

5.7 Geschäftsbesorgungsvertrag mit einem externen Datenschutzbeauftragten

Schrifttum: *Conrad*, Datenschutzkontrolle in der Anwaltskanzlei, ZD 2014, 165; *Conrad/Grützmacher* (Hrsg.), Recht der Daten und Datenbanken im Unternehmen, 2014; *Conrad/Hausen*, BAG: Entscheidung für einen internen Datenschutzbeauftragten kaum abänderbar?, ZD 2011, XIII; *Ehmann/Selmayr* (Hrsg.), Datenschutz-Grundverordnung: DSGVO, Kommentar, 2017; *Giesen*, Die Zuverlässigkeit interner Datenschutzbeauftragter, CR 2007, 202; *Gola/Klug*, Die Entwicklung des Datenschutzrechts in den Jahren 2009/2010, NJW 2010, 2483; *Gola/Schomerus*, BDSG, 12. Aufl. 2015; *Gola/Wronka/Pöppers*, Handbuch Arbeitnehmerdatenschutz, 7. Aufl. 2016; *Haag*, Betrieblicher Datenschutzbeauftragter, in: *Forgó/Helfrich/Schneider* (Hrsg.), Betrieblicher Datenschutz, 2. Auflage 2017; *Hallermann*, Wann ist der Datenschutzbeauftragte fachkundig und unabhängig?, DuD 2012, 122; *Härting*, Datenschutzreform in Europa: Einigung im EU-Parlament. Kritische Anmerkungen, CR 2013, 715; *Henkel*, Vertrag über die Beauftragung eines externen Datenschutzbeauftragten, in: *Moos* (Hrsg.), Datennutzungs- und Datenschutzverträge, 2014, S. 40 ff.; *Hoeren*, Der betriebliche Datenschutzbeauftragte, ZD 2012, 355; *Hornung*, Eine Datenschutz-Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25.1. 2012, ZD 2012, 99; *Jaspers/Reif*, Der betriebliche Datenschutzbeauftragte nach der geplanten EU-Datenschutz-Grundverordnung – ein Vergleich mit dem BDSG, RDV 2012, 78; *Jaspers/Reif*, Der Datenschutzbeauftragte nach der Datenschutz-Grundverordnung: Bestellpflicht, Rechtsstellung und Aufgaben, RDV 2016, 61; *Kahlert/Licht*, Die neue Rolle des Datenschutzbeauftragten nach der DSGVO – Was Unternehmen zu beachten haben, ITRB 2016, 178; *Klug*, Der Datenschutzbeauftragte in der EU. Maßgaben der Datenschutzgrundverordnung, ZD 2016, 315; *Knopp*, Dürfen juristische Personen zum betrieblichen Datenschutzbeauftragten bestellt werden?, DuD 2015, 98; *Kremer/Sander*, Dienstvertrag mit einem externen betrieblichen Datenschutzbeauftragten, in: *Koreng/Lachenmann* (Hrsg.), Formularbuch Datenschutzrecht, 2015; *Kremer/Sander*, Beratungsvertrag mit einem Dienstleistungsunternehmen, in: *Koreng/Lachenmann* (Hrsg.), Formularbuch Datenschutzrecht, 2015; *Kühling/Buchner*, Datenschutz-Grundverordnung, 2017; *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis, 1. Aufl. 2016; *Lücke*, Muster: Geschäftsbesorgungsvertrag zur Bestellung eines externen Datenschutzbeauftragten, in: *Hümmerich/Lücke/Mauer* (Hrsg.), Arbeitsrecht – Vertragsgestaltung, Prozessführung, Personalarbeit, Betriebsvereinbarungen, 8. Aufl. 2014; *Moos* (Hrsg.), Datennutzungs- und Datenschutzverträge, 2014; *Paal/Pauly* (Hrsg.), Datenschutzgrundverordnung, 2017; *Petri/Tinnefeld*, Völlige Unabhängigkeit der Datenschutzkontrolle, MMR 2010, 157; *Plath* (Hrsg.), BDSG/DSGVO, Kommentar zum BDSG und zur DSGVO sowie den datenschutzrechtlichen Regelungen des TMG und des TKG, 2. Auflage 2016; *Richter*, Anmerkung zu VG Düsseldorf, Beschl. v. 8.2. 2012 – 26 L 36/12, ZD 2012, 186; *Schefzig*, Der Datenschutzbeauftragte in der betrieblichen Datenschutzorganisation – Konflikt zwischen Zuverlässigkeit und datenschutzrechtlicher Verantwortung, ZD 2015, 503; *Simitis* (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl. 2014; *Sydow* (Hrsg.), Europäische Datenschutzgrundverordnung, 1. Aufl. 2017; *Taeger*, Kommentar zu EuGH v. 9.3.2010 zu

Datenschutz-Aufsicht, K&R 2010, 330; *Weberndörfer/Zieger*, Arbeitsvertrag mit einem Datenschutzbeauftragten, in: Moos (Hrsg.), Datennutzungs- und Datenschutzverträge, 2014, S. 1 ff.; *Wolff/Brink* (Hrsg.), BeckOK Datenschutzrecht, DSGVO, 21. Edition, Stand: 1.8.2017; *Wybitul/von Gerke*, Checklisten zur DSGVO – Teil 2: Pflichten und Stellung des Datenschutzbeauftragten im Unternehmen, BB 2017, 181; *Zilkens/Eikel*, Zur Bestellung eines „weiteren behördlichen Datenschutzbeauftragten“ – Anmerkung zu VG Düsseldorf, Beschl. v. 8.2. 2012 – 26 L 36/12, RDV 2012, 138.

A. Einleitung

- 1 Die europäische **Datenschutzrichtlinie 95/46/EG** ging vom **Grundsatz der Fremdkontrolle** des betrieblichen Datenschutzes aus. So sah Art. 18 Abs. 1 RL 95/46/EG eine staatliche Vorabkontrolle der privatwirtschaftlichen Datenverarbeitung vor, indem automatisierte Datenverarbeitungen einer unabhängigen Kontrollstelle iS von Art. 28 RL 95/46/EG gemeldet werden müssen. Als **Alternative** zur umfassenden Fremdkontrolle nach Art. 18 Abs. 1 RL 95/46/EG eröffnete Abs. 2 die Möglichkeit für eine **betriebliche Selbstkontrolle**. Als Ausnahme zur Meldepflicht konnten Mitgliedstaaten die Bestellung eines Datenschutzbeauftragten (DSB) durch den für die Verarbeitung Verantwortlichen vorsehen. Die Richtlinie schrieb nicht vor, dass die Bestellung eines DSB für den Verantwortlichen obligatorisch sein muss. Bei Bestellung oblag dem DSB die „*unabhängige Überwachung der Anwendung der zur Umsetzung dieser Richtlinie erlassenen einzelnen Bestimmungen*“, Art. 18 Abs. 2 (3. Spiegelstrich) RL 95/46/EG, und die „*Führung*“ (englische Fassung der Richtlinie „*keeping*“) eines Verfahrensverzeichnisses, Art. 18 Abs. 2 (4. Spiegelstrich) iVm. Art. 21 Abs. 2 RL 95/46/EG.
- 2 Im Gegensatz zu den anderen EU-Mitgliedstaaten hatte **Deutschland** von dem Wahlrecht in der RL 95/46/EG Gebrauch gemacht und ein **zweistufiges Kontrollsystem** eingerichtet, auf dessen erster Stufe – im Regelfall verpflichtend – die betriebliche Selbstkontrolle durch den DSB steht und nur unter bestimmten Bedingungen eine externe Kontrolle durch staatliche Aufsichtsbehörden (vgl. § 38 BDSG aF¹) stattfindet². Folgerichtig korrespondierten die Meldepflicht bei der Daten-

1 Eingef. mWv. 1.4.2010 durch Ges. v. 29.7.2009 (BGBl. I 2009, 2254).

2 Der EuGH hat das deutsche System staatlicher Aufsicht als nicht mit der Datenschutzrichtlinie vereinbar erklärt, Urt. v. 9.3.2010 – C-518/07, NJW 2010, 1265, und zwingt alle Bundesländer, die Datenschutzaufsichtsbehörden von jeglicher staatlicher Aufsicht freizustellen, vgl. *Gola/Klug*, NJW 2010, 2483, 2488 mwN.

schutzaufsichtsbehörde (§ 4d Abs. 1 BDSG aF) und die Ausnahme von der Meldepflicht bisher, wenn der Verantwortliche einen DSB bestellt hatte (§ 4d Abs. 2 BDSG aF).

Die **EU-Datenschutzgrundverordnung** (DSGVO), die am 25.5.2016 in Kraft trat und ab dem 25.5.2018 anzuwenden ist, sieht in Art. 37 DSGVO erstmalig EU-weit eine Pflicht zur Benennung¹ eines DSB für Behörden (mit Ausnahme von Gerichten oder unabhängigen Justizbehörden, die im Rahmen ihrer justiziellen Tätigkeit handeln²) und Unternehmen vor, wenn bestimmte Voraussetzungen vorliegen. Diese Pflicht trifft Behörden und Unternehmen nicht nur insoweit, als sie Verantwortliche sind. Die Pflicht gilt ausdrücklich auch für Auftragsverarbeiter. Art. 37 Abs. 1 DSGVO knüpft die Pflicht zur Benennung an bestimmte Voraussetzungen (dazu Rz. 11 ff.), wobei Art. 37 Abs. 4 Satz 1 DSGVO eine Öffnungsklausel vorsieht, von der der deutsche Gesetzgeber hinsichtlich Unternehmen mit § 38 Abs. 1 BDSG 2018³ Gebrauch gemacht hat. 3

Die Vorgaben der Richtlinie bedeuteten für die Stellung des DSB im Unternehmen, dass er v.a. eine Funktion als **neutrale Aufsicht** hat, die in Teilbereichen – sofern sie wirksam und ordnungsgemäß ausgeführt wird – die behördliche Aufsicht ersetzt. Auch die DSGVO betont in Art. 38 Abs. 3 Satz 1 die Unabhängigkeit bei der Erfüllung seiner Aufgaben, sieht den DSB allerdings vor allem als eine Person, die den Verantwortlichen bzw. Auftragsverarbeiter unterstützt und dafür über besonderes Fachwissen verfügen muss (s. Erwägungsgrund 97 Satz 1). Dass daneben weiterhin auch Überwachung und Kontrolle (s. Art. 39 Abs. 1 lit. b) DSGVO) zu den Aufgaben des DSB gehören, kann zu Interessenkonflikten führen (dazu Rz. 16). 4

1 Zur neuen Terminologie (in der englischen Fassung statt „appoint“ nunmehr „designate“) s. *Kahlert/Licht*, ITRB 2016, 178 (179).

2 S. dazu Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

3 Am 5.7.2017 wurde das neue Bundesdatenschutzgesetz (BDSG 2018) als Art. 1 des Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 30.6. 2017 im Bundesgesetzblatt (BGBl.) Teil I Nr. 44 veröffentlicht. Es tritt am 25.5.2018 in Kraft.

- 5 Alle Fragen im Zusammenhang mit Stellung und Aufgaben des DSB sind an der gesetzlichen Funktion des DSB auszurichten. Das gilt sowohl für die Abgrenzung der Aufgaben („Unterrichtung und Beratung“ sowie „Überwachung“ in Art. 39 Abs. 1 DSGVO) wie auch mit Blick auf alle – verständlichen – Bestrebungen der Unternehmen, den DSB nicht nur mit der Kontrolle, sondern auch mit der Verantwortlichkeit für Entwurf und Umsetzung des Datenschutz-Managements zu beaufschlagen. Im Ergebnis gilt eine ähnliche Faustregel wie für die Jahresschluss-Prüfer: Wer für die Umsetzung von Maßnahmen (mit-)verantwortlich ist, kann die Umsetzung nicht unabhängig kontrollieren. Eine personelle Trennung des Amts des DSB von den Datenschutz-Konzeptions- und Umsetzungsaufgaben ist somit erforderlich. In großen Unternehmen wird dies zunehmend realisiert.
- 6 Das BAG hat in einer älteren Entscheidung – ergangen zu BDSG 1990 – verneint, dass der DSB eine ausreichend neutrale Position hat, um den **Betriebsrat** zu kontrollieren¹. Aus Sicht des BAG schließt die „*vom Betriebsverfassungsgesetz geforderte Unabhängigkeit der Betriebsräte vom Arbeitgeber [...] eine Kontrolle durch den Datenschutzbeauftragten*“² aus. Als Voraussetzung für die Kontrolle durch den DSB sah das BAG an, dass dieser „– etwa aufgrund entsprechender Mitbestimmungsrechte des Betriebsrats bei seiner Bestellung und Abberufung – des Vertrauens beider Seiten in gleicher Weise bedürfte und unabhängig vom Arbeitgeber über eigene Handlungsmöglichkeiten verfügte“³. Zwar wurde die Stellung des DSB seit BDSG 1990 fortentwickelt und verbessert. Doch das Verhältnis zum DSB ist nach wie vor ungeklärt. Auch die DSGVO regelt diesen Aspekt nicht – wohl mangels Gesetzgebungskompetenz, die im arbeitsrechtlichen Bereich – anders als bei der Datenverkehrsfreiheit – beschränkt ist. Bei richtlinienkonformer Auslegung und auch nach dem Wortlaut der DSGVO ist die vom BAG seinerzeit bemängelte fehlende Unabhängigkeit vom Arbeitgeber zu hinterfragen (Art. 38 Abs. 3 DSGVO zur Weisungsunabhängigkeit). In der Praxis ist häufig zu beobachten, dass der DSB zwischen allen Stühlen sitzt und weder dem Lager des Arbeitgebers noch dem Lager der Betriebsräte zugeordnet werden kann.
- 7 Die Entwicklung des BDSG und die Regelungen in der DSGVO zeigen, dass die Bedeutung des DSB als innerbetriebliches Aufsichtsorgan seit

1 BAG v. 11.11.1997 – 1 ABR 21/97.

2 BAG v. 11.11.1997 – 1 ABR 21/97, Rz. 46.

3 BAG v. 11.11.1997 – 1 ABR 21/97, Rz. 53.

1990 erheblich zugenommen und sich sogar auf die anderen EU-Staaten ausgeweitet hat:

- Für den nicht-öffentlichen Bereich fanden sich bereits in den §§ 28, 29 **BDSG 1977**¹ sowie in den §§ 36, 37 **BDSG 1990**² Regelungen zur Bestellung und den Aufgaben des DSB. Fachkunde und Zuverlässigkeit als Voraussetzung für eine Bestellung, die direkte Unterstellung unter die Geschäftsleitung, die Weisungsfreiheit, das Benachteiligungsverbot, die Verschwiegenheitspflicht sowie die Unterstützungspflicht durch die verantwortliche Stelle waren bereits Bestandteil der Erstregelung.
- Mit der Änderung des BDSG im **Mai 2001**³ wurden die Regelungen zum DSB in den ersten Abschnitt des BDSG (§§ 4f und g BDSG 2001) verlagert, so dass damit erstmals **einheitliche** Bestimmungen für die Institution des DSB im öffentlichen wie im nicht-öffentlichen Bereich geschaffen wurden.
- Die Änderung des BDSG im **August 2006**⁴ brachte nicht nur eine Anhebung des Schwellenwertes in § 4f Abs. 1 Satz 4 BDSG für die Bestellung eines DSB von mehr als vier auf mehr als neun Personen, die mit der Verarbeitung personenbezogener Daten ständig beschäftigt sind. Dazu ist nur auf die bestimmungsgemäße Wahrnehmung der Datenverarbeitung durch diese Anzahl an Personen abzustellen, soweit sie in die betriebliche Organisation eingegliedert sind (nicht aber darauf, ob es sich um Arbeitnehmer, Geschäftsführer oder Leiharbeiter handelt oder welche Wochenarbeitszeit sie zu erfüllen haben).⁵ Des Weiteren führte die Änderung des BDSG auch eine Präzisierung der Fachkunde i.S.v. § 4f Abs. 2 BDSG sowie ein Beratungsrecht der DSB ggü. der Aufsichtsbehörde ein, § 4g Abs. 1 Satz 2 BDSG.

1 Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (BDSG) vom 27.1.1977, BGBl. I S. 201, verkündet am 1.2.1977.

2 Art. 1 des Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20.12.1990, BGBl. I S. 2954, in Kraft getreten am 30.12.1990.

3 Art. 1 des Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18.5.2001, BGBl. I 2001, S. 904, in Kraft getreten am 23.5.2001.

4 Art. 1 des Ersten Gesetzes zum Abbau bürokratischer Hemmnisse insb. in der mittelständischen Wirtschaft vom 22.8.2006, BGBl. I S. 1970, in Kraft getreten am 26.8.2006.

5 Gola/Schomerus/*Gola/Klug/Körffer*, BDSG, § 4f Rz. 10aff.; LfD Hamburg, Merkblatt zum betrieblichen Datenschutzbeauftragten nach §§ 4f, 4g BDSG, S. 1f.

- Mit der zum 1.9.2009 in Kraft getretenen BDSG-Novelle III¹ wurde ua. die Position des DSB durch die Aufnahme eines Kündigungsschutzes (über den bereits zuvor bestehenden Abberufungsschutz hinaus) sowie die Verpflichtung der verantwortlichen Stelle zur Übernahme von Kosten für Fort- und Weiterbildungsmaßnahmen in § 4f Abs. 3 BDSG weiter gestärkt. Zudem wurde der Bußgeldrahmen für eine nicht, nicht richtig oder zu spät erfolgte Bestellung des DSB erhöht.

8 Die DSGVO macht den DSB zum Grundmodell der Aufsicht, allerdings ergänzt um stärkere Kompetenzen der staatlichen Aufsicht. Dadurch wird das Amt des DSB weiter an Bedeutung gewinnen:

- Bereits in dem am 25.1.2012 von der EU-Kommission veröffentlichten **Entwurf einer Datenschutz-Grundverordnung (DSGVO-KOM)**² waren eine Benennungspflicht (allerdings erst ab 250 Beschäftigte), die Position und die Aufgaben DSB in den Art. 35–37 geregelt. Der DSB sollte einerseits zusätzliche Aufgaben bekommen (z.B. Pflicht zur Erstellung der Verfahrensübersicht und nicht mehr Anspruch auf Zurverfügungstellung durch den Verantwortlichen bzw. Auftragsverarbeiter und insgesamt umfangreiche Dokumentationspflichten des DSB, vgl. Art. 37 Abs. 1 lit. d DSGVO-KOM). Andererseits wurde der Aufgabenbereich des DSB reduziert und abgespeckt. So sollten z.B. Vorabkontrollen nicht mehr zum zukünftigen Aufgabenkreis des DSB gehören.
- Der Kommissionentwurf vom 25.1.2012 wurde in den Mitgliedstaaten – v.a. in Deutschland – sehr kritisiert, auch wenn manche Ansätze durchaus Anklang fanden. Aus den Mitgliedstaaten gab es über 3.000 Änderungsanträge. Am 21.10.2013 hat der Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments (**LIBE**) insgesamt 102 Änderungsanträge zu den 91 Artikeln des Entwurfs der Datenschutzgrundverordnung vom 25.1.2012 mit großer Mehrheit angenommen³. Die im Kommissionsentwurf v. 25.1.2012 vorgeschlagene Grenze von 250 Beschäftigten wurde im Entwurf des LIBE-Ausschusses v. 21.10.2013 zugunsten eines ande-

1 Art. 1 des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 14.8.2009, BGBl. I S. 2814, in Kraft getreten am 20.8.2009.

2 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.1.2012.

3 Zum damaligen Stand nach der Einigung im EU-Parlament s. *Härtling*, CR 2013, 715 ff.

ren – aber wohl unpraktikablen – Berechnungsschemas (Anzahl der von einer personenbezogenen Datenverarbeitung betroffenen Personen während einer **12-Monatsperiode; grds. bei 5.000 Betroffenen**¹⁾ aufgegeben. Im Übrigen sollte – wie im Kommissionsentwurf – die Bestellpflicht bei bestimmten „core activities“ **unabhängig von einer Personengrenze** gelten. Die zweite Neuerung brachte Art. 35 Abs. 7 des LIBE-Entwurfs, der einen Mindestbestellzeitraum vorsah und zwischen internem (4 Jahre) und externem Datenschutzbeauftragten (2 Jahre) differenzierte. Im Prinzip war eine Klarstellung wünschenswert, weil bereits die Forderungen der deutschen Datenschutzbehörden zwischen 3 und 5 Jahren variieren. Die Differenzierung leuchtete ein, da der interne DSB üblicherweise stärker geschützt werden muss und ein 4-jähriger Zwangsvertrag mit einem Externen unangemessen ist.

In Deutschland hat große Diskussionen ausgelöst², dass der Kommissionsentwurf der DSGVO eine teilweise Anhebung des **Schwellenwerts für die Bestellpflicht** vorsah³ und insoweit eine Erleichterung für kleinere und mittlere Unternehmen darstellte⁴. Speziell in Deutschland hatte sich ein Markt für externe DSB gebildet, der sich von der geplanten Schwellenanhebung bedroht sah. Der Rat der Europäischen Union nahm am 10.10.2014 eine „partielle allgemeine Ausrichtung“ zur DSGVO an⁵, die die Verpflichtung zur Benennung eines DSB in das Ermessen der Mitgliedstaaten stellte, vgl. Art. 35 Abs. 1 DSGVO-Rat, wobei es dem Verantwortlichen und Auftragsverarbeiter freistand, ob sie eine Person innerhalb oder außerhalb des Verantwortlichen oder Auftragsverarbeiters zum DSB benannte⁶. 9

Die DSGVO sieht nun in ihrer in Kraft getretenen Fassung sowohl eine **freiwillige Benennung** (Art. 37 Abs. 4 Satz 1, 1. Halbs. DSGVO) als auch eine **Benennungspflicht** vor, wobei letztere gem. Art. 37 Abs. 1 lit. b) und c) DSGVO, wie es schon der Kommissionsentwurf vorsah, an be- 10

1 Conrad/Grützmacher/Conrad/Schneider, Recht der Daten und Datenbanken im Unternehmen, S. 1137 f.

2 Statt vieler *Hornung*, ZD 2012, 99 (104); *Hoeren*, ZD 2012, 355 (356 f.); *Jasper/Reif*, RDV 2012, 78.

3 Nach BDSG-alt liegt die Schwelle bei mind. 10 Personen hins. automatisierter Verarbeitung und (weniger praxisrelevant) mindestens 20 Personen bei nicht-automatisierter Verarbeitung (§ 4f Abs. 1 Satz 3 und Satz 4 BDSG).

4 *Hoeren*, ZD 2012, 355 (356 f.).

5 <http://data.consilium.europa.eu/doc/document/ST-13772-2014-INIT/de/pdf>.

6 Vgl. Art. 35 Abs. 8 der Fassung des Rates.

stimmte „Kerntätigkeiten“ eines Unternehmens anknüpft (s. dazu Rz. 12) oder durch mitgliedstaatliches Recht vorgegeben werden kann (vgl. Art. 37 Abs. 4 Satz 1, 2. Halbs. DSGVO). Weitere wesentliche Neuerungen sind zB¹:

- Pflicht zur Benennung eines DSB auch für Auftragsverarbeiter
- Möglichkeit für öffentliche Stellen, einen externen DSB zu benennen
- Pflicht, die Kontaktdaten des DSB zu veröffentlichen und der Aufsichtsbehörde mitzuteilen
- Stärkerer Fokus auf die Beratungsaufgaben des DSB
- Stärkerer Fokus auf die risikoorientierte Aufgabenerfüllung durch den DSB

11 Gem. DSGVO besteht die Bestellpflicht für Verantwortliche und Auftragsverarbeiter, wenn

- die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem. Art. 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 DSGVO besteht.

12 Die DSGVO selbst regelt keine Mindestbeschäftigtenzahl (s. aber sogleich BDSG 2018). Gem. Erwägungsgrund 97 der DSGVO bedeutet „Kerntätigkeit“ eines Unternehmens seine Haupttätigkeiten und nicht die Verarbeitung personenbezogener Daten als Nebentätigkeit – wobei Haupttätigkeit nicht wesentlich klarer sein dürfte als Kerntätigkeit. Die Verarbeitung bestimmter Gesundheitsdaten in der Personalabteilung (etwa Krankmeldungen und Schwerbehinderteneigenschaft) gilt z.B. als Nebentätigkeit, wohingegen bei einem Krankenhaus Gesundheitsdatenverarbeitung eine Haupttätigkeit ist.² Bei einer Anwalts-

1 LfD Hessen, Der behördliche und betriebliche Datenschutzbeauftragte nach neuem Recht, Stand 2017.

2 Forgó/Helfrich/Schneider/Haag, Betrieblicher Datenschutz, 2. Aufl. 2017, S. 183.

kanzlei mit Strafverteidigern dürfte die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten zur Haupttätigkeit gehören. Seit langem umstritten ist, ob **Berufsgeheimnisträger** – insbesondere Anwaltskanzleien – einen DSB bestellen bzw. benennen müssen¹. Weder die RL 95/46/EG noch die DSGVO sehen eine Ausnahme für die Anwaltschaft oder andere Berufsgeheimnisträger vor, so dass auch Art. 37 Abs. 1 lit. b) („*Kerntätigkeit (...) umfangreiche regelmäßige und systematische Überwachung erforderlich*“) und lit. c) („*umfangreichen Verarbeitung besonderer Kategorien von Daten (...) strafrechtliche Verurteilungen und Straftaten*“) DSGVO für die Benennung heranzuziehen sind. Gem. Erwägungsgrund 91 Satz 4 DSGVO soll die Verarbeitung personenbezogener Daten allerdings dann **nicht als umfangreich** gelten, wenn die Verarbeitung personenbezogener Daten von Patienten oder von Mandanten betroffen ist und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt.²

Was eine „aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke umfangreiche regelmäßige und systematische Überwachung“ ist, wird nicht erläutert. In der Literatur³ wird erwähnt, dass z.B. Auskunftfeien und Adresshändler darunter fallen sowie alle Unternehmen, deren Geschäft aus dem Handel mit Daten besteht. Ob auch alle Webseiten-Betreiber, die Analytics bzw. Tracking-Methoden einsetzen, umfangreich regelmäßig und systematisch überwachen, ist nicht klar. Im Ergebnis hat die Regelung in der DSGVO zur Folge, dass viele Unternehmen in der EU eine Pflicht zur Benennung eines DSB trifft. 13

Deutschland hat noch vor Ende der Legislaturperiode 2013-2017 von der Öffnungsklausel (richtiger wohl „Konkretisierungsklausel“) in 14

1 Der Streit entspinnt sich v.a. an § 1 Abs. 3 Satz 2 BDSG und der Frage, ob das BDSG insgesamt für Anwälte Anwendung findet. Dagegen ua. *Rüpke*, AnwBl. 2004, 552; *Rüpke*, NJW 2008, 1121; *Härtig*, AnwBl. 2005, 131; dafür oder differenzierend: *Schneider*, AnwBl. 2004, 618. *Redeker*, AnwBl. 1996, 512. Der DSB selbst ist (ebenfalls) ein Berufsgeheimnisträger (s. § 203 Abs. 2a StGB; am 29.6.2017 hat der Bundestag eine Neuregelung des § 203 StGB beschlossen; der Bundesrat hat am 22.9.2017 entschieden; Einzelheiten siehe Kommentierung bei Rz. 169).

2 S. auch Artikel-29-Gruppe, WP 243 (rev01), Stand: 5.4.2017, S. 7, die auf den großen Graubereich zwischen zwei Extremen hinweist, aber auch dass sich Erwägungsgrund 91 grds. auf die DS-FA bezieht und für DSB nicht unbedingt auf die gleiche Art und Weise Anwendung finden muss; s. auch Artikel-29-Gruppe, WP 248, Stand: 4.4.2017, S. 8.

3 Forgó/Helfrich/Schneider/*Haag*, Betrieblicher Datenschutz, 2. Aufl. 2017, S. 183.

Art. 37 Abs. 4 Satz 1, 2. Halbs. DSGVO Gebrauch gemacht. Gem. § 38 Abs. 1 Satz 1 BDSG 2018¹ müssen **nicht-öffentliche Stellen** (wie bisher) einen DSB benennen, wenn idR mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Auf die Eigenschaft als Arbeitnehmer kommt es nicht an, so dass auch Auszubildende, Teilzeitkräfte und Praktikanten als Beschäftigte gelten. Eine automatisierte Verarbeitung liegt nicht erst dann vor, wenn Kernaufgabe des Beschäftigten die Verarbeitung personenbezogener Daten ist. Vielmehr genügt bspw. schon die Einrichtung eines personalisierten E-Mail-Kontos für die Erfüllung des Tatbestandes.² Unabhängig von der Zahl der Beschäftigten besteht eine Benennungspflicht zudem, wenn Datenverarbeitungen vorgenommen werden, die einer Datenschutz-Folgenabschätzung (DSFA), Art. 35 DSGVO, unterliegen oder wenn Unternehmen personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten, vgl. § 38 Abs. 1 Satz 2 BDSG 2018.

- 15 Gem. Art. 37 Abs. 6 DSGVO kann DSB sowohl ein Beschäftigter des Verantwortlichen oder Auftragsverarbeiters sein oder seine Aufgaben – als externer – auf der „Grundlage eines Dienstleistungsvertrags“ erfüllen. Das gilt nun auch für Behörden. Es kann auch – sofern der DSB von jeder Niederlassung aus leicht erreichbar ist – eine Unternehmensgruppe einen gemeinsamen DSB bestellen (Art. 37 Abs. 2 DSGVO).
- 16 Der Akt der Benennung ist grds. unabhängig von dem zugrundeliegenden Rechtsgeschäft (**Trennungsprinzip**). Beim internen DSB ist dies der Arbeitsvertrag, beim externen DSB ein Geschäftsbesorgungsvertrag. Gerade kleine und mittlere Unternehmen tun sich häufig schwer, einen Beschäftigten als DSB zu bestellen, der einerseits ausreichend fachkundig ist (juristisch, technisch und was die Geschäftsmodelle des Verantwortlichen und des Auftragsverarbeiters betrifft) und andererseits die gesetzlich erforderliche „Zuverlässigkeit“ besitzt, Art. 37 Abs. 5 DSGVO.³ Mit Zuverlässigkeit ist neben persönlicher Integrität und der gesetzlich ausdrücklich vorgesehenen Weisungsunabhängigkeit und dem Benachteiligungsverbot des DSB vor allem verbunden,

1 Regelungen zum Datenschutzbeauftragten öffentlicher Stellen s. § 5–7 BDSG 2018.

2 Der Hessische Datenschutzbeauftragte, Der behördliche und betriebliche Datenschutzbeauftragte nach neuem Recht, Stand: Juni 2017, S. 8.

3 S. auch Beschluss des Düsseldorfer Kreises v. 25.11.2010; *Hallermann*, DuD 2012, 122 ff.

Auftragnehmerfreundlich wäre denkbar, den Vertrag mit dem externen DSB sehr kurz zu gestalten, hinsichtlich Art und Umfang der Tätigkeit auf die gesetzliche Regelung zu verweisen (was für den DSB viele Spielräume lässt) und ansonsten im Wesentlichen Vergütungsfragen, Haftung und Vertragslaufzeit zu regeln.¹ 30

3. AGB-Kontrolle im Datenschutzbereich

In der Literatur² werden bisweilen AGB-Probleme in Verträgen mit internen DSB behandelt (AGB-Kontrolle von Arbeitsverträgen). AGB-widrig können zB folgende Klauseln sein: 31

- Betriebliche Eingliederung/Berichtswege nicht direkt zur Geschäftsleitung
- Interessenkollisionen bei Tätigkeitsbeschreibung/Aufgaben,
- Verfallsklausel unter der Überschrift „Schlussbestimmungen“,
- Schriftform und Salvatorische Klausel.

Inwieweit die Verpflichtung eines externen DSB zu Leistungen, die über seine gesetzlichen Pflichten hinausgehen und im Widerspruch zu seinen gesetzlichen Aufgaben (z.B. wegen Interessenkollision) stehen, AGB-widrig sind (wegen § 307 Abs. 2 Nr. 1 BGB), wird in der Literatur bislang wenig behandelt³. 32

II. Erläuterung der einzelnen Klauseln

1. Erläuterungen des Rubrums

Geschäftsbesorgungsvertrag mit einem externen Datenschutzbeauftragten 33

*(nachfolgend „**dieser Vertrag**“)*

zwischen

1 Ähnlich wohl Koreng/Lachenmann/Kremer/Sander, Formularhandbuch Datenschutzrecht, S. 15 ff.

2 Zum Arbeitsvertrag mit einem DSB nach BDSG aF s. Moos/Weberndörfer/Zieger, Datennutzungs- und Datenschutzverträge, S. 1 ff.

3 Zur Inhaltskontrolle im Datenschutzbereich s. Conrad, Vortrag bei den Kölner Tagen des IT-Rechts 2014, in Köln. Speziell zur Inhaltskontrolle bei Datenschutzerklärung s. LG Berlin v. 30.4.2012 – 15 O 92/12 – Apple; LG Berlin v. 19.11.2013 – 15 O 402/12 – Google.

XYZ GmbH

(nachfolgend „XYZ“ oder „Auftraggeber“)

und

Rechtsanwalt und Dipl. Inf. Max Mustermann

(nachfolgend „der **DSB**“)

a) Vertragspartei auf Seiten des DSB

- 34 DSGVO und BDSG 2018 gehen grundsätzlich davon aus, dass der DSB ein Arbeitnehmer ist. In der DSGVO ergibt sich aus der Klarstellung in Art. 37 Abs. 6 DSGVO, dass alternativ auch ein externer Beauftragter benannt werden kann. Das gilt im Übrigen mangels Differenzierung sowohl für öffentliche als auch für nicht-öffentliche Stellen. Im BDSG 2018 wird das (wie bisher nach § 4f BDSG aF) an der Regelung zur betrieblichen Eingliederung und dem nachwirkenden Kündigungsschutz (§ 38 Abs. 2 iVm. § 6 Abs. 4 Satz 3 BDSG 2018) besonders deutlich. Ist der DSB Arbeitnehmer, ist die Vereinbarung zur Tätigkeit Teil des Arbeitsvertrags. Die Benennung ist wohl – ebenso wie nach BDSG aF die Bestellung – ein davon zu unterscheidendes Rechtsverhältnis. Dessen Beendigung erfolgt ggf. durch Amtsniederlegung.
- 35 Ist der DSB nicht Arbeitnehmer, sind grundsätzlich zwei Konstellationen denkbar¹: In der ersten Konstellation erfolgt der Vertragsschluss (Auftragsverhältnis) mit einer natürlichen Person (wie etwa einem Rechtsanwalt oder Dipl. Inf.), die auch als externer DSB bestellt wird (Personenidentität zwischen dem Vertragspartner des Geschäftsbesorgungsvertrags und dem benannten DSB). Das hier vorgeschlagene Vertragsmuster deckt diese erste Konstellation ab.
- 36 In der zweiten Konstellation – die evtl. sogar häufiger sein dürfte – besteht das Auftragsverhältnis mit einem spezialisierten Dienstleister (also einer juristischen Person, bei der der DSB Gesellschafter oder Arbeitnehmer ist).² Benannt wird dagegen unmittelbar die natürliche Person.

1 Zum ganzen s. Moos/Henkel, Datennutzungs- und Datenschutzverträge, Teil 1 II Rz. 6.

2 Vertragsmuster zu dieser Konstellation s. in Koreng/Lachenmann/Kremer/Sander, Formularhandbuch Datenschutzrecht, A. I. 3.

Inwieweit es zulässig ist, eine juristische Person als DSB zu benennen, war lange umstritten. Die DSGVO hat diesen Streit nicht gelöst.¹ Erwägungsgrund 97 Satz 1 DSGVO sieht zwar im DSB eine weitere Person, die sich insbesondere durch Fachwissen besonders qualifiziert. Bisher wurde dabei vertreten, dass die Merkmale des § 4f Abs. 2 Satz 1 BDSG aF („Fachkunde“ und „Zuverlässigkeit“) jeweils Eigenschaften einer natürlichen Person sind, was wohl zutreffen dürfte.² Die Artikel-29-Datenschutzgruppe hat im Zusammenhang mit Art. 37 Abs. 3 DSGVO (gemeinsamer DSB) allerdings ausdrücklich festgehalten, dass ein DSB auch mit Hilfe eines Teams, tätig werden darf.³ Die Möglichkeit der Benennung externer DSB bedeute, dass auch ein Unternehmen („organisation“) die Aufgaben des DSB ausüben kann, so lange es einen Hauptansprechpartner bestimmt, der für das Unternehmen verantwortlich ist.⁴ Alle Teammitglieder hätten in diesem Fall die Voraussetzungen der DSGVO, insbesondere wohl Unabhängigkeit und Fachwissen zu erfüllen.⁵ Im Vertrag mit dem Dienstleister müsste zudem eine klare Zuordnung der Aufgaben innerhalb des Teams erfolgen und ein einzelner als Hauptansprechpartner bestimmt werden. In Anbetracht der Verpflichtung zur Verschwiegenheit gem. § 38 Abs. 5 iVm. § 6 Abs. 5 Satz 2 BDSG 2018 (flankiert durch § 203 Abs. 2a StGB) muss zudem gewährleistet sein, dass im Zusammenhang mit dem Anrufungsrecht der betroffenen Personen, diese nicht befürchten müssen, dass die von ihnen gemachten Angaben anderen, aber auch solchen, für die keine entsprechende Pflicht besteht, bekannt werden.

Wenn Anwälte das Amt des DSB regelmäßig ausüben, empfiehlt es sich, diese Tätigkeit von der übrigen Kanzleitätigkeit getrennt zu halten und eine gesonderte Gesellschaft zu gründen, um nicht zu riskieren, dass die Einnahmen der Kanzlei insgesamt der Gewerbesteuerpflicht unterliegen. Zudem decken viele Anwaltschaftpflichtversicherungen die Tätigkeit des DSB nicht mit ab, sondern verlangen Zusatzversicherungen. Zur Benennung eines DSB im Konzern s. die Erläuterungen unter Rz. 50 ff.

1 Zur Möglichkeit der Bestellung einer juristischen Person *Laue/Nink/Kremer*, S. 197 Rz. 17; aA: *Helfrich* in Sydow, DSGVO, Art. 37 Rz. 119 mit Verweis auf *Paal* in *Paal/Pauly*, DSGVO, Art. 37 Rz. 15; *Knopp*, DuD 2015, 98 (101).

2 Zum Meinungsstand *Simitis/Simitis*, § 4f BDSG Rz. 48 ff.

3 Artikel-29-Gruppe, WP 243 (rev01), S. 10, 22.

4 Artikel-29-Gruppe, WP 243 (rev01), S. 22.

5 Artikel-29-Gruppe, WP 243 (rev01), S. 22 f.

b) Vertragstyp

- 39 Die Ausübung des Amtes des DSB ist überwiegend eine entgeltliche Geschäftsbesorgung¹. Auch die Tätigkeit als Anwalt dürfte in vielen Fällen als entgeltliche Geschäftsbesorgung einzuordnen sein. Die entgeltliche Geschäftsbesorgung (§ 675 Abs. 1 BGB) ist kein selbständiger Vertragstyp. Vielmehr verdrängt § 675 BGB bei einem Dienst- oder Werkvertrag einzelne Vorschriften und ersetzt sie mit Regelungen aus dem Auftragsrecht. Es entsteht – je nach Einzelfall – ein „Hybrid“ aus Dienstvertrag und Auftrag bzw. aus Werkvertrag und Auftrag). Diese Verweisung auf das Auftragsrecht dient vor allem der Wahrung der Interessen des Auftraggebers.
- 40 Da der Tätigkeit des DSB im Regelfall der Erfolgscharakter fehlt, dürfte sie zumindest überwiegend dienstvertraglich einzuordnen sein. Das gilt jedenfalls für alle gesetzlich normierten Aufgaben (etwa Schulungs- und Prüfungsaufgaben). Werkvertragliche Elemente kommen in Betracht, wenn der DSB – was an sich gesetzlich nicht vorgesehen und daher tendenziell im Hinblick auf die unabhängige Stellung des DSB nicht unkritisch ist (s. Rz. 143 ff.) – überschießende Pflichten hat, etwa die Erstellung des Verarbeitungsverzeichnisses oder umfangreiche Berichts- und Dokumentationspflichten gegenüber der Geschäftsleitung.
- 41 Wo die dienst- bzw. werkvertraglichen Regeln nicht verdrängt werden, gelten sie weiterhin neben dem Auftragsrecht. Wie bei anderen Vertragstypen auch gelten primär die (wirksamen) vertraglichen Vereinbarungen der Parteien, ferner das für die einzelnen Vertragstypen bestehende handels- oder berufsrechtliche Sonderrecht (z.B. BRAO). Erst sekundär gilt nach Maßgabe des § 675 BGB Auftragsrecht. Soweit das Auftragsrecht keine Regelung trifft, gelten Dienst- und Werkvertragsrecht, z.B. hinsichtlich der Vergütung (§§ 612, 632 BGB) oder der Kündigung².

1 Hümmerich/Lücke/Mauer/Lücke, Arbeitsrecht, Muster 23 S. 636 ff.; im Ergebnis wohl auch Koreng/Lachenmann/Kremer/Sander, Formularhandbuch Datenschutzrecht, A. I. 2.

2 Jauernig/Mansel, BGB, 16. Aufl. 2015, § 675 Rz. 9 f.

2. Erläuterung der Präambel

Präambel

42

(1) XYZ ist ein Unternehmen der-Branche, das zum Zeitpunkt des Vertragsschlusses Beschäftigte hat. Die Kern-tätigkeit der XYZ besteht

[Ggf. nähere Konkretisierung der Art der Datenverarbeitung, insbesondere Fälle des § 38 Abs. 1 Satz. 2 BDSG 2018 empfehlenswert; ggf. Verweis auf das Verzeichnis der Verarbeitungstätigkeiten (Verarbeitungsverzeichnis)].

(2) XYZ ist gesetzlich verpflichtet, einen Datenschutzbeauftragten (DSB) zu benennen. XYZ hat sich entschieden, keinen Beschäftigten, sondern einen Externen mit den gesetzlichen Aufgaben und der gesetzlichen Stellung eines DSB für den Datenschutz zu betrauen (siehe § 2).

Alternativ: XYZ ist gesetzlich nicht verpflichtet, einen Datenschutzbeauftragten (DSB) zu benennen. XYZ hat sich aber ohne gesetzliche Verpflichtung entschieden, einen Externen mit den gesetzlichen Aufgaben und der gesetzlichen Stellung eines DSB für den Datenschutz betrauen.

(3) Der DSB ist [z.B. Rechtsanwalt und Diplom-Informatiker] und externer DSB auf Grundlage seiner beruflichen Qualifikation und weist infolge von Ausbildungen und im Bereich des Datenschutzrechts und der Datenschutzpraxis das erforderliche Fachwissen auf. Entsprechende Ausbildungsnachweise [z.B. Zertifikat] liegen der XYZ in Kopie vor. Der DSB verfügt über eine-jährige Berufserfahrung als [z.B. Fachanwalt für Informations-technologierecht und als externer DSB]. Ausweislich seines Angebots vom hat der DSB Referenzen von Mandanten aus der-Branche, die der DSB speziell auch in Datenschutzmandaten beraten hat. Der DSB kann somit auf optimierte Standard-Prozesse und Musterdokumente im Hinblick auf die Aufgaben als externer DSB zurückgreifen. Zur Fachkunde und Zuverlässigkeit siehe auch § 3.

(4) Im Hinblick auf die Vermeidung etwaiger Interessenkollisionen erklärt der DSB, dass er vor Abschluss dieses Vertrages noch nicht für XYZ tätig war, insbesondere nicht als [z.B. Rechtsanwalt in datenschutz- oder IT-vertragsrechtlichen Mandaten]. Der DSB ist auch nicht Mitgesellschafter oder stiller Teilhaber der XYZ und steht oder stand auch sonst in keinem Verhältnis zu XYZ, das mit dem Amt als DSB aufgrund Interessenkollision inkompatibel wäre.

(5) Dieser Vertrag regelt das der Benennung zugrundeliegende Auftragsverhältnis und konkretisiert und präzisiert individuell für die Unternehmenssituation beim XYZ die gesetzlichen Aufgaben des DSB und die Pflichten der XYZ im Hinblick auf die Stellung des DSB und die Unterstützung durch XYZ.

a) Ratio

43 In der Präambel können die Rahmenbedingungen bzw. Geschäftsgrundlagen der Aufgabenerfüllung durch den DSB kurz angesprochen werden. Dazu gehören insbesondere:

- Beschäftigtenzahl und somit Größe des Auftraggebers (in seiner Funktion als Verantwortlicher oder Auftragsverarbeiter),
- Branche des Auftraggebers (mit Hinweis auf sensible Datenkategorien iS von Art. 9 Abs. 1 DSGVO)
- Verflechtung im Konzern (evtl. Datenübermittlungen ins Ausland; Prüfung der Erforderlichkeit/Möglichkeit eines gemeinsamen DSB gem. Art. 37 Abs. 2 DSGVO).

Aus diesen Rahmenbedingungen ergeben sich regelmäßig Indikationen für die erforderlichen Spezialkenntnisse des DSB und für den regelmäßig erforderlichen Zeitaufwand, der für Regelaufgaben des DSB voraussichtlich anzusetzen ist.¹

b) Erläuterungen zu Präambel Abs. 1 (Art der Datenverarbeitung und Verantwortlicher)

44 Gegenstand der Präambel ist zunächst die Konkretisierung der Art der Datenverarbeitung, um den Vertragsparteien eine Vorstellung vom Schutzbedarf hinsichtlich der personenbezogenen Daten zu ermöglichen. Denn verarbeiten Unternehmen zB **besondere Arten von personenbezogenen Daten** (Art. 9 Abs. 1 DSGVO), so gelten sowohl für den Verantwortlichen bzw. Auftragsverarbeiter, aber auch den DSB sehr hohe Anforderungen. Es muss in diesem Falle die Ordnungsmäßigkeit der Datenverarbeitung in vollstem Maße gewährleistet sein,

¹ S. ArbG Offenbach (RDV 1993, 63), das im Jahr 1993 davon ausging, dass bei einem Betrieb mit knapp 300 Mitarbeitern die Aufgabe des DSB mit idR 20% der Tätigkeit eines vollzeitbeschäftigten Angestellten wahrgenommen werden kann. Mittlerweile dürfte aufgrund der stark angestiegenen Durchdringung aller Unternehmen durch IT und wachsender Komplexität der IT (Smart Devices, Cloud, Big Data etc.) der zeitliche Aufwand eher gestiegen sein.