

Hamburg

Ob eine Pflicht besteht einen Datenschutzbeauftragten (bDSB) zu bestellen, hängt zunächst vom Tatbestand des Art. 37 DSGVO ab sowie § 38 BDSG n.F. Letzterer eröffnet sodann den Regelungsrahmen des Art. 35 DSGVO und bestimmt, dass ein bDSB erforderlich ist, wenn auch eine DSFA notwendig ist.

Nach Art. 37 Abs. 1 lit c) DSGVO besteht die Pflicht, wenn die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten nach Art. 9 DSGVO besteht. Kerntätigkeit ist dabei die Haupttätigkeit eines Verantwortlichen, die es untrennbar prägt, und nicht die Verarbeitung personenbezogener Daten als Nebentätigkeit (ErwG 97). Zu den Kerntätigkeiten gehören danach auch alle Vorgänge, die einen festen Bestandteil der Haupttätigkeit des Verantwortlichen darstellen. Hierzu gehören nicht die das Kerngeschäft unterstützenden Tätigkeiten wie z. B. die Verarbeitung der Beschäftigendaten der eigenen Mitarbeiter.

Für die Definition des Begriffs "umfangreich" können aus ErwGr 91 der DS-GVO folgende Faktoren herangezogen werden:

- Menge der verarbeiteten personenbezogenen Daten (Volumen),
- Verarbeitung auf regionaler, nationaler oder supranationaler Ebene (geografischer Aspekt),
- Anzahl der betroffenen Personen (absolute Zahl oder in Prozent zur relevanten Bezugsgröße) und
- Dauer der Verarbeitung (zeitlicher Aspekt).

Sind mehrere Faktoren hoch, so kann dies für eine "umfangreiche" Überwachung bzw. Verarbeitung sprechen. Erfolgt eine Verarbeitung von Patienten- oder Mandantendaten durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufs oder Rechtsanwalt, handelt es sich regelmäßig nicht um eine die Benennungspflicht auslösende umfangreiche Datenverarbeitung (siehe ErwGr. 91).

Vgl. insoweit Kurzpapier Nr. 12 der DSK, abrufbar unter: https://www.datenschutz-hamburg.de/news/detail/article/kurzpapiere-der-dsk-zur-dsgvo.html?tx_ttnews%5BbackPid%5D=209&cHash=44a1ecec5c99eca9229232a027633d8f

Insofern ist es zweifelhaft, ob dies für die von Ihnen benannten (Einzel)Versicherungsmakler gilt. Eine generelle Beurteilung lässt sich allerdings kaum vornehmen. Entscheidend ist vielmehr die konkrete Einzelfallsituation. Wir möchten auch betonen, dass eine ‚Blacklist‘, bzw. eine ‚Whitelist‘ bisher nicht besteht, bzw. sich derzeit in Erstellung befindet (Blacklist zur DSFA). Daher kann die Einordnung bis dato nur als vorläufig betrachtet werden.

Eine Personalunion von Datenschutzbeauftragter und Einzelunternehmer ist aufgrund des damit verbundenen Interessenkonflikts nicht möglich.

<p>Berlin</p>	<p>in Ihrem Beispielfall ist kein betrieblicher Datenschutzbeauftragter zu benennen, da keine umfangreiche Verarbeitung besonderer Kategorien von Daten gemäß Art. 9 Datenschutz-Grundverordnung vorliegt.</p> <p>Falls ein Versicherungsmakler aus anderen Gründen einen betrieblichen Datenschutzbeauftragten ernennen muss, etwa weil 10 Personen Zugang zu personenbezogenen Daten haben, kann er diese Aufgabe nicht selbst ausüben, da ein Interessenkonflikt vorliegt.</p>
<p>Bayern</p>	<p>wir vertreten für unseren Zuständigkeitsbereich (Bayern) nicht die Auffassung, dass einzelne Versicherungsmakler oder Finanzanlagenvermittler eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne von Art. 37 Abs. 1 lit. c DS-GVO durchführen und deshalb immer einen DSB benennen müssen. Siehe dazu auch Nr. 2.1.3 im WP 243, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048 , wonach z. B. auch ein einzelner Arzt oder Rechtsanwalt hier nicht dazu gezählt wird.</p> <p>Für Versicherungsmakler und Finanzanlagenvermittler kommt es für uns folglich auf die Beschäftigtenanzahl gemäß § 38 BDSG-neu an (10-Personen-Grenze). Der Inhaber selbst kann dabei nicht auch gleichzeitig DSB sein (unzulässige Interessenkollision).</p>
<p>Saarland</p>	<p>Halten sich uns gegenüber für örtlich nicht zuständig</p>
<p>Mecklenburg-Vorpommern</p>	<p>verweisen auf Hamburg</p>

Hessen

Wie bei vielen anderen Themen, die sich aus der Datenschutz-Grundverordnung (DSGVO) ergeben, arbeiten die Datenschutzaufsichtsbehörden der EU-Mitgliedstaaten zur Frage der Bestellpflicht eines Datenschutzbeauftragten an Auslegungshilfen. Die Verabschiedung von Leitlinien durch die Artikel-29-Gruppe, ein Arbeitsgremium der Datenschutzaufsichtsbehörden auf europäischer Ebene, ist mit dem Workingpaper 243 (WP 243; abrufbar unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083) erfolgt. Die Diskussionen zu dieser Frage befinden sich dennoch im Anfangsstadium, so dass wir um Verständnis bitten, dass wir Ihnen hierzu derzeit noch keine abschließende Position zukommen lassen können, zumal es künftig bei praktisch allen wichtigen Fragestellungen der DSGVO auf die Auslegung durch den Europäischen Datenschutzausschuss (EDSA) ankommt; ebendieser Festlegung von Leitlinien des künftigen EDSA diene die o.g. geplante Erarbeitung von Leitlinien des „Vorläufergremiums“ Artikel-29-Gruppe. Die folgenden Ausführungen sind daher nur eine vorläufige Einschätzung der Rechtslage.

Mit Wirksamwerden der DSGVO am 25. Mai 2018 gelten für die Bestellpflicht von Datenschutzbeauftragten Artikel 37 DSGVO und § 38 BDSG-neu i.V.m. Artikel 35 DSGVO.

Ergänzend zu den Bestellpflichten des Artikel 37 Abs. 1 DSGVO hat der deutsche Gesetzgeber über die Öffnungsklausel des Artikel 37 Abs. 4 Satz 1 DSGVO für die Benennung betrieblicher Datenschutzbeauftragter nationale Sonderregelungen geschaffen und sich dafür entschieden, das bereits aus dem deutschen Recht bekannte Kriterium der quantitativen Bestellpflicht beizubehalten (vgl. § 38 BDSG-neu). Somit ist auch künftig ein Datenschutzbeauftragter zu benennen, wenn in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Die Pflicht zur Bestellung eines Datenschutzbeauftragten kann sich in Deutschland künftig aus einem der folgenden fünf Umstände ergeben:

1. regelmäßig sind mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 38 Abs. 1 Satz 1 BDSG-neu)
2. Verantwortlicher ist eine öffentliche Stelle oder Behörde (Artikel 37 Abs. 1 lit. a DSGVO)
3. die Kerntätigkeit umfasst die umfangreiche Verarbeitung besonderer Kategorien von Daten oder strafrechtlicher Verurteilungen (Artikel 37 Abs. 1 lit.c DSGVO)
4. es ist eine Datenschutz-Folgenabschätzung durchzuführen (§ 38 Abs. 1 Satz 2 BDSG-neu)
5. die Kerntätigkeit ist die umfangreiche oder systematische Überwachung von betroffenen Personen (Artikel 37 Abs. 1 lit. b DSGVO).

Sind weniger als zehn Mitarbeiter mit der Verarbeitung personenbezogener Daten beschäftigt, besteht nach § 38 Abs. 1 Satz 2 BDSG-neu eine Benennungspflicht, wenn der Verantwortliche oder der Auftragsverarbeiter einer Datenschutz-

Folgenabschätzung nach Artikel 35 der DSGVO unterliegt oder aber personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden.

Meist werden die Ziffern 2, 4 und 5 nicht erfüllt sein. Dies ist selbstverständlich im Einzelfall zu prüfen. Im Ergebnis wird es wie bisher in der Regel auf die unter Ziff. 1 genannte Zehn-Personen-Grenze ankommen, wenn beurteilt werden soll, ob ein Leistungserbringer im Gesundheitswesen einen Datenschutzbeauftragten bestellen muss. Darüber hinaus kann aber auch das Erfordernis einer Datenschutz-Folgenabschätzung eine Bestellpflicht begründen.

Wann eine Datenschutz-Folgenabschätzung erforderlich ist, muss vom Verantwortlichen im Einzelfall geprüft werden. Sie ist nach Artikel 35 Abs. 3 lit. b DSGVO insbesondere bei der umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten, wozu u.a. Gesundheitsdaten zählen, notwendig. Wann die Grenze zur umfangreichen Verarbeitung überschritten ist, wird derzeit sehr unterschiedlich gesehen. Wir streben aber noch in 2018 eine bundesweite Klärung unter den Datenschutzaufsichtsbehörden dieser Frage für Arztpraxen, Gesundheitshandwerk, Apotheken, Physiotherapeuten und auch Versicherungsbüros an.

Wir gehen derzeit bei kleineren Einheiten, bei denen keine Sonderkonstellationen vorliegen, nicht von einer umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten aus. Grundsätzlich ist es von der DSGVO nicht gewollt, dass jede kleine Arztpraxis oder Apotheke einen Datenschutzbeauftragten bestellen oder eine Datenschutz-Folgenabschätzung durchführen muss, nur weil Gesundheitsdaten verarbeitet werden (siehe auch die vergleichbare Bewertung zur Datenschutz-Folgenabschätzung in ErwGr. 91 Satz 4 zu Artikel 35 Abs. 3 lit. b DSGVO sowie Nr. 2.1.3 des WP 243 der Artikel 29-Gruppe unter http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 bzw. http://ec.europa.eu/newsroom/document.cfm?doc_id=44100).

Diese Regel kann allerdings widerlegt sein, wenn eine Datenschutz-Folgenabschätzung und damit auch die Bestellung eines Datenschutzbeauftragten aus anderen Gründen als der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten, beispielsweise wegen der Art der Verarbeitung oder der Nutzung von besonderen Kommunikationswegen erforderlich ist.

Größere Einheiten, wie Krankenhäuser führen in jedem Fall auch nach dem WP 243 eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten durch und sind daher sowohl zur Durchführung einer Datenschutz-Folgenabschätzung als auch zur Bestellung eines Datenschutzbeauftragten verpflichtet. Hinsichtlich der 10-Personengrenze stellt § 38 BDSG-neu nicht nur auf Mitarbeiter ab. Dies entspricht der bisherigen Praxis der Aufsichtsbehörden. Weil wir bisher bei der 10-Beschäftigten-Grenze auch den Arzt, Apotheker, Steuerberater, Versicherungsvermittler usw. als Chef der Praxis/Kanzlei mitgezählt haben (nach der BDSG-Änderung zur DSB-Bestellpflicht im Jahre 2006 mit Ersetzung der

	<p>Begrifflichkeit „beschäftigte Arbeitnehmer“ durch „beschäftigte Personen“, wie auch manche andere Aufsichtsbehörde), ist wie bisher ein Datenschutzbeauftragter ab 9 Mitarbeitern zu bestellen.</p> <p>Zusammenfassend kommt man hiernach für Gesundheitsberufe und Versicherungsunternehmen zu folgendem Ergebnis:</p> <ol style="list-style-type: none"> 1. Verantwortliche mit zehn oder mehr Beschäftigten müssen wie bisher einen Datenschutzbeauftragten benennen (vgl. Artikel 37 Abs. IV Satz 1 DSGVO i.V.m. § 38 Abs. 1 Satz 1 BDSG-neu). 2. Verantwortliche, bei denen nur eine Person tätig ist, müssen, wenn keine Sonderkonstellation vorliegt, in der Regel keinen Datenschutzbeauftragten benennen (vgl. für den Fall des Artikel 37 Abs. IV Satz 1 DSGVO i.V.m. § 38 Abs. 1 Satz 2 BDSG-neu und für den Fall des Artikel 37 Abs. 1 lit. c DSGVO vor allem Erwägungsgrund 91). 3. Verantwortliche mit weniger als zehn Beschäftigten, bei denen aber mehr als eine Person tätig ist, müssen bei Erfüllung folgender Voraussetzungen einen Datenschutzbeauftragten benennen: <ol style="list-style-type: none"> a. Die Datenverarbeitungen unterfallen einer Datenschutz-Folgenabschätzung nach § 38 Abs. 1 Satz 2 BDSG-neu (hier wären also die Voraussetzungen des Artikel 35 DSGVO zu prüfen). b. Es ist nach Artikel 37 Abs. 1 lit. c DSGVO von einer umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 DSGVO auszugehen. c. Es liegt nach Artikel 37 Abs. 1 lit b DSGVO eine umfangreiche regelmäßige und systematische Überwachung vor. <p>Daher sind sämtliche vorstehend beschriebenen Fälle an Hand einer Einzelfallprüfung zu bewerten und zu entscheiden. Hierzu können zum einen die zuvor genannten Kriterien herangezogen werden. Darüber hinaus kann es sinnvoll sein, die Ausführungen der Artikel-29-Datenschutzgruppe zum Thema Datenschutz-Folgenabschätzung zu beachten. In Zweifelsfällen sollte aus Gründen der Rechtssicherheit und vor dem Hintergrund der deutlich verschärften Sanktionen ab Inkrafttreten der Verordnung am 25. Mai 2018 vom Bestehen einer Benennungspflicht ausgegangen werden.</p>
<p>Brandenburg</p>	<p>Sehen sich bisher als für uns örtlich nicht zuständig an</p>

<p>Thüringen</p>	<p>Bitten um Geduld</p>
<p>Niedersachsen (Antwort direkt an einen Einzelmakler)</p>	<p>Da Sie ein selbständiger Versicherungsmakler nach § 94 HGB mit nur einer Beschäftigten sind, liegen Sie unter der Grenze des § 38 Bundesdatenschutzgesetz neu (BDSG neu) von 10 Personen und müssen daher keinen Datenschutzbeauftragten (DSB) benennen.</p> <p>Auch nach Art. 37 Abs. 1 c) Datenschutzgrundverordnung (DS-GVO) sind Sie nicht verpflichtet einen DSB zu benennen. In Ihrer Kerntätigkeit (siehe dazu auch Erwägungsgrund 97), beschäftigen Sie sich nicht in ihrer Hauptaktivität mit Datenverarbeitung in einer umfangreichen Verarbeitung besonderer personenbezogener Daten (z.B. Gesundheitsdaten). Erwägungsgrund 91 erläutert "umfangreiche Verarbeitungsvorgänge" . Hier spricht das Gesetz von großen Mengen personenbezogener Daten die eine große Zahl von Personen betreffen können und ein hohes Risiko bei der Verarbeitung wahrscheinlich ist. Mögliche Anhaltspunkte für eine umfangreiche Verarbeitung</p> <ul style="list-style-type: none"> - Einsatz umfangreicher digitaler Medizinprodukte - Auswertung von Patientendaten durch Auftragnehmer im Ausland (auch USA) - Intensive Nutzung telemedizinischer Anwendungen - Einsatz von Videotechnik im Behandlungsverfahren (z.B. bei Psychiatern) - Große (aber unter 10 Personen) Hausarzt, Kinderarzt oder internistische Praxen, welche einen Generationsübergreifenden Datenbestand zu einer Person / Familie haben - Überproportional großer Patientenstamm im Vergleich zu anderen Praxen selber Ausrichtung und Größe - Nutzen von Big Data Anwendungen - Begleitende Forschungstätigkeit (Erhebung (auch mit Einwilligung) von mehr Daten, als zur Behandlung erforderlich sind) <p>Unabhängig von einer DSB-Bestellungspflicht, haben Sie die DSGVO zu beachten, da dies ein umfangreiches und für einen Laien meist unverständliches Regelwerk ist, kann es von Vorteil sein, sich Rat von einem externen DSB zu holen.</p> <p>Hilfreich sind auch die auf meiner Homepage https://www.lfd.niedersachsen.de/startseite/dsgvo/anwendung_dsgvo_kurzpapiere/ds-gvo---kurzpapiere-155196.html eingestellten Kurzpapiere bzw. die Hinweise zum Verzeichnis der Verarbeitungstätigkeiten https://www.lfd.niedersachsen.de/themen/wirtschaft/verfahrensverzeichnis_und_verfahrensregister_nach_bdsb/verfahrensregister-und-verfahrensbeschreibung-fuer-den-nicht-oeffentlichen-bereich-56247.html</p>