W+M-Ratgeber: Externer Datenschutzbeauftragter – So kommen Unternehmen ihren Schutzpflichten leichter nach

Die Gesetzgebung schreibt vor, dass Unternehmen abhängig von ihrer Größe und ihrer Tätigkeit einen Datenschutzbeauftragten bestellen müssen. Er überwacht die Einhaltung der DSGVO und weiterer Datenschutzgesetze im Betrieb und arbeitet mit der Aufsichtsbehörde zusammen. Seine Tätigkeiten sind damit weit gespannt, der Beauftragte muss fachlich gut aufgestellt sein. Viele Unternehmen vergeben die Aufgabe intern, was aber nicht immer die beste Lösung darstellt. Denn ein externer Datenschutzbeauftragter ist nicht nur meist kostengünstiger, sondern auch ein Fachmann ohne Interessenskonflikte. **Ein Beitrag von Mario Arndt.**

Wann Unternehmen einen Datenschutzbeauftragten bestellen müssen, ist vom Gesetzgeber im Bundesdatenschutzgesetz (BDSG-neu) und der EU-Datenschutz-Grundverordnung (DSGVO) geregelt. Eine Bestellung ist gemäß § 38 Abs.1 BDSG (ergänzend zu Artikel 37 Abs. 1 lit. b und c der Verordnung (EU) 2016/679 DSGVO) in drei Fällen notwendig: Zum einen, wenn im Unternehmen mindestens 20 Personen regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Erhebt und verarbeitet ein Unternehmen personenbezogene Daten

geschäftsmäßig zum Zweck der Übermittlung oder für Markt- oder Meinungsforschung, muss es unabhängig von seiner Größe ebenfalls einen Datenschutzbeauftragten benennen. Das Gleiche gilt, wenn besonders sensible Daten, etwa zu Gesundheit oder Bonität, verarbeitet werden.

Datenschutz ist umfangreich

Datenschutzbeauftragter ist nun kein geschützter Begriff und oft wird die Aufgabe an interne Mitarbeiter mit einer Affinität zum Thema übertragen. Doch das Aufgabengebiet ist komplex und umfassend: Dazu gehören laut Art. 39 der DSGVO unter anderem die Beratung der Verantwortlichen und die Schulung und Sensibilisierung der Mitarbeitenden, aber auch die Überwachung der Einhaltung von Verschriften oder eine Beratung bzw. Überwachung der Datenschutz-Folgenabschätzung nach Art. 35 DSGVO. Der Datenschutzbeauftragte veranlasst die Erstellung einer internen Verarbeitungsübersicht nach Art. 30 DSGVO und betreut die Auftragsverarbeitung, samt Übersicht der Auftragsverarbeiter, der Erstellung der Verträge und einem Prozess zur Kontrolle der Dienstleister. Außerdem überwacht er die datenschutzgerechte Gestaltung der Technik und sorgt dafür, dass die Informationspflichten bei der Datenerhebung umgesetzt werden. Nicht zuletzt ist er Ansprechpartner für die Aufsichtsbehörde.

Um all diese Aufgaben kompetent erfüllen zu können, benötigt ein Datenschutzbeauftragter Fachwissen und damit juristische Expertise auf dem Gebiet des Datenschutzrechts zum Beispiel zur korrekten Beurteilung der Rechtmäßigkeit der Datenverarbeitung. Er muss sich aber auch in der Datenschutzpraxis auskennen und technisches Wissen mitbringen, um die Verarbeitungsprozesse beurteilen zu können. Daneben muss er organisatorische, pädagogische und kommunikative Fähigkeiten besitzen sowie die Bereitschaft zur steten Weiterbildung, um Gesetzesänderungen und technische Entwicklungen im Blick zu haben.

Die interne Bestellung des Datenschutzbeauftragten ist für Unternehmen nicht per se die beste Wahl. Denn zum einen steht der Mitarbeiter auf der Gehaltsliste und verursacht damit stete Kosten. Zum anderen kann es durchaus zu Interessenskonflikten kommen, etwa wenn er gegen die Interessen der Marketing-Abteilung oder des Vertriebs argumentieren muss. Auch sind seine Erfahrung und Expertise oft nicht ohne Weiteres valide festzustellen. In kleineren Unternehmen wird die Stelle oft besetzt, weil es eben sein muss und die Qualifikation nachrangig ist. Interne Datenschutzbeauftragte sind oft überlastet, da sie die Aufgaben zusätzlich zu ihren normalen Tätigkeiten übernehmen. Hinzu kommt das Risiko eines Ausfalls, etwa bei Krankheit oder während Urlaubszeiten. Und nicht zuletzt trägt das Unternehmen die Kosten für notwendige Weiterbildungen und haftet im Schadensfall mit.

Externer Datenschutzbeauftragter: Die Vorteile

Es empfiehlt sich deswegen die Option eines externen Datenschutzbeauftragten in Betracht zu ziehen, um die Einhaltung der Datenschutzbestimmungen sicherzustellen und gleichzeitig die Kosten des betrieblichen Datenschutzes überschaubar zu halten. Ein guter externer Partner sollte in der Lage sein, ganzheitlich und vollumfänglich zu beraten und einen Full-Service mit vertraglich geregelter Laufzeit anzubieten. Unbedingt abgedeckt werden sollten die Prüfung von Verträgen mit Auftragsverarbeitern, der technischen und organisatorischen Maßnahmen (TOM), Datenschutz-Folgenabschätzungen und Schulungen der Mitarbeitenden. Auch Datenschutzpannen müssen berücksichtigt werden, nur so sind die Kosten kalkulierbar und transparent. In der Praxis zeigt sich, dass sich externe Dienstleister oft als günstiger erweisen. Da Datenschutz ihre Kerntätigkeit ist, bringen sie umfassende fachliche und juristische Expertise mit. Gerade KMU unterhalten oft keine Rechtsabteilung mit Fachkräften in diesem Gebiet. Ein guter externer Datenschützer hat stets einen Überblick über marktübliche Lösungen und Best Practices und verfügt über entsprechende Erfahrung in der Anwendung.

Idealerweise weist der Datenschutz-Partner seinem Kunden-Unternehmen einen festen Ansprechpartner zu, um Probleme auf direktem Weg lösen zu können. Größere Anbieter mit einem Datenschutz-Team haben gegenüber Einzelkämpfern den Vorteil, dass ein Austausch zwischen den Beratern und Fachbereichen stattfindet. Von diesem Mehr an Wissen und dem größeren Netzwerk profitiert am Ende auch der Kunde. Ein größerer Partner kann auch Ausfälle leichter kompensieren und im Falle einer Datenschutzpanne, wenn die Zeit knapp ist, die Verfügbarkeit von Unterstützung garantieren: Ein Vorfall muss innerhalb von 72 Stunden bearbeitet werden. Außerdem kann er die Kommunikation mit Behörden leichter übernehmen und den Spielraum bei der Umsetzung des Datenschutzes zugunsten des Unternehmens aufgrund seiner Erfahrung gezielter nutzen. Auch eine notwendige Mitarbeiterschulung ist von Externen leichter zu leisten.

Mit der Anwendungspflicht der DSGVO im Mai 2018 entstanden viele neue Marktteilnehmer im Bereich der Beratungen und Datenschutzbeauftragten. Unternehmen, die schon länger auf dem Markt sind, verfügen dagegen über mehr Erfahrung. Wichtig ist darüber hinaus eine größenunabhängige und branchenübergreifende Beratung. Zudem muss der Partner in der Lage sein, bedarfs- und anforderungsgerechte, individuelle Audits durchzuführen. Er sollte eine entsprechende Versicherung mitbringen, um bei Schäden die Haftung übernehmen zu können und Compliance, die Beratung nach den gültigen Regeln, sicherstellen. Keine Kleinigkeiten, sondern essenziell, sind die Gewährleistung einer sauberen Dokumentation und die Arbeit mit aktuellen, juristisch geprüften Vorlagen und Checklisten. Und nicht zuletzt verbessert ein externer Datenschutzbeauftragter die Außendarstellung: Er zeigt, dass das Unternehmen das Thema ernst nimmt.

Das Fazit

Viele Unternehmen müssen einen Datenschutzbeauftragten bestellen, der für die korrekte Verarbeitung personenbezogener Daten im Betrieb und damit einhergehenden Tätigkeitsfeldern verantwortlich ist. Ein externer Partner kann den umfangreichen Aufgaben mit breiter Expertise, Erfahrung und entsprechendem Netzwerk oft leichter nachkommen als ein interner Mitarbeiter.

Der Autor: Mario Arndt

Mario Arndt. Foto: Deudat

Mario Arndt ist seit März 2010 Geschäftsführer der DEUDAT® GmbH, einem Spezialisten für Datenschutz und Informationssicherheit mit drei Standorten in Deutschland. Davor war er als Datenschutzbeauftragter für ein mittelständisches Pharma-Unternehmen und als Techniker und Administrator im Bereich der IT-Sicherheit tätig. Arndts Qualifikationen und Mandate sind vielfältig: Er ist ausgebildeter Datenschutzauditor (TÜV), verfügt über Expertise im Informationssicherheitsmanagementsystem (ISMS) und ist ausgebildeter IRCA Lead-Auditor für Managementsysteme nach ISO/IEC 27001 sowie Qualitätsmanagement-Auditor. Für den TÜV Hessen und die ÖHMI EuroCert® GmbH ist Arndt als akkreditierter Leitender Auditor für Managementsysteme nach ISO/IEC 27001 und ISO/IEC TR 27019 tätig. Arndt arbeitete für verschiedenste Branchen wie Energieversorger, Automobil, Banken und IT-Dienstleister.