47. Jahrgang
datenschutz-berater.de
DSB 06/2023

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Laurenz Strassemeyer
Rechtsunklarheit kurz vor der Einschulung der DSGVO Seite 157

Stichwort des Monats

Dr. Gregor Scheja
Externe Ombudsperson als „interne" Meldestelle nach HinSchG im Rahmen einer Auftragsverarbeitung? Seite 158

Datenschutz im Fokus

Dr. Simon Assion
Das neue deutsche Gesetz über Massenschadensersatzklagen und sein Bezug zum Datenschutzrecht Seite 164

Dr. Dominik Nikol und Johannes Rost
„Pay or okay" – okay or not okay? Aktuelle Entwicklungen bei den sog. Pur-Modellen Seite 167

Anna Cardillo, Guido Hansch, Wolfgang Lehna und Heiko Markus Roth
Koordinierte Prüfung zu Stellung und Aufgaben von Datenschutzbeauftragten Seite 172

Rechtsprechung

Patrick Zeitvogel und Alexandra Rath
EuGH vertritt weiten Kopie-Begriff der DSGVO: Ein Überblick über Gründe und Auswirkungen Seite 175

Prof. Dr. Alexander Golland
Formelle DSGVO-Verstöße wirken sich nicht auf Rechtmäßigkeit der Verarbeitung aus Seite 178

Christoph Engling
EuGH zu (immateriellem) Schadensersatz: Bloßer Verstoß gegen DSGVO nicht ausreichend Seite 181

- **Nachrichten** Seite 160

ISSN 0170-7256

dfv Mediengruppe

Anna Cardillo, Guido Hansch, Wolfgang Lehna und Heiko Markus Roth

Koordinierte Prüfung zu Stellung und Aufgaben von Datenschutzbeauftragten

Der Beitrag ist der zweite seiner Art und knüpft an jenen in der Ausgabe 05/2023 an und widmet sich den Inhalten des Fragebogens des Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA), der im Rahmen der laufenden Coordinated-Enforcement-Framework-Prüfaktion in Bayern versendet wurde.

Einstieg

Ein kurzer Hinweis: Anders als es die Pressemitteilung des BayLDA auf dem ersten Blick vermuten lässt, wurden nicht 36.000 Organisationen mit dem Fragebogen adressiert, sondern nur 30. Der Fragebogen besteht aus 40 Fragen. Jede Aufsichtsbehörde (ASB) kann bei der Auswahl der Adressaten, bei der Gestaltung des Fragebogens und bei der Pflicht und Durchsetzung der Beantwortung eigene Akzente setzen (Art. 52 Abs. 1 DSGVO). Eine Übersicht dazu liefert die Confederation of European Data Protection Organisations (https://cedpo.eu/wp-content/uploads/CEDPO-1205-CEF-Questionnaire-gd-v20.pdf, 19.05.2023, Seite 2 f.).

Profilmerkmale

Fragen und Vorgabe der DSGVO

Die Fragen 1 bis 11, 31 und 32 knüpfen an die Vorgaben in Artt. 37 Abs. 5, 38. Abs. 2, Abs. 3 Satz 1 und Satz 2, 39 DSGVO an.

Einordnung und Bewertung der Fragen

Die obigen Fragen befassen sich mit der Geeignetheit und Unabhängigkeit des Datenschutzbeauftragten (DSB). Art. 37 Abs. 5 DSGVO setzt die berufliche Qualifikation und insbesondere das Fachwissen des DSB auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis voraus (BvD, Orientierung: Das berufliche Leitbild der Datenschutzbeauftragten). Die DSGVO fordert jedoch keine bestimmte berufliche Ausbildung oder näher konkretisierte Fachkenntnisse. Die Art. 29-Gruppe fordert im WP 243 rev.01, 5.4.2017 recht vage „Erfahrung sowohl im einzelstaatlichen als auch im europäischen Datenschutzrecht und in der diesbezüglichen Praxis". Daneben wird ein umfassendes Verständnis der DSGVO, Branchenkenntnis, Vertrautheit mit der Organisationsstruktur, ein gutes Verständnis der durchgeführten Datenverarbeitungsvorgänge, der betreffenden Informationssysteme sowie der Datensicherheits- und Datenschutzerfordernisse vorausgesetzt. Je nach Organisationsstruktur und Unternehmenskultur wird es auch auf weitere Fähigkeiten und Kenntnisse ankommen. Führungskompetenzen wie Mitarbeiterführungs-, Beziehungs- und Veränderungskompetenzen sind mindestens genauso wichtig wie juristische und technisch-organisatorische Kompetenzen. Nicht unerwähnt bleiben soll die Persönlichkeitskompetenz, wozu eigene Stabilität, Integrität, Mut, Rollenbewusstsein, aber auch Rollenübernahmefähigkeit zählen.

Der DSB muss zudem zur Erfüllung der in Art. 39 DSGVO genannten Aufgaben fähig, also geeignet und in der Lage sein, die sie benennende Stelle und deren Beschäftigte hinsichtlich ihrer Pflichten zu unterrichten und zu beraten. Dies bedeutet zunächst, dass er über Fachwissen zu den gebotenen Datenschutzverfahren und -prozessen wie Datenschutz-Folgenabschätzungen, Betroffenenrechte und Meldung von Datenpannen verfügt. Kenntnisse im Projektmanagement, im Riskmanagement, zu Grundlagen der Vorbereitung, Durchführung und Nachbereitung eines Audits sowie zu Managementsystemen sind unverzichtbar. Gelten für den Verantwortlichen bereichsspezifische Datenschutzvorschriften (z. B. aus dem Sozialgesetzbuch), muss der DSB auch diese Regelungen kennen und anwenden können. Um die in Art. 39 DSGVO beschriebenen Aufgaben erfüllen zu können, wird es auch auf die vorstehend beschriebenen Führungskompetenzen ankommen, die zwingend mit Kommunikationsstärke und Durchsetzungsfähigkeit einhergehen. ErwGr. 97 zur DSGVO beschreibt ferner, dass das erforderliche Niveau des Fachwissens sich insbesondere nach den durchgeführten Verarbeitungsvorgängen und dem erforderlichen Schutz für die verarbeiteten personenbezogenen Daten richten solle. Je schutzbedürftiger die Daten sind, desto höhere Anforderungen sind an die Qualifikation und Fachkunde des DSB (Fragen 7 und 8) zu stellen. Die Fragen 1 und 3 aus dem Fragebogen zielen offensichtlich auf die Sensibilität der verarbeiteten Daten sowie Komplexität und Risiken der Datenverarbeitungen ab. Schon vorab werden Angaben zu Größe, Struktur sowie Branche und Sektor des Unternehmens abgefragt. Die Angaben zur Qualifikation des DSB sollten – ebenso die vom DSB leistbaren Stunden (Frage 4) – damit im Einklang stehen.

Die Frage 6 knüpft weniger an die Qualifikation des DSB, sondern vielmehr an die Zuordnung seiner Funktion zu einer bestimmten Abteilung an. Hier können sich Interessenskonflikte und Beeinträchtigungen der Unabhängigkeit zeigen (siehe noch unten). Aufgelistet sind vor allem Negativbeispiele. Idealerweise ist der DSB einem eigenen Be-

reich „Datenschutz“ zugeordnet und nur dem Management unterstellt.

Soweit sich Fragen mit 9 und 10 mit der Anzahl von Jahren der „Erfahrungen“ beschäftigen, so fehlt es zum einen an einer weiteren Unterteilung nach Teil- oder Vollzeit, zum anderen stellt sich die Frage, inwieweit Erfahrungen überhaupt in Jahren messbar sind.

Fragen 5, 31 und 32 haben die in Art. 38 Abs. 3 DSGVO geforderte Unabhängigkeit des DSB im Fokus. Art. 38 Abs. 3 Satz 1 DSGVO normiert die Weisungsfreiheit des DSB. Verantwortliche und Auftragsverarbeiter haben sicherzustellen, dass der DSB bei der der Erfüllung seiner Aufgaben keinen Anweisungen bezüglich der Ausübung dieser Aufgaben unterworfen wird.

Art. 38 DSGVO sieht keine Mindest-Amtszeit für den DSB vor, sodass eine Befristung nicht per se unzulässig ist. Eine zu kurze Befristung könnte jedoch die Wahrnehmung der Pflichten und Aufgaben durch den DSB vereiteln, da zum einen eine zu kurze Zeit weder eine vernünftige Einarbeitung noch ein sinnvolles Wirken ermöglicht, zum anderen der DSB um die Fortsetzung des Vertragsverhältnisses fürchten müsste, was seine Unabhängigkeit beeinträchtigte (vgl. BvD, Positionspapier: Benennung von Datenschutzbeauftragten – Unabhängigkeit nur mit Bindung für die Ewigkeit möglich?). Bei der Festlegung der Befristung sollten daher Größe, Strukturen und Branche des Unternehmens sowie die Komplexität und Art und Weise der Datenverarbeitungen berücksichtigt werden. Art. 38 Abs. 3 Satz 2 DSGVO verbietet die Abberufung des Datenschutzbeauftragung wegen der Erfüllung seiner Aufgaben. Er soll also nicht entlassen werden können, weil er zu „unbequem“ wird. Die Vorschrift schützt den DSB auch vor sonstiger Benachteiligung (z. B. Versagung von Urlaub, Beförderung, Weiterentwicklungsmaßnahmen).

Frage 11 befasst sich mit der in Art. 38 Abs. 2 DSGVO normierten Pflicht der Verantwortlichen, dem DSB die zur Erhaltung des Fachwissens erforderlichen Ressourcen zur Verfügung zu stellen. Auch diesbezüglich wird es bei der Beurteilung der Angemessenheit der zur Verfügung gestellten Ressourcen auf Größe, Strukturen und Branche des Unternehmens sowie die Sensibilität der verarbeiteten Daten, die Komplexität und Art und Weise der Datenverarbeitungen ankommen. Unklar bleibt, ob die Fragestellung sich lediglich auf Fortbildungsangebote Dritter bezieht oder auch zeitliche Ressourcen für das Eigenstudium, den Austausch in Peergroups, fachbezogene Aktivität in sozialen Netzwerken wie Twitter und LinkedIn („TeamDatenschutz“), kostenfrei abrufbare Webinare oder Aufzeichnungen von Fachbeiträgen berücksichtigt werden können. Längst ist die Teilnahme an klassischen (kostenpflichtigen) Fortbildungsangeboten von Seminarveranstaltern, die in der Regel langfristig vorbereitet werden müssen, nicht mehr das Mittel der Wahl. Zu dynamisch sind die Entwicklungen im Datenschutzrecht. Sehr schnell sind Fachbeiträge – ob Text, Podcast, Video – zu aktuellen Themen verfügbar. Will der DSB am Ball bleiben, bleibt ihm nichts anderes übrig, als sich kontinuierlich über diverse Kanäle zu informieren, ohne dass es Teilnahmebestätigungen gäbe. Verantwortliche werden bei der Ermittlung dieser Zeiten auf entsprechende Informationen ihrer DSBen angewiesen sein. Diese wiederum sollten ihren Zeitaufwand für Wissensaufbau – und Erhalt zumindest ungefähr erfassen und z. B. in ihren Tätigkeitsberichten dem Verantwortlichen nebst Beschreibung übermitteln. Schließlich ermöglicht eine Zeiterfassung der Wissenserhaltung dem DSB auch eine Beurteilung darüber, ob die ihm bereitgestellten finanziellen und zeitlichen Ressourcen ausreichen.

Fortbildung, personelle Aufstellung, Budget, Zusatzaufgaben, Interessenkonflikt

Fragen und Vorgabe der DSGVO

Die Fragen 11, 17-24 knüpfen an die Vorgaben in Art. 38 Abs. 2, 6 DSGVO an.

Einordnung und Bewertung der Fragen

Nach Art. 38 Abs. 2 DSGVO „unterstützen“ Verantwortliche und Auftragsverarbeiter den DSB bei der Erfüllung seiner Aufgaben. Dazu müssen die für die Erfüllung dieser Aufgaben „erforderlichen“ Ressourcen zur Verfügung gestellt werden.

Genauso wenig wie die DSGVO „messbare“ Vorgaben dazu liefert, so existiert, soweit den Autoren bekannt, auch keine aussagekräftige oder gar amtliche Empirie, die Anhaltspunkte für ein zahlenmäßig bezifferbares und zugleich organisationsunabhängig ableitbares Minimum an Fortbildungen, Vollzeitäquivalente oder Budget des DSB geben könnte. Dreh- und Angelpunkt ist die Bestimmung der „Erforderlichkeit“ (Art. 38 Abs. 2 DSGVO).

Die Kontrollfrage lautet: Sind die einzelnen dem DSB zugeordneten sachlichen, zeitlichen, finanziellen und personellen Ressourcen so ausgebaut, dass der DSB damit seine Aufgaben in der Organisation lückenlos erfüllen kann und in seiner Unabhängigkeit nicht verletzt wird? Wenn der DSB nach Art. 38 Abs. 3 Satz 3 DSGVO regelhaft Bericht erstattet, der Reifegrad der Prozesse der eigenen Datenschutzorganisation sowie die Risikoneigung der einzelnen Verarbeitungen bekannt sind, sollte die Beantwortung nicht schwerfallen. Ob die zugewiesenen Ressourcen „erforderlich“ sind, kann sich im Zeitverlauf ändern und muss regelmäßig überprüft werden. Anlässe zur Neubewertung sind bspw. neue Geschäftsmodelle, Gesellschaften und Digitalrechtsakte.

Zum „Stellvertreter“: Die DSGVO sieht keine Pflicht des Verantwortlichen und Auftragsverarbeiters vor, einen „Ver-

treter“ für den DSB zu benennen. ErwGr. 97 zur DSGVO spricht in bestimmten Fällen von einer „weiteren Person“. Im öffentlichen Bereich haben einzelne Bundesländer die Rolle eines Vertreters geschaffen. Ein Beispiel hierfür ist § 4 Abs. 3 Satz 1 BlnDSG, nach dessen Gesetzesbegründung sehe Kapitel 4 der DSGVO eine solche Rolle zwar nicht vor, schließe sie aber auch nicht aus. Ein Vertreter gewährleiste die Aufgabenerfüllung auch in Abwesenheit des DSB (AH Berlin, Drs. 18/1033, S. 74). Zur Kontinuität der Kontrollfunktion empfiehlt sich auch für den nicht-öffentlichen Bereich die Benennung eines Stellvertreters.

Es folgen einzelne, nicht abschließende „Negativ-Beispiele“. Sie zeigen nach Ansicht der Autoren anhand offensichtlicher Fälle, welche Maßnahmen nicht genügen, um Art. 38 Abs. 2 DSGVO zu erfüllen.

- Über Fortbildungsanträge des internen DSB entscheidet nicht die höchste Managementebene. Abwandlung: Diesem DSB wird eine Fortbildung zur juristischen Bewertung besonders umfassender und risikoreicher Verarbeitungen des Verantwortlichen verwehrt. Die Fortbildung hätte den aktuellen Diskussions- und Wissensstand in der Branche in konzentrierter Form vermittelt. Neben seinen übrigen, eng getakteten Aufgaben und Terminen mit Prozessverantwortlichen bleiben dem internen DSB keine Zeiträume, sich so effizient selbst auf diesen Stand zu bringen.
- Ein Verantwortlicher benennt für eine Gesellschaft mit mehreren tausend Beschäftigten sowie mit Betriebsstätten in mehreren Ländern einen internen DSB. In der Aufbauorganisation fehlt es an einer Rolle, die den DSB im Rahmen seiner Aufgaben unterstützt. Die Beauftragung eines Dritten zur Bewertung einer spezifischen Rechtsfrage, die die Gesellschaft nicht selbst beantworten kann, wird abgelehnt. Der Austausch mit anderen DSBen, z. B. über Erfa-Kreise, wird verweigert. Dienstreisen zu den Betriebsstätten werden untersagt.

Nach Art. 38 Abs. 6 DSGVO „kann“ der DSB „andere Aufgaben und Pflichten“ wahrnehmen, also grundsätzlich auch als Teilzeit-DSB tätig sein. Es gibt jedoch eine Einschränkung. Der Verantwortliche und der Auftragsverarbeiter müssen sicherstellen, dass solche Aufgaben nicht zu einem „Interessenkonflikt“ führen (Kontrollpflicht vs. Implementierungsverantwortung). Dem DSB dürfen „keine Aufgaben oder Pflichten übertragen werden (…), die ihn dazu veranlassen würden, die Zwecke und Mittel der Verarbeitung personenbezogener Daten (…) festzulegen“. Der Verantwortliche oder Auftragsverarbeiter muss im Einzelfall, insbesondere unter Berücksichtigung der Organisationsstruktur und interner Anweisungen, feststellen, ob ein Interessenkonflikt tatsächlich vorliegt (EuGH, Urt. v. 9.2.2023 – C-453/21, Rn. 44-45). Beispiele für (potenzielle) Konflikte, die seitens der ASB thematisiert wurden, sind die Folgenden:

- DSB als Geschäftsführer von zwei Dienstleistungsgesellschaften, die im Auftrag der den DSB benennenden Organisation als Auftragsverarbeiter tätig sind (BlnBDI, Pressemitteilung v. 20.9.22).
- DSB als Rechtsbeistand der Organisation vor Gericht (GPDP, 9.6.22, Entscheidung 9794895); DSB als Leiter des Operativen Risikomanagements, des Informationsrisikomanagements, der Sonderermittlungsgruppe (APD/GBA, 16.12.21, Entscheidung 141/2021); DSB als Leiter der Abteilung Compliance, Geldwäsche-Meldebeauftragter (CNPD, 13.10.21, Entscheidung n°37FR/2021); DSB als Direktor für Audit, Risiko und Compliance (APD/GBA, 28.4.20, Entscheidung 18/2020); DSB als „Privacy Officer“ (AP, Pressemitteilung vom 8.5.23, Entscheidung steht noch aus).

Fazit

Der durch die ASB genutzte Fragebogen zur Stellung und zur Rolle vom DSB ist anspruchsvoll und birgt Fallstricke. Nicht zuletzt wegen der sich häufenden Entscheidungen einzelner Behörden zur Konturierung der Artt. 37 ff. DSGVO sollte bei der Beantwortung ein waches Auge walten.

Autoren: **Anna Cardillo ist Rechtsanwältin bei Spirit Legal und zudem als Datenschutz-Auditorin sowie externe DSB tätig.**

Guido Hansch, LL. M. und CIPP/E, ist Legal Counsel und Group Data Protection Officer bei der codecentric AG in Solingen.

Dipl.-Jur. Wolfgang Lehna, CIPP/E, CIPM, FIP (IAPP) ist Konzern-DSB bei der SAMSON GROUP.

Heiko Markus Roth, LL. M., ist interner DSB im Konzernumfeld.

Der Beitrag spiegelt die private Meinung der Autoren wider.