).

Die DSGVO teilt diese Auffassung, sieht jedoch ein Bußgeld von bis zu 10 Mio. Euro oder zwei Prozent des weltweiten Jahresumsatzes vor, je nachdem, welcher Betrag höher (!) ist (vgl. Art. 83 Abs. 4 lit. a DSGVO).

2. Qualifikationen des Datenschutzbeauftragten

Art. 37 Abs. 5 DSGVO fordert, dass der Datenschutzbeauftragte über eine gewisse „berufliche Qualifikation“ und „Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis“ verfügt (vgl. bisher: § 4f Abs. 2 Satz 1 BDSG).

Nach Auffassung der Art. 29 Gruppe ist es maßgeblich, dass der Datenschutzbeauftragte Fachwissen

- im nationalen und europäischen Datenschutzrecht,
- in der Datenschutzpraxis und zusätzlich
- ein fundiertes Verständnis der DSGVO selbst haben muss.

Der Datenschutzbeauftragte übt eine Unterrichtungs-, Beratungs-, und Überwachungsfunktion aus. Deshalb sollte er nicht nur Kenntnisse über den Inhalt und Umgang mit datenschutzrechtlichen Bestimmungen haben. Stattdessen sollte er über ein umfassendes technisches Verständnis verfügen, um Sachverhalte der IT (Stichwort: Cloud-Computing bzw. Virtualisierung) und Risiken aus der Anwendung dieser Systeme richtig einschätzen zu können. Die konkreten Anforderungen an die Qualifikation des Datenschutzbeauftragten

hängen also stark von der Komplexität der Datenverarbeitungen und den Auswirkungen auf die Betroffenen ab.

Vor allem für international aufgestellte Unternehmen und Unternehmensgruppen ist es zudem relevant, dass der Datenschutzbeauftragte nicht nur über Kenntnisse des europäischen Datenschutzrechts verfügt, sondern auch über verschiedene nationale Spezialgesetze. Da die DSGVO den einzelnen Ländern für einige Bereiche Spielraum die nationalen Gesetzgeber überlässt (z. B. im Beschäftigungsdatenschutz), muss ein Datenschutzbeauftragter, der in mehreren Ländern tätig ist, solche nationalen Ausnahmevorschriften kennen und anwenden können.

3. Stellung des Datenschutzbeauftragten im Unternehmen

Grundsätzlich bleibt es Unternehmen auch unter der DSGVO überlassen, ob sie einen internen oder externen Datenschutzbeauftragten bestellen (vgl. Art. 37 Abs. 6 DSGVO). Um sicherzustellen, dass der Datenschutzbeauftragte seine Aufgaben erfüllen kann, formuliert Art. 38 Abs. 1-3 DSGVO einige Garantien:

3.1. Rechtzeitige Einbindung des Datenschutzbeauftragten

Der Verantwortliche bzw. der Auftragsverarbeiter ist verpflichtet, den Datenschutzbeauftragten frühzeitig in datenschutzrechtliche Fragen einzubinden (vgl. Art. 38 Abs. 1 DSGVO). So soll sichergestellt werden, dass erforderliche Informationen und Unterlagen für die Prüfung durch den Datenschutzbeauftragten diesem rechtzeitig vorliegen. Auf Basis seiner Überprüfung kann der Datenschutzbeauftragte dann konkrete Maßnahmen vorschlagen oder auf mögliche Datenschutzverletzungen hinweisen.

Frühzeitig oder rechtzeitig bedeutet demnach, dass der Datenschutzbeauftragte eingebunden werden muss, bevor konkrete Maßnahmen durchgeführt werden.

3.2. Unterstützung des Datenschutzbeauftragten

Der Verantwortliche bzw. der Auftragsverarbeiter ist verpflichtet, den Datenschutzbeauftragten bei der Erledigung seiner Aufgaben zu unterstützen (vgl. Art. 38 Abs. 2 DSGVO). Daraus ergibt sich, dass dem Datenschutzbeauftragten erforderliche Ressourcen, Zugang zu personenbezogenen Daten und Verarbeitungsprozessen sowie die Teilnahme an Weiterbildungen ermöglicht werden müssen.

In der DSGVO wird nicht explizit erwähnt, welche konkreten Mittel hierfür notwendig sind. Die Artikel 29 Gruppe listet in ihrem Leitfaden relevante Ressourcen auf, wie z. B. Personal, Räume und Arbeitsmittel, aber auch die Möglichkeit der kontinuierlichen Fortbildung.

3.3. Unabhängigkeit des Datenschutzbeauftragten

Um die Aufgaben sinnvoll erfüllen zu können, muss ein Datenschutzbeauftragter unabhängig von der verantwortlichen Stelle handeln können. Der Datenschutzbeauftragte darf im Hinblick auf die Erfüllung der Aufgaben deshalb nicht weisungsgebunden sein (vgl. Art. 38 Abs. 3 S. 1 DSGVO). Demnach dürfen dem Datenschutzbeauftragten keine Anweisungen erteilt werden, wie bei einem bestimmten Sachverhalt vorgegangen werden soll, beispielsweise welches Ergebnis erzielt oder nicht erzielt werden soll.

Hinzu kommt, dass der Datenschutzbeauftragte unmittelbar der höchsten Managementebene (Geschäftsführung, Vorstand) unterstellt ist (vgl. Art. 38 Abs. 3 S. 3 DSGVO). So soll ein unmittelbarer Berichtsweg zur Managementebene gewährleistet werden. Dies dient wiederum dem Zweck, dass der Datenschutzbeauftragte leichter auf die Einhaltung des Datenschutzes im Unternehmen hinwirken kann.

3.4. Arbeitsrechtliche Stellung des Datenschutzbeauftragten

Die DSGVO enthält (wie auch aus dem BDSG bekannt) einen Abberufungsschutz sowie ein Benachteiligungsverbot zum Schutz des Datenschutzbeauftragten (Art. 38 Abs. 3 S. 2 DSGVO). Eine ordentliche Kündigung kann demnach nicht auf Gründe gestützt werden, die mit der „Erfüllung seiner Aufgaben“ verbunden sind.

Allerdings enthält die DSGVO keine Angaben zu einem Sonderkündigungsrecht. Die Vorteile in Form eines Sonderkündigungsschutzes für den Datenschutzbeauftragten wie im BDSG (vgl. § 4f Abs. 3) geregelt, bleibt in Deutschland jedoch bestehen (vgl. § 38 Abs. 2 DSAnpUG-EU mit Verweis auf § 6 Abs. 4 DSAnpUG-EU).

3.5. Andere Tätigkeiten und Interessenskonflikte des Datenschutzbeauftragten

Nach Art. 38 Abs. 6 Nr. 1 DSGVO können dem Datenschutzbeauftragten auch andere Aufgaben und Pflichten übertragen werden, die nicht im Interessenkonflikt zu seinen sonstigen Aufgaben stehen. Der Leitfaden der Artikel 29 Datenschutzgruppe behandelt diese Thematik ausführlich und dient als Orientierungshilfe bei der Benennung eines Datenschutzbeauftragten:

So darf der Datenschutzbeauftragte keine sonstigen Aufgaben und Pflichten haben, die einen engen Bezug zu Verarbeitungen personenbezogener Daten aufweisen. Als Faustregel wird z. B. die Leitung der IT- oder der Personal-Abteilung genannt, wenn diese Positionen bei der Festlegung der Zwecke und Mittel zur Verarbeitung personenbezogener Daten mitwirken.

Es ist daher sehr zu empfehlen, die Funktionen der entsprechenden Positionen im Unternehmen zu ermitteln und zu benennen, um einen

Interessenkonflikt von vorneherein ausschließen zu können. Hierbei wird vom Einzelfall, d. h. der konkreten Situation im Unternehmen ausgegangen.

Auch bei der Benennung eines externen Datenschutzbeauftragten muss darauf geachtet werden, Interessenkonflikte zu vermeiden. Anwälte, Steuerberater, Wirtschaftsprüfer o. ä., die bereits für das Unternehmen tätig sind, würden im Zweifelsfall ebenso im Interessenkonflikt stehen. Es ist wichtig zu beachten, dass der Datenschutzbeauftragte ausschließlich dem Datenschutz und nicht dem Mandanten verpflichtet ist.

4. Aufgaben des Datenschutzbeauftragten

Die Aufgaben des Datenschutzbeauftragten werden künftig ausschließlich durch die DSGVO bestimmt. Regelungsspielräume für nationale Regelungen – wie etwa bei der Bestellpflicht – gibt es hier nicht. In Deutschland wird sich der Aufgabenbereich des Datenschutzbeauftragten deswegen im Vergleich zur bisherigen Rechtslage etwas verändern. Die Aufgaben des Datenschutzbeauftragten ergeben sich im Kern aus Art. 39 DSGVO. Dazu zählen:

- Unterrichtung und Beratung des Unternehmens sowie der datenverarbeitenden Beschäftigten über die bestehenden Datenschutzpflichten (Gesetze, Rechtsprechung etc.);
- Überwachung der Einhaltung datenschutzrechtlicher Regelungen (DSGVO und nationale Sonderregelungen) und betrieblicher Strategien für den Schutz personenbezogener Daten;
- Beratung bei und Überwachung der Durchführung einer Datenschutz-Folgenabschätzung;
- Anlaufstelle für und Zusammenarbeit mit der Aufsichtsbehörde;
- Ansprechpartner für betroffene Personen.

Der Datenschutzbeauftragte hat bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung zu tragen, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigen muss.

4.1. Aufgaben im Unternehmen

Das bisherige BDSG sieht lediglich vor, dass ein Datenschutzbeauftragter auf die Einhaltung der datenschutzrechtlichen Regelungen hinwirkt. Nach DSGVO muss der Beauftragte für Datenschutz zukünftig auch die Einhaltung überwachen. Nach wie vor ist jedoch das Unternehmen für die Einhaltung datenschutzrechtlicher Vorschriften verantwortlich.

Die Unterrichtung und Beratung sind die zentralen Aufgaben des Datenschutzbeauftragten im Unternehmen (vgl. Art. 39 Abs. 1 lit. a DSGVO). Die Unterrichtung richtet sich dabei auf allgemeine Information über die bestehenden datenschutzrechtlichen Pflichten. Die Beratung zielt auf die Unterstützung bei der Lösung von konkreten datenschutzrechtlichen Fragestellungen. Darüber hinaus muss der Datenschutzbeauftragte die Einhaltung dieser Pflichten durch regelmäßige Kontrollen der Verarbeitungsprogramme überwachen (vgl. Art. 39 Abs. 1 lit. b DSGVO).

Der Datenschutzbeauftragte ist – anders als nach BDSG – nicht für die Sensibilisierung bzw. der Schulung der Mitarbeiter verantwortlich, sondern lediglich für die Überwachung der Umsetzung durch den Verantwortlichen (vgl. Art. 39 Abs. 1 lit. b DSGVO).
Der für die Verarbeitung Verantwortliche kann jedoch dem Datenschutzbeauftragten die Durchführung der Schulungsaufgabe übertragen.

Neu ist auch, dass der Datenschutzbeauftragte künftig weder für die Durchführung von Datenschutz-Vorabkontrollen (nach DSGVO-Terminologie: Folgenabschätzung) noch für die Erstellung von Verfahrensverzeichnissen verantwortlich sein wird. Hierfür ist nun explizit das Unternehmen selbst verantwortlich.

Bei der Datenschutz-Folgenabschätzung kann der Datenschutzbeauftragte „auf Anfrage“ beratend beteiligt sein und muss ihre Durchführung überwachen (Art. 39 Abs. 1 lit. c). Trotz der Formulierung „auf Anfrage“ darf der Datenschutzbeauftragte bei der Datenschutz-Folgenabschätzung nicht außen vorgelassen werden. Dieses ergibt sich aus Art. 38 Abs. 1 DSGVO, der vorschreibt, dass der Datenschutzbeauftragte „ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen“ einzubinden ist. Entsprechendes gilt für die Anfertigung von Verarbeitungsverzeichnissen (Art. 30 DSGVO).

Der Leitfaden der Artikel 29 Datenschutzgruppe listet Fälle auf, bei denen der Verantwortliche den Datenschutzbeauftragten bei der Datenschutz-Folgenabschätzung insbesondere zu Rate ziehen sollte.

Im Falle, dass der Verantwortliche der Empfehlung des Datenschutzbeauftragten nicht zustimmt, muss in der Dokumentation zur Datenschutz-Folgenabschätzung ausdrücklich schriftlich begründet werden, warum der Empfehlung nicht Folge geleistet wurde (vgl. Art. 24 Abs. 1 DSGVO).

Gemäß Art. 39 Abs. 2 DSGVO trägt der Datenschutzbeauftragte „bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.“ Demnach ist der Datenschutzbeauftragte verpflichtet, seine Aufgaben nach Prioritäten zu ordnen und sich auf Aufgaben zu kon-

zentrieren, von denen größere Bedrohungen für den Datenschutz ausgehen, ohne jedoch weniger risikobehafte Vorgänge zu vernachlässigen.

Dieser Ansatz soll dem Datenschutzbeauftragten dabei helfen, Verantwortliche über die Vorgehensweise bei der Datenschutz-Folgenabschätzung zu beraten, welche internen Schulungsmaßnahmen für Mitarbeiter durchgeführt und welchen Datenverarbeitungsvorgängen mehr Ressourcen zur Verfügung gestellt werden sollten.

4.2. Aufgaben außerhalb des Unternehmens

Nach außen fungiert der Datenschutzbeauftragte als Kontaktperson sowohl für die Aufsichtsbehörde als auch für die Betroffenen.

Die Zusammenarbeit mit den Datenschutzbehörden wird demnach intensiviert, da die im BDSG enthaltene optionale Zusammenarbeit (§ 4g Abs. 1 S. 2, 3 BDSG) nun eine Pflicht wird (Art. 39 Abs. 1 lit. d und e DSGVO). Der Datenschutzbeauftragte ist demnach zentraler Ansprechpartner für die Aufsichtsbehörden und hat die Pflicht, mit diesen zusammen zu arbeiten.

Art. 38 Abs. 4 DSGVO regelt, dass der Datenschutzbeauftragte künftig zentraler Ansprechpartner des Unternehmens gegenüber allen Betroffenen ist. Demnach haben betroffene Personen das Recht, den Datenschutzbeauftragten zu allen Fragen zu Rate zu ziehen, die „mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte“ gemäß DSGVO im Zusammenhang stehen.

Deshalb ist es zwingend, dass der Datenschutzbeauftragte nach außen hin mit Kontaktdaten bekannt gegeben wird. Dieses muss zum

Zeitpunkt der Erhebung personenbezogener Daten geschehen und nicht erst auf Anfrage (Art. 38 Abs. 4 DSGVO im Vgl. mit Art. 13 Abs. 1 DSGVO).

Aus den gennannten Aufgaben außerhalb des Unternehmens ergibt sich zwangsläufig, dass die Kommunikation mit den Betroffenen und der zuständigen Aufsichtsbehörde in deren verwendeten Sprachen erfolgen muss.

5. Haftung des Datenschutzbeauftragten

Dem Datenschutzbeauftragten wird mit der DSGVO ein höherer Stellenwert im Unternehmen beigemessen. Daraus ergeben sich neue Haftungsfragen. Die mögliche persönliche Haftung des Datenschutzbeauftragten bei Nichtbeachtung der Regelungen der DSGVO durch das Unternehmen oder bei Verstößen ist seit der Veröffentlichung der DSGVO ein viel diskutiertes Thema.

Die Artikel 29 Gruppe verdeutlicht in ihrem Leitfaden zwar, dass das Unternehmen (d. h. der Verantwortliche bzw. der Auftragsverarbeiter) selbst für die Einhaltung der DSGVO verantwortlich ist (vgl. Art. 24 Abs. 1 DSGVO), die Haftung des Datenschutzbeauftragten in seinem Verantwortungsbereich für Datenschutzverletzungen bleibt jedoch bestehen. Auch hier wird abzuwarten sein, wie Aufsichtsbehörden und Gerichte den Umfang der Haftung des Datenschutzbeauftragten für begangene Datenschutzverstöße in von ihm betreuten Unternehmen zukünftig bewerten.

Als Ratschlag bleibt deswegen, dass der Datenschutzbeauftragte zukünftig vor allem darauf achten sollte, seine Handlungsempfehlungen zu dokumentieren. Im Streitfall kann er mit Hilfe des Dokumentierten zumindest nachweisen, dass er alles für ihn Mögliche getan hat, um dem Datenschutz Rechnung zu tragen.

Über die activeMind AG

Wir leben in einer Welt der Spezialisierung und Digitalisierung. Durch die Transparenz digitaler Angebote kommen Unternehmen an einer Spezialisierung nicht mehr vorbei. Internet und digitale Systeme sind überall, unsere digitalen Spuren aber auch. Bei der Datensammelwut vieler Staaten und Unternehmen wird der Mensch hinter den Daten oft vergessen. Das Vertrauen in Unternehmen und Mitarbeiter sinkt; gleichzeitig steigen die Sicherheitsanforderungen in Unternehmen.

Seit mehr als 15 Jahren steuern die Gesetzgeber diesen Bereich durch Regelungen wie Datenschutzgesetze und deutlich verschärfte Haftungsregelungen. Landesämter für Datenschutz werden ausgebaut, um flächendeckende Prüfungen der Unternehmen durchzuführen. Werbung neuer Kunden wird durch verschärfte Regelungen immer schwerer.

Der Zwang zur Spezialisierung bei gleichzeitiger Erfüllung der gesetzlichen Anforderungen steht bei mittelständischen Unternehmen im Widerspruch zueinander. Es bestehen meist keine ausreichenden Ressourcen für Datenschutz, IT-Sicherheit oder Qualitätsmanagement. Gesetzlich geforderte Regelungen oder Prozesse sind unbekannt, ethische Werte werden nicht vermittelt. Für Zertifizierungen stehen keine qualifizierten Mitarbeiter zur Verfügung. Im Ergebnis können Sicherheits- und Qualitätsanforderungen größerer Unternehmen nicht erfüllt werden und daher scheiden diese als interessante Auftraggeber aus.

An diesen Punkt setzt die activeMind AG an. Seit dem Jahr 2000 stellen wir für Unternehmen externe Datenschutzbeauftragte, IT-Sicherheitsbeauftragte und Qualitätsmanagementbeauftragte. Je nach Anforderung der Unternehmen erfüllen wir punktuelle Anforderungen oder übernehmen vollständig die Verantwortung bis hin zur Zertifizierung nach internationalen Normen.

In den letzten Jahren haben wir zahlreiche Unternehmen erfolgreich durch ISO 9001, ISO 27001 und BSI-Grundschutz Zertifizierungen geführt. Die Zahl der Unternehmen, bei denen wir als Datenschutz- und IT-Sicherheitsbeauftragte bestellt sind, nimmt jeden Monat zu.

Wir sind Juristen, die mit tiefen IT-Kenntnissen als Auditoren auch bei diversen Prüfstellen wie TÜV, Bundes- und Landesämtern zugelassen sind.

Die Besonderheit unseres Angebotes sind die Pauschalleistungen. Durch monatliche Fixkosten bleiben unseren Kunden hohe Anfangsinvestitionen erspart. Viele unserer Leistungen können zudem durch EU-Fördermittel subventioniert werden. Insgesamt liegen die Kosten für unsere Leistungen oft unter den Mitteln, die für Aus- und Fortbildung eines Mitarbeiters aufzuwenden wären.

Lassen Sie sich jetzt beraten!

E-Mail: anfrage@activemind.de
Web: www.activemind.de

Impressum

activeMind AG
Management und Technologieberatung
V. i. S. d. P.: Klaus Foitzick
foitzick@activemind.de

Potsdamer Straße 3 | 80802 München
Tel.: +49 (0)89 / 418 560 170
www.activemind.de