

Datenschutzbeauftragte

Ein Praxisleitfaden für Einsteiger –
Grundlagen und Vertiefungen

Mit Mustern & Vorlagen

Stephan Hansen-Oest, Rechtsanwalt

2., aktualisierte Auflage 2023

Alle im Buch verwendeten Begriffe verstehen sich geschlechterneutral. Aus Gründen der besseren Lesbarkeit wird teilweise auf eine geschlechtsspezifische Differenzierung verzichtet – entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat lediglich redaktionelle Gründe und beinhaltet keine Wertung.

Bibliografische Information Der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.de> abrufbar.

ISBN 978-3-8005-1882-1

dfv Mediengruppe

© 2023 Deutscher Fachverlag GmbH, Fachmedien Recht und Wirtschaft, Frankfurt am Main
www.ruw.de

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung des Verlages unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Druck: Beltz Grafische Betriebe GmbH, 99947 Bad Langensalza

Printed in Germany

Vorwort

Nach nunmehr drei Jahren freue ich mich, die zweite Auflage dieses Buches präsentieren zu dürfen.

Die Neuauflage war erforderlich, um gesetzliche Änderungen und vor allem die Rechtsprechung des EuGH, der deutschen Gerichte und auch die Aufsichtsbehördenpraxis zu berücksichtigen.

Stil und Aufbau des Buches sind ansonsten gleichgeblieben. Es ist immer noch ein Lernbuch, mit dem Anfängerinnen und Anfänger sich dem umfangreichen Stoff erfolgreich nähern können. Der Untertitel des Buches ist leicht verändert worden, um deutlich zu machen, dass sich das Buch nicht nur zum Einstieg, sondern auch zur Vertiefung eignet.

Die zahlreichen Muster im Buch sind nun auch als Download verfügbar und jeweils im Buch gekennzeichnet.

Wie die erste Auflage ist auch diese zweite Auflage meiner Frau und meinen Kindern gewidmet. Sie halten mir immer noch den Rücken frei und unterstützen mich bei fast jeder, manchmal auch verrückten Idee, die ich gerne umsetzen möchte. Danke!

Flensburg, 30.7.2023

Stephan Hansen-Oest

Inhaltsverzeichnis

Vorwort	V
1. Einleitung – Warum ist dieses Buch so, wie es ist	1
2. Drei Buchstaben: DSB	4
Was muss ich als DSB wissen?	5
3. Begriffsklärungen	10
3.1 Verantwortlicher	10
3.2 Gemeinsam Verantwortliche	12
3.3 Auftragsverarbeiter	13
3.4 Personenbezogene Daten	14
3.5 Besondere Kategorien personenbezogener Daten („Magendaten“)	16
3.6 Gebräuchliche Abkürzungen	17
4. Wer bin ich als DSB?	18
4.1 Stellung des DSB	19
4.2 Aufgaben des DSB	23
4.3 Was ist nicht Aufgabe des DSB?	25
4.4 Haftung des DSB	26
4.5 Wann muss ein DSB benannt werden?	28
4.6 Muster einer Benennung	29
5. Rechtliche Grundlagen	32
5.1 Rechtsquellen	32
5.2 Sachlicher und räumlicher Anwendungsbereich	34
5.3 Struktur der DSGVO	37
6. Grundsätze für die Verarbeitung personenbezogener Daten	43
6.1 Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz	43
6.2 Zweckbindung	44
6.3 Datenminimierung	45
6.4 Richtigkeit	46
6.5 Speicherbegrenzung	46
6.6 Integrität und Vertraulichkeit	47
6.7 Rechenschaftspflicht	47
7. Grundüberlegungen zur „Gemüsenorm“	48
7.1 Art. 6 Abs. 1 lit. a) DSGVO – Einwilligung → „ALTer- native“	50
7.2 Art. 6 Abs. 1 lit. b) DSGVO – Datenverarbeitung zur Vertragserfüllung → „Dickes B“	50

Inhaltsverzeichnis

7.3	Art. 6 Abs. 1 lit. c) DSGVO – Datenverarbeitung zur Erfüllung rechtlicher Pflichten → „Caesar“	51
7.4	Art. 6 Abs. 1 lit. d) DSGVO – Datenverarbeitung für lebenswichtige Interessen → „Dead“	51
7.5	Art. 6 Abs. 1 lit. e) DSGVO – Datenverarbeitung für öffentliche Aufgaben → „Echt jetzt“	52
7.6	Art. 6 Abs. 1 lit. f) DSGVO – Datenverarbeitung auf Basis einer Interessenabwägung → „FETT“	53
8.	Die Einwilligung – „ALternative“	54
9.	Datenverarbeitung für Vertragszwecke – „Dickes B“	57
10.	Datenverarbeitung zur Erfüllung rechtlicher Pflichten – „Caesar“	60
11.	Datenverarbeitung für lebenswichtige Interessen – „Dead“	61
12.	Datenverarbeitung für öffentliche Aufgaben – „Echt jetzt“	62
13.	Datenverarbeitung auf Basis einer Interessenabwägung – „FETT“	63
13.1	Erste Stufe – Berechtigtes Interesse des Verantwortlichen oder Dritten	63
13.2	Zweite Stufe – Zur Wahrung des berechtigten Interesses erforderlich	64
13.3	Dritte Stufe – Abwägung mit entgegenstehenden Interessen der betroffenen Personen	64
13.4	Widerspruchsrecht	65
13.5	Kein „FETT“ für öffentliche Stellen	65
14.	Verarbeitung von „Magendaten“	67
15.	Standard-Datenschutzmodell (SDM) – auf ein Wort	68
16.	Die Informationspflichten der DSGVO	70
16.1	Gut gedacht – schlecht gemacht	70
16.2	Grundsatz der Transparenz	70
16.3	Zeitvorgaben für die Beantwortung von Anfragen Betroffener	71
16.4	Daten zum Betroffenen nicht verfügbar	72
16.5	Zweifel an der Identität des Betroffenen	72
16.6	Bildsymbole	72
17.	Informationspflichten bei der Erhebung beim Betroffenen	73
17.1	Praktische Begrenzung der Informationsfülle	75
17.2	Die „Link-Lösung“	75
17.3	Ausnahmen von der Informationspflicht	75

17.4	Weiterverarbeitung	76
18.	Informationspflichten bei Daten, die nicht beim Betroffenen erhoben wurden	77
18.1	Weiterverarbeitung	78
18.2	Ausnahmen	78
19.	Beispiel einer Information – Datenschutzhinweise für Beschäftigte	82
20.	Auskunftsrecht und Recht auf Kopie	86
20.1	Erste Stufe – „Ob“ einer Verarbeitung	86
20.2	Zweite Stufe – Auskunft zu gespeicherten Daten	86
20.3	Dritte Stufe – Weitere Informationen	87
20.4	Vierte Stufe – Recht auf Kopie	87
21.	Löschansprüche von Betroffenen	89
21.1	Recht auf Vergessenwerden	89
21.2	Ausnahmen von Löschpflichten	90
22.	Weitere Betroffenenrechte	91
23.	Datenschutz-Compliance und risikobasierter Ansatz	94
24.	Privacy by Design & by Default	95
25.	Auftragsverarbeitung	98
25.1	Was ist Auftragsverarbeitung?	98
25.2	Wann liegt eine Auftragsverarbeitung vor?	100
25.3	Wann liegt keine Auftragsverarbeitung vor?	101
25.4	Der Auftragsverarbeitungsvertrag	102
25.5	Unterauftragnehmer	103
25.6	Technische und organisatorische Maßnahmen	104
25.7	Mustervertrag	105
26.	Gemeinsame Verantwortlichkeit	123
26.1	Wann liegt eine gemeinsame Verantwortlichkeit vor?	123
26.2	Wie muss ich die gemeinsame Verantwortlichkeit „regeln“?	124
26.3	Muster einer Vereinbarung zur gemeinsamen Verantwortlichkeit	125
27.	Meldepflichten bei „Datenpannen“	131
27.1	Was ist eine Datenschutzverletzung („Datenpanne“)?	131
27.2	Wann ist diese bei der Aufsichtsbehörde zu melden?	132
27.3	Wie schnell muss die Meldung erfolgen?	134
27.4	Wie muss die Meldung erfolgen?	134

Inhaltsverzeichnis

27.5	Dokumentation der Datenpanne.	135
27.6	Meldepflicht gegenüber Betroffenen	136
28.	Verzeichnis von Verarbeitungstätigkeiten	138
28.1	Gibt es Ausnahmen?	138
28.2	Was ist das Verarbeitungsverzeichnis?	139
28.3	Wie erstelle ich das Verarbeitungsverzeichnis praktisch?	140
28.4	Wie pflege ich das Verarbeitungsverzeichnis?	141
28.5	Muster für ein Verarbeitungsverzeichnis	141
29.	Datenschutz-Folgenabschätzung (DSFA)	172
29.1	„In dubio pro DSFA“	172
29.2	Wann ist eine DSFA durchzuführen?	173
29.3	Was muss eine DSFA beinhalten?	173
29.4	Empfehlung für die Praxis als DSB	175
29.5	Besonderheiten für „Caesar“ und „Echt jetzt“	176
30.	Haftung für Datenschutzverletzungen?	177
	Was muss ein DSB zu Schadensersatzansprüchen der DSGVO wissen?	177
31.	Aufsichtsbehörde.	178
32.	Beschäftigtendatenschutz	179
33.	Datenverarbeitung in Drittländern	181
34.	Datensicherheit nach DSGVO – Einleitung	182
35.	Rechtsgrundlagen zur Datensicherheit	183
35.1	Was ist eigentlich „Datensicherheit“?	183
35.2	Datensicherheit in der DSGVO	184
35.3	Grundsatz der „Integrität und Vertraulichkeit“ (Art. 5 Abs. 1 lit. f) DSGVO)	184
35.4	Sicherheit der Verarbeitung (Art. 32 DSGVO)	186
35.5	Weitere Rechtsgrundlagen zur Datensicherheit	189
36.	Sanktionen bei Nicht- oder Schlechtumsetzung von Daten- sicherheit	192
37.	Haftungsrisiken bei Nicht- oder Schlechtumsetzung von Daten- sicherheit	193
38.	Umsetzung von Datensicherheit (Theorie)	195
38.1	Datensicherheit für „Beginner“	195
38.2	Wie und wieviel Datensicherheitsmaßnahmen muss ich denn treffen?	197
38.3	Was wollen wir schützen?	198

38.4	Hilfreiche Dokumente	198
38.5	Schritt 1 – Die Analyse	199
38.6	Schritt 2 – Die Schutzbedarfsfeststellung	200
38.7	Schritt 3 – Die Risikoanalyse	202
38.8	Schritt 4 – Maßnahmen treffen	204
39.	Überlegung für eine praktikable Umsetzung von Datensicherheit in KMU	205
40.	Wie organisiere ich als DSB meine Arbeit?	206
41.	Wie fange ich an? – Erste Schritte als DSB	209
	Zu Beginn – Organisation und Abläufe kennenlernen	209
42.	Wir bauen uns ein Datenschutzmanagementsystem (DSMS)	212
42.1	Top-Management ins Boot holen	213
42.2	Leitlinie zu Datenschutz und Informationssicherheit	213
42.3	Datensicherheits-/Datenschutz-Team bilden	217
42.4	Verarbeitungsverzeichnis	217
42.5	TOM-Dokument	217
42.6	Beispiel: TOM-Dokument	218
42.7	Kritische Prozesse identifizieren & Schutzbedarf feststellen	223
42.8	Risikoanalyse in „dreieckig“	224
42.9	Richtlinien erstellen und verbindlich machen	226
42.10	Richtlinie zum Datenschutz (für Beschäftigte)	227
42.11	Richtlinie zur Umsetzung von Datenschutzmaßnahmen	229
42.12	Richtlinie für die Umsetzung von Betroffenenrechten	234
42.13	IT-Richtlinie für Nutzer	236
42.14	Richtlinie für Speicherorte	242
42.15	Richtlinie für die Nutzung mobiler IT-Systeme	244
42.16	Richtlinie für die Nutzung mobiler Datenträger	246
42.17	Richtlinie Regelungen für Lieferanten und sonstige Auf- tragnehmer	249
42.18	Richtlinie für Störungen und Ausfälle	252
42.19	Richtlinie für Sicherheitsvorfälle	253
42.20	Notfallplan	255
42.21	Evaluierung	258
43.	Schlusswort	259
	QR-Code zum Download der Muster	260

1. Einleitung – Warum ist dieses Buch so, wie es ist ...

Dieses Buch soll anders sein als andere Bücher zum Datenschutzrecht. Oder andere Bücher, deren Zielgruppe **Datenschutzbeauftragte** sind.

Dieses Buch darf auch anders sein, weil der Verlag mir dankenswerter Weise erlaubt hat, hier „offen zu sprechen“.

Und zwar in einer Art und Weise, die nicht dem klassischen, gewöhnlichen juristischen Stil entspricht. Sondern in einem lockeren, offenen und zugleich auch herzlich norddeutschen Ton.

Dem Datenschutzrecht eilt der Ruf voraus, dass es sich um ein trockenes, langweiliges und sprödes Rechtsgebiet handle. Auch wenn dem nach meiner Überzeugung nicht so ist, würde hier ein juristisch-trockener Schreibstil nicht gerade dazu beitragen, dass wir Datenschutzrecht gut erlernen können.

Die verstorbene Psychologin und Managementtrainerin Vera F. Birkenbihl hat einmal sinngemäß gesagt: „Das Gehirn lernt gern in einem guten Zustand.“

Und so habe auch ich die Vorstellung, dass Leserinnen und Leser dieses Buches sich die Inhalte nicht mit Gewalt versuchen, in ihr Hirn einzuarbeiten, sondern in einer gemütlichen Liege- oder Sitzposition dieses Büchlein nehmen und sich mit einem kleinen Schmunzeln und Augenzwinkern im Gesicht dem Thema Datenschutz nähern.

Übrigens war der Untertitel des Buches „Stroh im Kopf“ von Vera F. Birkenbihl dieser: „Vom Gehirn-Besitzer zum Gehirn-Benutzer“ – auch das ist ein schönes Bildnis, das gut für Anwenderinnen und Anwender der DSGVO passen könnte.

Dieses Buch ist in Du-Form geschrieben. Das ist so, weil ich meine, dass du die Inhalte dieses Buches so besser verinnerlichen kannst. Zumindest ist das meine Erfahrung in der Vermittlung von Datenschutzwissen der letzten 10 Jahre.

Vielleicht magst du diesen Ansatz nicht. Und vielleicht hast du auch mal gelesen, dass das gar nicht stimmt, sondern Siezen viel mehr zum Wissenserwerb beiträgt. Aber leg diesen Gedanken doch einfach einmal beim Lesen dieses Buches zur Seite und freunde dich zumindest mit dem Gedanken an, dass es stimmen könnte, dass ein „Du“ für ein Erlernen von Datenschutzwissen mehr wirkt.

Und vielleicht hilft dir dabei auch, dass es ein „respektvolles Du“ ist, das wir hier gemeinsam verwenden wollen.

Was vielleicht beim Lesen eines juristisch geprägten Werkes auch neu für dich ist: Die Sprache ist bewusst nicht staubtrocken formal, sondern so, dass du es (hoffentlich) nicht so schwer hast, dieses Buch nicht nur zu lesen, sondern die Inhalte auch zu verstehen.

Also suche dir ein schönes Plätzchen und fang einfach mal an.

Ach, und noch etwas: Ich verwende in diesem Buch mal das generische Femininum und mal das generische Maskulinum. Hierbei gilt, dass sich andere Geschlechter genauso angesprochen fühlen dürfen.

Ich schreibe die DSGVO in diesem Buch übrigens ohne Bindestrich. Du kannst in vielen anderen Büchern die Abkürzung „DS-GVO“ lesen. Ich finde es ohne Bindestrich angenehmer. Und letztlich kürzt nun auch das Bundesverfassungsgericht (BVerfG) den Gesetzesnamen mit DSGVO ab. Du befindest dich also in guter Gesellschaft, wenn du keinen Bindestrich verwendest.

Apropos gute Gesellschaft: Viele gute Informationen findest du heute in sozialen Netzwerken. In einer Zeit, in der Twitter noch Twitter hieß (und war), gab es z. B. unter dem Hashtag #teamdatenschutz viele zahlreiche und aktuelle Beiträge und Diskussionen zu datenschutzrechtlichen Themen. Die gibt es dort auch heute noch. Nur haben sich die sozialen Netzwerke diversifiziert bzw. die Teilnehmerinnen und Teilnehmer finden sich jetzt verstreut in unterschiedlichen Netzwerken. So kannst du heute auch bei Mastodon oder auch LinkedIn zahlreiche gute Beiträge und Diskussionen finden. Nur sind sie leider etwas schwieriger aufzufinden als zuvor.

Seit dem 25.5.2018 wird die Datenschutz-Grundverordnung (DSGVO) angewendet. In Kraft ist sie schon seit dem 24.5.2016. So hatten Unternehmen und öffentliche Stellen damals „eigentlich“ schon zwei Jahre Zeit, um sich auf die DSGVO vorzubereiten und die Umsetzung dieser neuen gesetzlichen Regelungen zur Verarbeitung personenbezogener Daten intern voranzutreiben.

Nur war das praktisch mitnichten der Fall. Während ich diese Zeilen schreibe, sind weit über 1.800 Tage seit der Geltung der DSGVO vergangen. Und wenn wir ganz ehrlich sind, wissen wir heute immer noch nicht so ganz genau, wie wir dieses „Ungetüm“, wie es manche bezeichnen, bewältigen wollen oder sollen.

Und schließlich möchte ich in diesem Buch auch gerne ehrlich sein. Natürlich kann ich dir empfehlen, jede Excel-Datei in dein Verzeichnis von Verarbeitungstätigkeiten zu übernehmen, damit dieses Verzeichnissesverzeichnis (viele kürzen es gerne als „VVT“ ab) möglichst komplett ist. Nur ist damit keinem geholfen. Dir nicht, weil du dann niemals fertig wirst, und der Aufsichtsbehörde nicht, weil sie mit so einem Verzeichnis nicht viel anfangen

kann. Und dem Betroffenen übrigens auch nicht. Denn diesem ist letztlich dein Verarbeitungsverzeichnis egal. Er möchte vielmehr, dass du seine personenbezogenen Daten ordentlich verarbeitest.

Ich erzähle in diesem Buch auch Geschichten von mir oder eben auch Dinge, die ich mit Mandantinnen erlebt habe. Die Geschehnisse habe ich dabei jeweils so abgeändert, dass keine Rückschlüsse auf meine Mandantinnen gezogen werden können.

Meine Hoffnung ist, dass dieses Buch auch deswegen „authentisch“ für dich ist. Und da bleibt es nicht aus, dass einige Dinge mit einem Augenzwinkern und manchmal auch einem Grinsen im Gesicht erzählt werden.

Ich fände es auch ein wenig traurig, wenn uns wegen DSGVO & Co. das Lachen vergehen würde. Ich habe gerade wegen der DSGVO in den letzten beiden Jahren viel gelacht. Ja, auch so manche Stilblüten hat die DSGVO oder vielmehr die Anwender der DSGVO hervorgebracht.

Und um ganz ehrlich zu sein, bemerke ich mich auch heute noch häufig laut lachend am Schreibtisch. So manche Urteilsbegründung oder auch Äußerungen einiger Aufsichtsbehörden lassen dann kein Auge trocken. Das ist in anderen Rechtsgebieten aber auch so. Und da merkst du... so trocken ist dieses Rechtsgebiet also wirklich nicht. Oder wir können auch sagen, dass es mit ein bisschen Humor eine feuchtfrohliche Angelegenheit sein kann.

2. Drei Buchstaben: DSB

Dieses Buch richtet sich an **Datenschutzbeauftragte**. Egal ob weiblich oder männlich, ob intern oder extern, ob in Unternehmen oder öffentlicher Stelle. Dieses Buch ist eine Einführung für jede Datenschutzbeauftragte und jeden Datenschutzbeauftragten.

Die gebräuchliche Abkürzung für Datenschutzbeauftragte ist **DSB**. Und daher verwende ich sie hier auch in diesem Buch. Wenn ich hier von DSB schreibe, darf sich damit jede Datenschutzbeauftragte und jeder Datenschutzbeauftragte eines Unternehmens oder einer öffentlichen Stelle angesprochen fühlen.

Und natürlich darfst du dich auch angesprochen fühlen, wenn du noch kein DSB bist, sondern erst auf dem Weg dahin bist bzw. überlegst, ob dieses Berufsbild etwas für dich ist.

Apropos Berufsbild – ein offizielles oder gar festes Berufsbild gibt es für Datenschutzbeauftragte nicht. Es gibt jedoch auf Verbandsebene Vorstellungen dazu. Beispielfhaft kann hier „Das berufliche Leitbild der Datenschutzbeauftragten“ des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e. V. genannt werden.

Das Fehlen eines amtlichen Berufsbildes wird vielerorts bedauert. Beklagt wird, dass ein fehlendes Berufsbild dazu führe, dass die Qualität der DSB nicht gewährleistet sei.

Nun, das mag stimmen. Jedenfalls in Teilbereichen. Ich berate als Anwalt seit mehr als 20 Jahren DSB und habe so eine ganze Menge Menschen aus dieser Berufssparte kennengelernt. Ich habe DSB kennengelernt, die eine – nach Ansicht einiger Berufsverbände von DSB – exzellente Ausbildung genossen haben. Andere wiederum waren „Selfmade“-DSB und haben sich sozusagen alles selbst beigebracht.

Ich kann aus meiner Erfahrung mit DSB mit unterschiedlichen Ausbildungen sagen, dass auch eine vermeintlich exzellente Ausbildung in bestimmten Kursen anerkannter Anbieter nicht zwingend dazu führt, dass eine Person als DSB auch das erforderliche Fachwissen anwenden kann. Und so habe ich manchen „Selfmade“-DSB kennengelernt, der jeden anderen DSB mit vermeintlich herausragender Ausbildung im Hinblick auf Kenntnis von Datenschutzrecht und Datensicherheit und die praktische Anwendung dieser Fachbereiche locker in die Tasche stecken konnte.

Und dennoch sehe auch ich das Problem, dass ein fehlendes „offizielles“ Berufsbild dazu führt, dass sich eben nahezu jede Person „DSB“ nennen kann, ohne den Hauch einer Ahnung im erforderlichen Datenschutzwissen zu haben.

Letztlich ist es Sache der „Verantwortlichen“, also der Unternehmen oder öffentlichen Stelle, einen geeigneten DSB auszuwählen und zu benennen. Hier ist eine sorgfältige Auswahl oberstes Gebot.

Was muss ich als DSB wissen?

Was ein DSB wissen muss, ergibt sich primär aus dem Gesetz. Oder – besser gesagt – den Gesetzen. Und davon gibt es eine ganze Reihe.

Welche Anforderungen an „Wissen“ an einen DSB nun aber zu stellen sind, ergibt sich erst einmal aus Art. 37 Abs. 5 DSGVO. Denn dort können wir nachlesen, welche Anforderungen ein DSB zu erfüllen hat, damit er zum DSB benannt werden kann.

Wörtlich heißt es in Art. 37 Abs. 5 DSGVO:

„Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.“

Benötigt wird also eine „berufliche Qualifikation“ und insbesondere ein **Fachwissen** auf dem Gebiet des **Datenschutzrechts** und der **Datenschutzpraxis**.

Aus dem Wortlaut ergibt sich zudem, dass dieses Fachwissen schon zum Zeitpunkt der Benennung vorliegen muss. Es gilt also, dass zunächst ein Fachwissen bestehen muss, bevor eine Benennung erfolgen kann.

Das ist in der Praxis häufig schwierig umzusetzen. Denn wie soll ein DSB Fachwissen in der Datenschutzpraxis erwerben, ohne zuvor DSB gewesen zu sein? Es ist ja mitnichten so, dass jede öffentliche Stelle oder jedes Unternehmen eine Abteilung „Datenschutz“ vorhält, in der Menschen Datenschutz praktisch ausüben können, um so eine Datenschutzpraxis zu erwerben.

In der Praxis läuft es vielmehr meist so ab, dass jemand in Unternehmen oder öffentlichen Stellen als DSB „ausgeguckt“ wurde, auf einen DSB-Lehrgang geschickt wurde und nach Rückkehr zum DSB benannt wurde. Wenn der DSB dann einen guten Lehrgang besucht und gut und aufmerksam zugehört hat, dann hat er vielleicht einen Teil des Fachwissens im Datenschutzrecht erlangt, aber sicher keine Datenschutzpraxis.

Und um es ganz ehrlich zu sagen: Das ist auch nicht wirklich schlimm. Denn am allermeisten lernen alle DSB, indem sie als DSB praktisch arbeiten.

Und solltest du bereits bei einem DSB-Lehrgang gewesen sein und nach der Rückkehr bemerkt haben, dass du eigentlich gar nicht weißt, wie du „anfangen“ sollst, dann kann ich dir versichern, dass du nicht alleine bist. Im Gegenteil, den meisten frischgebackenen DSB geht es so, wenn sie vom Lehrgang zurück sind.

Gefühlt liegt da vor vielen ein „Datenschutz-Berg“, dessen Besteigung nicht nur beschwerlich, sondern manchmal unmöglich scheint. Meine Empfehlung lautet dann: Nicht resignieren, sondern den Blick nach vorne richten. Und zwar nicht auf den Gipfel, sondern auf die erste Bergstation. Und dieses Buch wird dich dabei gerne ein wenig begleiten.

Und wenn du dann merkst, dass der Weg zur ersten Bergstation mit ein wenig Hilfe doch „gar nicht so schlimm“ war, dann schaffst du die weiteren Stationen bis zum Gipfel auch. Eine nach der anderen. Bis du dann ganz oben auf dem Gipfel stehst. Und dann hoffentlich den „Überblick“ hast.

Schon an dieser ersten kleinen Stelle, in der es um die gesetzlich geforderte Datenschutzpraxis geht, merken wir also, dass nicht alles, was in Gesetzen schriftlich niedergelegt ist, auch in exakt der Form so umsetzbar ist. Und das muss es auch nicht.

Wir Juristen haben dazu im Studium gelernt, wie Gesetze auszulegen sind, um diese Widersprüche aufzulösen. Und auch wenn du nicht alle Auslegungsmethoden von Gesetzen kennen musst, werden wir doch immer mal wieder an diesen Stellen einhaken, um zu schauen, wie bestimmte Probleme in der Anwendung des Datenschutzrechts gelöst werden könnten.

Aber zurück zum Thema: Ein DSB muss also Fachwissen bzgl. Datenschutzrecht und Datenschutzpraxis haben.

Einigkeit besteht darin, dass es für DSB nicht zwingend ist, ein Studium der Rechtswissenschaften absolviert zu haben. Sicher schadet es nicht, aber erforderlich ist es eben nicht. Dies gilt in gleicher Weise für ein technisches Studium, wie z.B. der Informatik. Auch das schadet einem DSB sicher nicht, zwingend ist es aber gleichwohl nicht.

Auch muss die berufliche Qualifikation nicht unbedingt einen Fokus auf dem Datenschutz gehabt haben. Ich denke zwar schon, dass es hilfreich ist, wenn ein DSB in einem rechtlichen Beruf oder einem IT-orientierten Beruf eine Ausbildung gemacht hat. Prädestiniert wäre auch eine berufliche Qualifikation im Bereich der Revision oder auch des Qualitätsmanagements. Denn gerade diese Bereiche prägten in den letzten Jahren den Datenschutz.

Aber zwingend ist dies – wie gesagt – alles nicht. Die rechtswissenschaftliche Literatur in Deutschland diskutiert die Anforderungen an einen DSB immer noch primär mit Blick auf das erforderliche **Fachwissen**. Dieses soll nach häufig vertretener Auffassung vorliegen, wenn ein DSB

- genügend rechtliche Kenntnisse im Datenschutzrecht,
- genügend technische Kenntnisse im Bereich der Datensicherheit und
- genügend organisatorische Kenntnisse über die Abläufe von Datenverarbeitung im Unternehmen oder der öffentlichen Stelle hat.

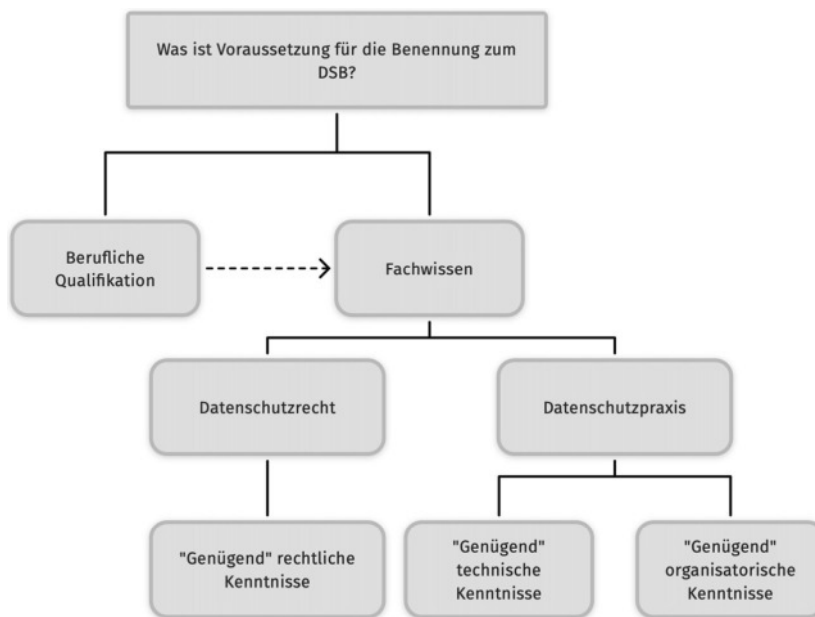


Abbildung 1: Voraussetzungen für die Benennung zum DSB

Auch in der Rechtsprechung sind die Anforderungen thematisch behandelt worden. So hat sich das Landesarbeitsgericht Mecklenburg-Vorpommern (Urteil vom 25.2.2020, Az.: 5 Sa 108/19) mit den Anforderungen befasst.

Zusammengefasst lassen sich die Anforderungen danach wie folgt aufstellen:

- Der Datenschutzbeauftragte muss über die Fähigkeit verfügen, seine in Art. 39 DSGVO genannten Aufgaben zu erfüllen.
- Die Tätigkeit des Datenschutzbeauftragten ist **nicht** an eine bestimmte Ausbildung oder näher bezeichnete **Fachkenntnisse** geknüpft.
- Welche Sachkunde erforderlich ist, richtet sich insbesondere nach der **Größe der Organisation, dem Umfang der anfallenden Datenverarbeitungsvorgänge, den eingesetzten IT-Verfahren und dem Typus der anfallenden Daten.**

2. Drei Buchstaben: DSB

- Wenn der DSB nur in einem **Teilbereich** über eine eigene Qualifikation verfügt, genügt es, wenn er im Übrigen auf fachkundige Mitarbeiter zurückgreifen kann.
- **Fortbildungen** des DSB zu neuen technischen Entwicklungen und Gesetzesänderungen bzw. Entwicklungen in der Rechtsprechung sind **unerlässlich**.
- Der DSB muss nicht nur die nötigen Fachkenntnisse besitzen, sondern auch die **Gewähr** bieten, dass er seinen Aufgaben **gewissenhaft nachkommt** und nicht gegen seine Pflichten als DSB (z. B. seine Verschwiegenheitspflicht) verstößt.
- Der DSB muss – über die Sachkunde hinaus – eine wirksame **Selbstkontrolle der Organisation** gewährleisten können.

Im Hinblick auf die erforderliche Fachkunde ist offen, wie dieses Fachwissen belegt werden kann.

Gebräuchlich ist eine Abschlussprüfung, die ein DSB ggf. am Ende seines Lehrgangs absolviert hat. Wirklich aussagekräftig ist dies jedoch häufig nicht.

Es kommt durchaus vor, dass Aufsichtsbehörden z. B. im Zusammenhang mit einer Beschwerde eines Betroffenen bei einem Unternehmen nachfragen, wer zum DSB benannt ist und wie dieser sein Fachwissen erworben hat.

Hier wird jedoch in aller Regel keine absolvierte Prüfung verlangt. Eine gewisse „Ausbildung“ in Form eines Lehrgangs, Teilnahme an Schulungen oder Seminaren sollte aber schon nachgewiesen werden können.

Ich persönlich halte es für viel wichtiger, dass DSB sich regelmäßig und fortwährend weiterbilden. Denn das eigentliche Fachwissen wird erst durch ein „Tun“ in der Praxis erworben und kann dann in weiteren Fortbildungen, Schulungen oder Seminaren (online/offline) vertieft werden.

Letztlich kann sich aber jede Person einfach DSB nennen, da die Berufsbezeichnung an sich nicht geschützt oder die Berufsausbildung nicht staatlich reguliert ist.

Ein DSB ohne „Grundausbildung“ wird allerdings schnell an seine oder ihre Grenzen kommen.

Zusammengefasst muss ein DSB also grundlegende Kenntnisse im Datenschutzrecht, der Datensicherheit und der Organisation von Datenverarbeitung im betreffenden Unternehmen bzw. der öffentlichen Stelle haben.

Nach Erwägungsgrund 97 der DSGVO ist das geforderte Niveau des Fachwissens übrigens abhängig von der durchgeführten Datenverarbeitung und dem Schutzbedarf der Daten.

Konkret formuliert: Je höher der Schutzbedarf der Daten, umso höher sind die Anforderungen an die Kenntnisse des oder der Datenschutzbeauftragten. So wird man beispielsweise bei der Benennung einer Datenschutzbeauftragten in einem größeren Krankenhaus nicht nur eine erwiesene Fachkunde, sondern auch eine mehrjährige Berufspraxis in einem medizinischen Umfeld erwarten können.