www.datenschutz-praxis.de

Datenschutz PRAXIS

Rechtssicher | vollständig | dauerhaft

Oktober 2023

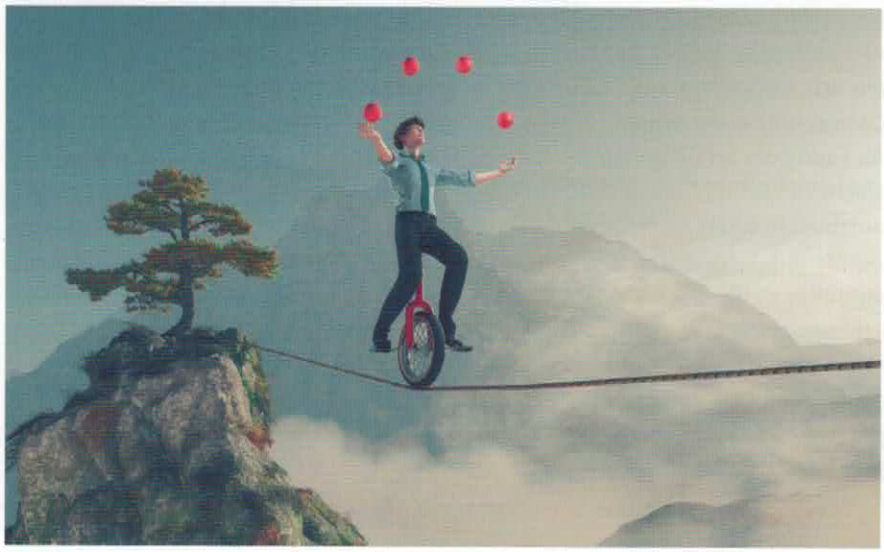

Bild: iStock.com/Orla

Die Weiterentwicklung und Ausdifferenzierung der Rolle von DSB ist noch nicht bei allen Akteuren angekommen. Das allein erzeugt schon ausreichend Potenzial für Spannungen.

DSB-Aufgaben & unternehmerische Realität

Spannungsfall(e) Datenschutzbeauftragte

DSB sehen sich heute mehr denn je in einem Konflikt zwischen ihren Aufgaben, die sich aus Art. 37 ff. DSGVO und § 5 bis 7 BDSG ergeben, und dem, was Unternehmen gern als „pragmatische Umsetzung" adressieren. Wo liegen die Hauptgründe dafür und was lässt sich dagegen tun?

Die Ursachen für das Spannungsfeld, in dem sich viele Datenschutzbeauftragte (DSB) wiederfinden, liegen oftmals im falschen Verständnis der Berichtslinie, in positionsbedingten Interessenkonflikten und in der unreflektierten Aufgabenzuweisung. Aber es resultiert teils auch daraus, dass es für beide Seiten schwierig ist, sich vom alten Berufsbild zu lösen. Noch komplizierter wird es, sobald DSB weitere Pflichten oder Aufgaben wahrnehmen sollen.

Die EU-weite koordinierte Prüfung zu Stellung und Aufgaben von Datenschutzbeauftragten, an der sich in Deutschland nur das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) beteiligte (siehe hierzu Marschall, Datenschutz PRAXIS 09/2023, S. 01), gibt zusätzlich Anlass, dieses Spannungsfeld zu thematisieren und zu analysieren. Und mitnichten geht alle Spannung nur vom Unternehmen aus.

Falle 1: keine direkte Berichtslinie an die Unternehmensleitung

Der Grundsatz der unmittelbaren Berichterstattung an die höchste Managementebene ist in Art. 38 Abs. 3 Satz 3 Datenschutz-Grundverordnung (DSGVO) unmissverständlich verankert. Vor diesem Hintergrund verwundert die Praxis und damit auch Risikobereitschaft mancher Unternehmen, den Datenschutzbeauftragten teilweise mehrere Ebenen tiefer zu „vergraben".

Zumal angesichts der Tatsache, dass das BayLDA in seiner Pressemitteilung vom 15. März 2023 anlässlich der gemeinsamen Prüfaktion deutliche Worte fand: „Auf Grundlage unserer Prüfbefugnisse werden wir die Handlungsbedingungen der betrieblichen Datenschutzbeauftragten gezielt in den Blick nehmen und uns sowohl Organigramme als auch Jah- →

Editorial

Ricarda Veidt,
Chefredakteurin

Datenschutz in der Schule

Liebe Leserin, lieber Leser! Nachdem nun auch in den südlichen Bundesländern endgültig die Ferien vorbei sind, stellt sich wieder verstärkt die Frage nach dem Datenschutz in der Schule. Gleich, ob aus Sicht der Eltern, der Schülerinnen und Schüler oder aus Sicht von Lehrkräften und beratenden Datenschutzbeauftragten.

Die Aufsichtsbehörden stellen zu diesem Thema eine ganze Menge an Informationen zur Verfügung. Auf der Website des Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz z.B. findet sich eine umfangreiche FAQ-Liste für Lehrkräfte und DSB an Schulen (https://ogy.de/datenschutz-rlp-faq-schule). Sachsen-Anhalt bietet ein „Infopaket Schule und Kita" an (https://ogy.de/infopaket-schule-kita).

Und ganz aktuell hat der Bayerische Landesbeauftragte für den Datenschutz Arbeitshilfen zum Datenschutz bei Schülerunterlagen sowie zu Foto- und Videoaufnahmen in der Schule veröffentlicht (https://ogy.de/baylfd-datenschutz-schule; hier nach den genannten Dokumenten suchen).

Einen guten (Schul-)Start allen
Ihre Ricarda Veidt

resberichte der Datenschutzbeauftragten vorlegen lassen. Wir werden sehr genau hinterfragen, wie Datenschutzbeauftragte, die nur über eine sog. dotted line über verschiedene Hierarchieebenen hinweg an die Unternehmensleitung herantreten können, dem Erfordernis jederzeitiger unmittelbarer Berichtsrechte genügen, um so ein klares Bild zur Situation der Datenschutzorganisation zu vermitteln und Fehlentwicklungen entgegenzutreten."

Die Botschaft, dass das Recht von Datenschutzbeauftragten auf unmittelbaren Zugang zur Ebene der Geschäftsführung oder der Vorstände weder durch die Zwischenschaltung noch durch die Delegation auf eine untere Managementebene eingeschränkt werden darf, ist klar.

Gesprächen mit Datenschutzbeauftragten, die nicht direkt dem obersten Management berichten, lässt sich immer wieder entnehmen, dass diese gut daran tun, sich mit ihren Führungskräften abzustimmen, bevor sie kritische Entwicklungen dem Vorstand oder der Geschäftsführung vortragen. Im Ergebnis kann das zu „gefilterten" Botschaften führen.

Tatsächlich aber müssen Datenschutzbeauftragte sich eigeninitiativ direkt an die oberste Managementebene wenden können, um z.B. datenschutzrechtliche Risiken, fehlende Ressourcen, Vorschläge zur Verbesserung technischer und organisatorischer Maßnahmen oder Prozessanpassungen zu adressieren, ohne dass zwischengeschaltete Führungskräfte oder divergierende Bestrebungen von Fachabteilungen dies beeinträchtigen.

Falle 2: hausgemachte Interessenkonflikte

Unter der DSGVO haben DSB Überwachungs- und Kontrollaufgaben. Sie können zusätzliche Aufgaben nur dann übernehmen, wenn diese hiermit nicht in Interessenkonflikt geraten (Art. 38 Abs. 6 DSGVO).

Die jüngste Entscheidung des Europäischen Gerichtshofs (EuGH) zur Personalunion mit dem Betriebsratsvorsitzenden (C453/21) hat verdeutlicht, wo die Grenzen dieser Interessenkonflikte auszumachen sind. Randnummer 46 konkretisiert, „dass ein ‚Interessenkonflikt' im Sinne dieser Bestimmung bestehen kann, wenn einem Datenschutzbeauftragten andere Aufgaben oder Pflichten übertragen werden, die ihn dazu veranlassen würden, die Zwecke und Mittel der Verarbeitung personenbezogener Daten bei dem Verantwortlichen oder seinem Auftragsverarbeiter festzulegen."

Im 51. Tätigkeitsbericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit (HBDI) findet sich dazu folgende Beschreibung: „Kontrolliert eine Person unterhalb der Geschäftsleitung aufgrund ihrer Funktion oder Verantwortlichkeit bereits den Inhalt und den Umfang der Verarbeitung personenbezogener Daten, kann sie zur Überwachung ihrer eigenen Funktion nicht eingesetzt werden." (siehe https://ogy.de/tb-hessen-2022).

Ergänzend gibt der HBDI Beispiele für Zusatzfunktionen von DSB, die einen Interessenkonflikt begründen:

- Leitungsverantwortung innerhalb der IT-, Marketing- oder Vertriebsabteilung
- IT-Sicherheitsbeauftragte
- Geldwäsche- und Antikorruptionsbeauftragte

Das BayLDA benennt in seiner oben erwähnten Pressemitteilung als Beispiele

- Compliance-Beauftragte und
- IT- bzw. Personalverantwortliche.

Aktuell ergeben sich zudem Fragen bei der Zuweisung der Aufgabe des Meldestellenbeauftragten nach dem Hinweisgeberschutzgesetz. Aus dem Beitrag „DSB & interner Meldestellenbeauftragter – ein Widerspruch?" (Fehr, Datenschutz PRAXIS 09/2023, S. 18, abrufbar unter https://ogy.de/dp-dsb-hinschg) entsteht jedoch ein klares Bild der Dos and Don'ts in Bezug auf Zusatzfunktionen.

Falle 3: unreflektierte Aufgabenzuweisung – Berater & Überwacher statt Kümmerer

War im BDSG nach alter Fassung (a.F.) der Datenschutzbeauftragte „Kümmerer" in Sachen Datenschutz, so kommt ihm heute die Rolle des Beraters und Überwachers zu.

Selbst schulen – ein Kann, kein Muss

Die Weiterentwicklung und Ausdifferenzierung der Rolle des Datenschutzbeauftragten ist augenscheinlich noch nicht bei allen Akteuren angekommen. Das an sich erzeugt schon ausreichend Potenzial für Spannungen. Wo er früher höchstpersönlich die Aufgabe hatte, die Beschäftigten mit dem Datenschutz vertraut zu machen, muss er heute überwachen, dass das Unternehmen klare Zuständigkeiten und nachweisbare Sensibilisierungsmaßnahmen etabliert hat.

Die Erwartung, dass der DSB jede Schulung selbst hält, ist nicht mehr zeitgemäß. Gleichwohl kann das – soweit von den Ressourcen, die zur Verfügung stehen, vertretbar – eine zusätzliche Aufgabe ein

DSB geben keine Verarbeitungstätigkeiten frei

Auch wurde das sogenannte Hinwirken früher oft als einzelfallbezogenes Begleiten der Beschäftigten und ihrer Verarbeitungstätigkeiten mit einer Freigabe als Ergebnis verstanden und fokussierte sich in der Regel auf Datenverarbeitungsprogramme. All das findet man heute noch wieder, wenn man in Verzeichnisse von Verarbeitungstätigkeiten (VVT) blickt, die im Grunde eine Aufstellung der IT-Systeme mit untergeordneten Verarbeitungen sind statt ein VVT nach Art. 30 DSGVO.

Eine Freigabe von Verarbeitungstätigkeiten oder IT-Systemen durch den Datenschutzbeauftragten ist mit seiner Kontrollfunktion nicht vereinbar und erzeugt eine massive Verantwortungsdiffusion. Auf diese Weise verlagert sich die Verantwortung für die Rechtskonformität einer Datenverarbeitung (vermeintlich) auf den Datenschutzbeauftragten. Interessenkonflikte sind damit vorprogrammiert.

WICHTIG

Der Datenschutzbeauftragte überwacht und überprüft Verarbeitungen, die personenbezogene Daten enthalten, entweder selbst oder mittels prüffähiger Prozesse und Ressourcen, die der Verantwortliche ihm bereitstellt. Er erteilt für diese aber keine Freigabe. Eine Freigabe muss in Ansehung u.a. datenschutzrechtlicher Risiken der Verantwortliche (Prozesseigentümer oder -eigentümerin) fällen und vertreten. Diese feine Trennlinie zwischen Prüfung/Bewertung und Freigabe zu ziehen, zu erklären, zu vertreten und zu verteidigen, ist für den Datenschutzbeauftragten entscheidend, um die eigene Unabhängigkeit zu wahren.

DSB führen kein VVT – aber überwachen die Eintragungen

Auch das Führen des Verzeichnisses von Verarbeitungstätigkeiten wird zumeist beim Datenschutzbeauftragten verortet sein. Hier können falsche Erwartungen entstehen, wenn nicht klargestellt ist, was darunter zu verstehen ist. Sicherlich kann und soll der Datenschutzbeauftragte wie auch seine Mitarbeiter und Mitar- →

DSB nach BDSG a.F.	DSB nach DSGVO
Hinwirkung auf Datenschutz (§ 4g Abs. 1 BDSG a.F.)	Unterrichtung des Verantwortlichen/der Beschäftigten (Art. 39 Abs. 1 Buchst. a DSGVO)
Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden (§ 4f Abs. 5 BDSG a.F.).	Betroffene Personen können den DSB zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen (Art. 38 Abs. 4 DSGVO).
Überwachen der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme (§ 4g Abs. 1 Nr. 1 BDSG a.F.)	Überwachung der Einhaltung dieser Verordnung (Art. 39 Abs. 1 Buchst. a DSGVO)
Personen mit Datenschutz vertraut machen (§ 4g Abs. 1 Nr. 2 BDSG a.F.)	Überwachung der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der Mitarbeiter und der diesbezüglichen Überprüfungen (Art. 39 Abs. 1 Buchst. b DSGVO)
Zuständig für die Vorabkontrolle (Freigabe von Datenverarbeitungen; § 4d Abs. 6 BDSG a.F.)	Beratung – auf Anfrage – bei Datenschutz-Folgenabschätzungen (Art. 39 Abs. 1 Buchst. c DSGVO)
Keine Entsprechung unter BDSG a.F.	DSB muss frei von Interessenkonflikten und risikoorientiert agieren (Art. 38 Abs. 6, 39 Abs. 2 DSGVO).

Aufgaben im Licht des Wandels vom Bundesdatenschutzgesetz (BDSG) in der alten Fassung zur DSGVO

beiterinnen die Einträge dort nicht selbst vornehmen. Denn dadurch würde wieder die Verantwortungsdiffusion entstehen.

Das lässt sich vermeiden, indem im Rahmen eines definierten Verfahrens der DSB überwacht, dass Informationen zu Verarbeitungstätigkeiten, die man ihm vorträgt, in das VVT eingetragen werden (Art. 39 Abs. 1 DSGVO). Der Datenschutzbeauftragte ergänzt diese dann um einen Prüfvermerk zu Plausibilität, Vollständigkeit und Risikobewertung. Er fordert zudem beim Verarbeitungsverantwortlichen Aktualisierungsprüfungen ein, und zwar in Zeitintervallen, die sich aus der Datenschutzrichtlinie ergeben.

DSB sollten allerdings keinesfalls die Verantwortung für das technische System, die Rechte- und Rollenverwaltung oder das Backup des VVT haben. Das würde im schlimmsten Fall, etwa bei einem Totalausfall und fehlendem Backup, unerfreuliche Fragen nach der Verantwortung aufwerfen.

Zusammengefasst: 6 zentrale Empfehlungen

Insgesamt ist festzustellen, dass ein Großteil an Spannungselementen durch indirekte Berichtslinien, unzureichende Festlegung der Aufgaben des Datenschutzbeauftragten und fehlende Abgrenzungen hinsichtlich dessen, was gerade nicht seine Aufgabe sein wird, entsteht. Das lässt sich durch folgende Maßnahmen vermeiden:

1. Die Berichtslinie, Berichtswege (Jahresbericht, regelmäßige Besprechungen, Stellungnahmen) und Aufgaben des Datenschutzbeauftragten sollten grundsätzlich schriftlich in einer Stellen- bzw. Aufgabenbeschreibung bzw. bei einem externen DSB in dessen Beauftragung beschrieben sein.
2. Zusätzliche Aufgaben sind dabei klar und eindeutig gegenüber den gesetzlichen Pflichten des Datenschutzbeauftragten abgegrenzt.
3. In diesem Rahmen gilt es, auch wesentliche Unterschiede darzulegen. Es fällt etwa die gesetzliche Privilegierung weg. Zudem greifen für diese zusätzlichen Aufgaben weder die Unabhängigkeit noch die Weisungsfreiheit.
4. Ebenso sollten die Aufgaben des DSB klar und eindeutig gegenüber denen der Fachbereiche bzw. anderer Unternehmensfunktionen (z.B. IT, Interne Revision, Rechtsabteilung, Compliance) abgegrenzt werden.
5. Die Aufgabenbeschreibung sollte idealerweise mit einer Festlegung des Budgets verknüpft sein (siehe oben) sowie einer regelmäßigen Prüfung und ggf. Anpassung unterliegen.
6. Ein Organigramm und eine im Intranet veröffentlichte Aufgabenbeschreibung sollten die wesentlichen Punkte dieser Vereinbarung für alle Beschäftigten verfügbar machen.

Fazit: DSB sind keine „Kümmerer für den Datenschutz" mehr

Datenschutzbeauftragte unter der DSGVO sind Manager und Managerinnen, Strateginnen und Strategen, risikoorientierte Prüferinnen und Prüfer. Sie sollten den Aufbau und die Führung einer operationalisierten Datenschutzorganisation betreiben, die unternehmensinternen Strategien unter Berücksichtigung der Rechtsentwicklung begleiten, durch nachvollziehbare Prüfaktionen mit klar kommunizierten Ergebnissen und praxisnahen Handlungsempfehlungen arbeiten – mit der klaren Zielsetzung, Datenschutz-Compliance messbar und so die Entwicklung des Unternehmens sichtbar sowie für den Verantwortlichen nachvollziehbar zu machen.

Fünf Jahre nach Geltungsbeginn der DSGVO ist es allerhöchste Zeit, alte Traditionen abzulegen und Aufgaben sowie Stellung der Datenschutzbeauftragten nach diesem Leitbild auszurichten. Das bedeutet auch, heute nicht mehr verträgliche Vorstellungen vom Kümmerer für den Datenschutz hinter sich zu lassen.

Daniela Will moderiert vom 07. bis zum 08. November gemeinsam mit Dr. Eugen Ehmann wieder den großen Datenschutz-Kongress IDACON in München. Programm und Anmeldung finden sich unter www.idacon.de.

Persönliches und allgemeines Budget

Das Budget von Datenschutzbeauftragten

Eng verknüpft mit der Anschaffung einer Software für das VVT ist die Frage nach dem Budget, das allein der DSB zu seiner Verfügung hat. Es muss im angemessenen Verhältnis zu seinen Aufgaben stehen. Darin sollten folgende Posten enthalten sein:

- Weiterbildung des Datenschutzbeauftragten und seines Teams
- Verbandsmitgliedschaften, Wissensportale, Fachzeitschriften
- Reisekosten
- Maßnahmen für eigene Sensibilisierungskampagnen
- ggf. Beauftragung externer technischer Prüferinnen und Prüfer sowie datenschutzrechtlicher Beratung

Nicht im Budget des DSB, aber als Bestandteil eines allgemeinen Datenschutzbudgets sollten diese Positionen Berücksichtigung finden:

- Tool für ein Datenschutzmanagement-System (Evaluierung/Anschaffung/Einführung/Betrieb)
- Learning- & Sensibilisierungsmaßnahmen (E-Learning/Präsenzschulungen) für die Belegschaft
- internes Datenschutz-Informationsportal
- Learning-Maßnahmen für die Koordinatoren und Koordinatorinnen
- Kosten für datenschutzrechtliche Beratung durch Externe
- Auditierungsmaßnahmen