Praxisratgeber

Die/der Beauftragte für den Datenschutz

Teil I:

In welchen Fällen muss ein Datenschutzbeauftragter benannt werden?

Ein Überblick über die rechtlichen Voraussetzungen hinsichtlich der Benennung eines betrieblichen oder behördlichen Datenschutzbeauftragten

2. Auflage, November 2019

Herausgegeben
vom Landesbeauftragten
für den Datenschutz und die Informationsfreiheit
Dr. Stefan Brink
Mitautor: Christian Storr
Königstraße 10a, 70173 Stuttgart
Telefon 0711/615541-0
https://www.baden-wuerttemberg.datenschutz.de
E-Mail: poststelle@lfdi.bwl.de
PGP Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962

Inhalt

Benutzungshinweis

Der vorliegende Praxisratgeber stellt eine zusammenfassende Information über das Thema Datenschutzbeauftragter nach der Datenschutz-Grundverordnung (DS-GVO) und nach dem neuen Bundesdatenschutzgesetz (BDSG) dar. Er soll die Umsetzung der neuen Regelungen erleichtern und Hilfestellung bieten.

Angesichts des Umstands, dass es sich in weiten Teilen um eine neue Rechtsmaterie handelt, stellt dieses Papier keine abschließende Information dar, welche die Datenschutzaufsichtsbehörde in allen Verfahren binden könnte, sondern spiegelt den Kenntnis- und Erfahrungsstand zum Zeitpunkt der Veröffentlichung wider.

Der Praxisratgeber wird regelmäßig einer Evaluierung und Aktualisierung unterzogen, um neue Entwicklungen und Erkenntnisse (v.a. durch den Europäischen Datenschutzausschuss, durch Beschlüsse der Konferenz der Datenschutzaufsichtsbehörden sowie durch einschlägige Rechtsprechung) einbeziehen zu können.

I. Wer muss eine(n) Datenschutzbeauftragte(n) benennen?

Die Voraussetzungen, die zur Pflicht führen, einen betrieblichen oder behördlichen Datenschutzbeauftragten[1] (DSB) zu benennen, sind seit dem 25. Mai 2018 in zwei Vorschriften geregelt: In **Art. 37 Abs. 1 der EU-Datenschutz-Grundverordnung (DS-GVO) sowie in §§ 5, 38 des Bundesdatenschutzgesetzes (BDSG)**.

Diese Pflicht trifft – beim Vorliegen der jeweiligen gesetzlichen Voraussetzungen (siehe Abschnitt II.) – den **Verantwortlichen** und den **Auftragsverarbeiter**.

„**Verantwortlicher**“ ist nach Art. 4 Nr. 7 DS-GVO die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

„**Auftragsverarbeiter**“ ist nach Art. 4 Nr. 8 DS-GVO eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Art. 37 gilt im Hinblick auf die Benennung eines DSB gleichermaßen für Verantwortliche und Auftragsverarbeiter. Je nachdem, wer die Kriterien für eine zwingend vorgeschriebene Benennung erfüllt, muss einen Datenschutzbeauftragten benennen. Auch dann, wenn der Verantwortliche die Kriterien für eine obligatorische Benennung eines DSB erfüllt, gilt dies daher nicht zwangsläufig auch für dessen Auftragsverarbeiter. Das bedeutet zum Beispiel, dass nicht automatisch jeder Auftragsverarbeiter einer Behörde, die nach Art. 37 Abs. 1 Buchst. a DS-GVO immer einen DSB benennen muss, auch einen eigenen DSB benennen muss, sondern nur dann, wenn auch er selbst als Auftragsverarbeiter einen der Tatbestände von Art. 37 DS-GVO oder § 38 BDSG erfüllt.

Zu den **verpflichteten natürlichen oder juristischen Personen im nicht-öffentlichen Bereich** zählen insbesondere

- natürliche Personen als Selbständige oder freie Unternehmer bzw. Handwerker und Kaufleute (z.B. Ärzte, Apotheker, Rechtsanwälte, Steuerberater, Handels-, Handwerks- und Industriebetriebe usw.)
- juristische Personen (z. B. als GmbH organisierte Auskunfteien, Markt- und Meinungsforschungsinstitute, Telefondienste, Adressverlage, Detekteien, Handels-, Handwerks- und Industriebetriebe, als Kommanditgesellschaft auf Aktien konstituierte Banken, als Aktiengesellschaften tätige Kliniken, eingetragene Vereine, rechtsfähige Stiftungen des bürgerlichen Rechts)

[1] Wenn bei bestimmten Begriffen, die sich auf Personengruppen beziehen, nur die männliche Form gewählt wurde, so ist dies nicht geschlechtsspezifisch gemeint, sondern geschah ausschließlich aus Gründen der besseren Lesbarkeit.

- Personengesellschaften (z. B. ein als Gesellschaft des bürgerlichen Rechts organisiertes Baukonsortium, ein als GmbH & Co. KG agierendes Versandunternehmen oder Servicerechenzentrum, eine Anwaltssozietät als Partnerschaftsgesellschaft oder ein als OHG auftretender Filmverleih)
- Nicht rechtsfähige Vereinigungen (z. B. Parteien, Vereine, Gewerkschaften und Berufsverbände).

II. In welchen Fällen muss ein Datenschutzbeauftragter benannt werden?

Nach **Art. 37 Abs. 1 der DS-GVO sowie § 38 BDSG** besteht seit dem 25. Mai 2018 **in den folgenden sechs Fallkonstellationen** jeweils die Pflicht, einen Datenschutzbeauftragten zu benennen (das Vorliegen nur einer Konstellation genügt bereits):

<u>Übersicht</u>: Obligatorische Benennung **Sechs Fallkonstellationen, welche die Pflicht begründen, einen behördlichen oder betrieblichen Datenschutzbeauftragten zu benennen:**
1. Verantwortlicher ist eine **<u>öffentliche Stelle oder Behörde</u>** (Art. 37 Abs. 1 Buchst. a DS-GVO). *Hier muss immer ein Datenschutzbeauftragter benannt werden.*
2. Die **<u>Kerntätigkeit</u>** besteht in der **<u>umfangreichen oder systematischen Überwachung</u>** von betroffenen Personen (Art. 37 Abs. 1 Buchst. b DS-GVO). *Achtung: Überwachung meint nicht nur Videoüberwachung, Detekteien und private Sicherheitsunternehmen, sondern z.B. auch die Nachverfolgung des Surfverhaltens im Internet oder des Kaufverhaltens durch ein Treueprogramm.*
3. Die **<u>Kerntätigkeit</u>** umfasst die **<u>umfangreiche Verarbeitung besonderer Kategorien von Daten oder strafrechtlicher Verurteilungen</u>** (Art. 37 Abs. 1 Buchst. c DS-GVO).
4. Regelmäßig sind **<u>mindestens 20 Personen</u>** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 38 Abs. 1 S. 1 BDSG).

Bitte beachten: Die Leitung des Verantwortlichen (Geschäftsführer/in, Chef/Chefin, Inhaber/in, Partner usw.) bzw. des Auftragsverarbeiters wird hierbei immer hinzugerechnet.

5. Es ist eine **Datenschutz-Folgenabschätzung** durchzuführen (§ 38 Abs. 1 S. 2 1. HS BDSG in Verbindung mit Art. 35 DS-GVO).

6. Es werden personenbezogene **Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung** verarbeitet (§ 38 Abs. 1 S. 2 2. HS BDSG).

   In diese Gruppe gehören insbesondere Wirtschaftsauskunfteien, Adresshändler sowie Markt- und Meinungsforschungsinstitute.

Bei neuen Datenverarbeitungsvorgängen oder dem Hinzukommen neuer Geschäftsfelder oder anderen Veränderungen, die sich auf die Datenverarbeitung auswirken, ist stets neu zu prüfen, ob eine der o.g. Fallgruppen einschlägig ist. Umgekehrt kann die Pflicht zur Benennung durch entsprechende Veränderungen des Geschäftsfeldes und/oder bei der Datenverarbeitung natürlich auch wieder entfallen.

1. Verantwortlicher ist eine öffentliche Stelle oder Behörde (Art. 37 Abs. 1 Buchst. a DS-GVO).

Behörden – außer Gerichte, die im Rahmen ihrer justiziellen Tätigkeit handeln[2] – und öffentliche Stellen müssen **immer** einen Datenschutzbeauftragten bestellen. Behörde ist nach § 1 Abs. 2 des Landesverwaltungsverfahrensgesetzes (LVwVfG) jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt.

Dem Working Paper 243 rev. 01 des Europäischen Datenschutzausschusses ist zu entnehmen, dass sich die Auslegung der Begriffe Behörde und öffentliche Stelle nach dem jeweiligen Recht des Mitgliedstaates richtet. Daher sind hier § 2 Abs. 2, 3 BDSG und § 2 des Landesdatenschutzgesetzes (LDSG) heranzuziehen. Danach gilt:

[2] Siehe Artikel 32 der Richtlinie (EU) 2016/680; § 7 Abs. 1 S. 2 BDSG stellt klar, dass die Aufgaben eines behördlichen Datenschutzbeauftragten eines Gerichts sich nicht auf das Handeln des Gerichts im Rahmen seiner justiziellen Tätigkeit beziehen.

Öffentliche Stellen sind Behörden und sonstige Stellen des Landes, der Gemeinden und Gemeindeverbände und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts. Als öffentliche Stellen gelten nach § 2 Abs. 2 LDSG auch juristische Personen und sonstige Vereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen und an denen eine oder mehrere der in Absatz 1 genannten juristischen Personen des öffentlichen Rechts mit absoluter Mehrheit der Anteile oder absoluter Mehrheit der Stimmen beteiligt sind. Beteiligt sich eine juristische Person oder sonstige Vereinigung des privaten Rechts nach Satz 1 an einer weiteren Vereinigung des privaten Rechts, findet § 2 Abs. 2 S. 1 LDSG entsprechende Anwendung.

Nehmen nicht-öffentliche Stellen hoheitliche Aufgaben der öffentlichen Verwaltung wahr (sog. **Beliehene**), sind sie insoweit **öffentliche Stellen** im Sinne dieses Gesetzes. Eine öffentliche Aufgabe und öffentliche Gewalt kann nämlich nicht nur von öffentlichen Einrichtungen und Stellen wahrgenommen bzw. ausgeübt werden, sondern auch von jeglicher natürlichen oder juristischen Person, die – je nach den Bestimmungen des betreffenden Mitgliedstaates – in Bereichen wie etwa dem öffentlichem Transportwesen, der Wasser- und Energieversorgung, der Verkehrsinfrastruktur, dem öffentlich-rechtlichen Rundfunk, dem sozialen Wohnungsbau oder den Disziplinarkommissionen für reglementierte Berufe öffentlichem oder privatem Recht unterliegt.

Soweit öffentliche Stellen als Unternehmen mit eigener Rechtspersönlichkeit am Wettbewerb teilnehmen, sind – außer für Zweckverbände – gemäß § 2 Abs. 6 LDSG die für nicht-öffentliche Stellen geltenden datenschutzrechtlichen Vorschriften entsprechend anzuwenden.

Nach Art. 37 Abs. 3 DS-GVO können Behörden, je nach Organisationsstruktur und Größe, einen **gemeinsamen Datenschutzbeauftragten** benennen.

2. Die Kerntätigkeit besteht in der umfangreichen regelmäßigen und systematischen Überwachung von betroffenen Personen (Art. 37 Abs. 1 Buchst. b DS-GVO)

Der Begriff der umfangreichen regelmäßigen und systematischen Überwachung ist in der DS-GVO zwar nicht definiert, doch das Konzept einer „Beobachtung des Verhaltens von betroffenen Personen“ wird in Erwägungsgrund (ErwGr) 24 der DS-GVO erwähnt und **erstreckt sich demnach eindeutig auf jede Form der Verfolgung und Profilerstellung im Internet (siehe Art. 22 DS-GVO), darunter auch zu Zwecken der verhaltensbasierten Werbung**.

Gleichwohl beschränkt sich der Begriff der Überwachung nicht auf die Online-Umgebung, weshalb die Online-Verfolgung nur als ein Beispiel für die Überwachung des Verhaltens von betroffenen Personen angesehen werden sollte.

In Anlehnung an den Europäischen Datenschutz-Ausschuss[3] ist der Begriff **„regelmäßig“** als mindestens eine der folgenden Eigenschaften zu interpretieren:

- fortlaufend oder in bestimmten Abständen während eines bestimmten Zeitraums vorkommend;
- immer wieder oder wiederholt zu bestimmten Zeitpunkten auftretend;
- ständig oder regelmäßig stattfindend.

Der Begriff **„systematisch“** ist als mindestens eine der folgenden Eigenschaften auszulegen:

- systematisch vorkommend;
- vereinbart, organisiert oder methodisch;
- im Rahmen eines allgemeinen Datenerfassungsplans erfolgend;
- im Rahmen einer Strategie erfolgend.

Beispiele für eine regelmäßige und systematische Überwachung von betroffenen Personen:

Betrieb eines Telekommunikationsnetzes, Anbieten von Telekommunikationsdienstleistungen, verfolgende E-Mail-Werbung, **Internet-Trackingprogramme**, datengesteuerte Marketingaktivitäten, Typisierung und **Scoring** zu Zwecken der Risikobewertung (zum Beispiel zu Zwecken der Kreditvergabe, der Festlegung von Versicherungsprämien, Maßnahmen zur Verhinderung von betrügerischen Handlungen, Ermittlung von Geldwäsche), **Standortverfolgung** (beispielsweise durch Mobilfunkanwendungen), Treueprogramme, Nachverfolgung über ÖPNV-Netzkarten, verhaltensbasierte Werbung, Überwachung von Wellness-, Fitness- und gesundheitsbezogenen Daten durch sog. Wearables, **Überwachungskameras** oder vernetzte Geräte (zum Beispiel intelligente Stromzähler, intelligente Autos, Haustechnik usw.).

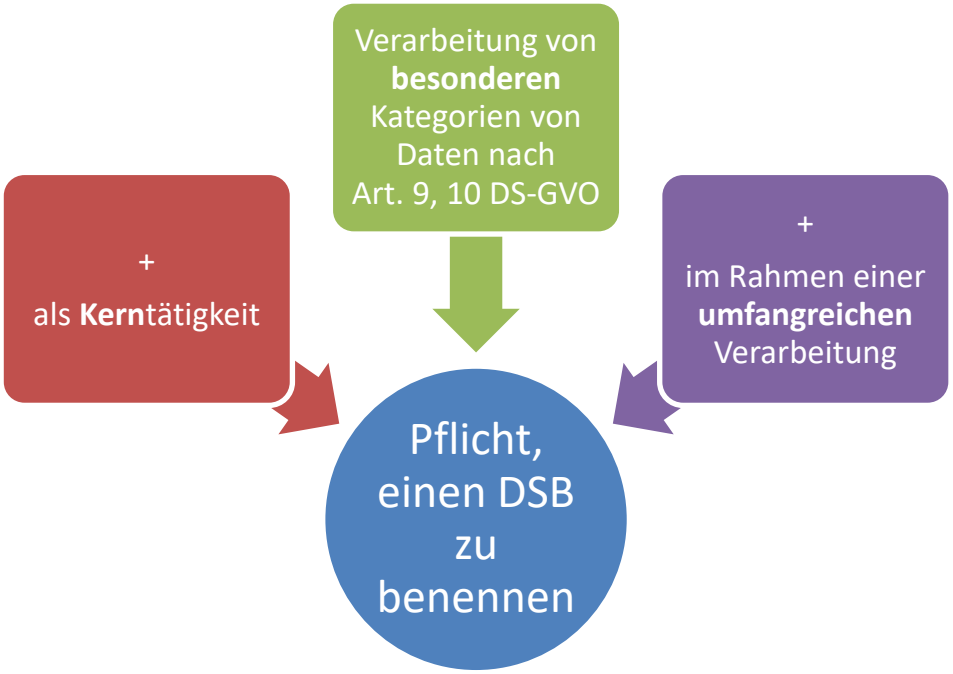
3. Die Kerntätigkeit umfasst die umfangreiche Verarbeitung besonderer Kategorien von Daten oder strafrechtlicher Verurteilungen (Art. 37 Abs. 1 Buchst. c DS-GVO)

Es müssen in Ihrem Unternehmen (bzw. Betrieb, Praxis, Kanzlei, Verein, Partei usw.) also die Tatbestände

[3] Siehe Working-Paper Nr. 243 rev. 01

1. Verarbeitung von besonderen Kategorien von Daten nach Art. 9, 10 DS-GVO
2. als Kerntätigkeit und
3. im Rahmen einer umfangreichen Verarbeitung

kumulativ gegeben sein, um nach dieser Vorschrift die - risikobasierte - Benennungspflicht auszulösen.



a) Verarbeitung von besonderen Kategorien von Daten

Besondere Kategorien von Daten nach Art. 9 Abs. 1 DS-GVO sind u.a.

- Gesundheits- und Patientendaten,
- Daten, aus denen die rassische oder ethnische Herkunft hervorgeht,
- Daten, aus denen politische Meinungen hervorgehen,
- Daten, aus denen religiöse oder weltanschauliche Überzeugungen hervorgehen,
- Daten, aus denen die Gewerkschaftszugehörigkeit hervorgeht,
- genetische Daten,
- biometrische Daten zur eindeutigen Identifizierung,
- Daten zum Sexualleben sowie zur sexuellen Orientierung.

Hinzu kommen nach Art. 10 DS-GVO

- Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln.

b) Verarbeitung von besonderen Kategorien von Daten ist Kerntätigkeit

Zum Begriff der „Kerntätigkeit“ führt ErwG 97 S. 2 der DS-GVO aus:

> *„Im privaten Sektor bezieht sich die Kerntätigkeit eines Verantwortlichen auf seine **Haupttätigkeiten** und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit.“*

Demnach muss hier eine Haupttätigkeit des Verantwortlichen in der Verarbeitung besonderer Datenkategorien liegen. Eine dem eigentlichen Geschäftszweck **völlig untergeordnete reine Neben- bzw. Hilfstätigkeit** oder die Durchführung **reiner Verwaltungs- und Erhaltungsaufgaben** (soweit diese überhaupt Personenbezug haben, so z.B. unternehmensinterne Personalverwaltung einschließlich der Entlohnung, das Führen eines Zeiterfassungssystems bei den Beschäftigten, der Betrieb eines hausinternen IT-Systems) sind hier **unbeachtlich**.

Der Begriff der Kerntätigkeit steht immer in Wechselwirkung zum Umfang der Tätigkeiten insgesamt, so dass stets eine **Gesamtbetrachtung** anzustellen ist: Macht eine Tätigkeit 55 % der Gesamttätigkeit eines Unternehmens aus, ist sie eben keine Hilfs- oder Nebentätigkeit mehr. Die Kerntätigkeit muss also die verantwortliche Stelle qualitativ und quantitativ prägen.

Als „Kerntätigkeit“ lassen sich die wichtigsten Arbeitsabläufe betrachten, die zum Erreichen der Ziele des Verantwortlichen oder des Auftragsverarbeiters (Geschäfts- / Unternehmenszweck bzw. Unternehmensstrategie) erforderlich sind, also alle Maßnahmen, die den Geschäftszweck unmittelbar fördern, die wesentlich oder maßgeblich zum Gesamtwertschöpfungsprozess des Verantwortlichen beitragen.

Gleichwohl sollte der Begriff „Kerntätigkeit“ nicht dahingehend interpretiert werden, dass sich dieser nicht auch auf Tätigkeiten erstreckte, bei denen die Verarbeitung von Daten einen untrennbaren Bestandteil der Tätigkeit des Verantwortlichen oder Auftragsverarbeiters darstellt.

Für die Antwort auf die Frage, ob im Sinne des Artikels 37 Abs. 1 Buchst. c DS-GVO die Kerntätigkeit insbesondere eines sonstigen Angehörigen eines **Gesundheitsberufs** in der (umfangreichen) Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 DS-GVO besteht, kann auch von Bedeutung sein, ob durch Rechtsvorschriften eine **Dokumentation** und eine damit einhergehende Verarbeitung solcher personenbezogenen Daten vorgeschrieben ist. Solche Vorschriften finden sich für Ärzte beispielsweise in § 10 Abs. 1 der Berufsordnung der Landesärztekammer Baden-Württemberg sowie

in § 630 f des Bürgerlichen Gesetzbuchs. Neben den Ärzten oder Zahnärzten, den Psychologischen, Psychotherapeuten sowie den Kinder- und Jugendpsychotherapeuten können auch Angehörige anderer Heilberufe als Behandelnde einen Behandlungsvertrag gemäß § 630 a BGB schließen wie Heilpraktiker, Hebammen, Physiotherapeuten, Masseure, medizinische Bademeister, Ergotherapeuten oder Logopäden. Soweit für andere Angehörige eines Gesundheitsberufs, beispielsweise Apotheker, Heilpraktiker und Physiotherapeuten, vergleichbare rechtliche Anforderungen gelten (und es nicht nur ins Ermessen oder Belieben dieser Akteure gestellt ist, Vorgänge zu dokumentieren), wäre auch für diese das Vorliegen einer **Kerntätigkeit** im oben genannten Sinne zu **bejahen**.

Wenn die Frage nach dem Vorliegen einer solchen Kerntätigkeit mit „**nein**“ beantwortet wird, ist die Prüfung beendet. Eine Pflicht zur Benennung eines Datenschutzbeauftragten nach Artikel 37 Abs. 1 Buchst. c DS-GVO besteht dann nicht. Auf weitere Fragen, etwa nach dem Vorliegen einer umfangreichen Bearbeitung, kommt es nicht mehr an.

Übersicht 1: Beispiele im Zusammenhang mit der Verarbeitung von Gesundheits- und Patientendaten

Verarbeitung von Gesundheits- und Patientendaten ist Kerntätigkeit	**Verarbeitung von Gesundheits- und Patientendaten ist keine Kerntätigkeit**
Arzt und Zahnarzt (alle Fachrichtungen)	Augenoptiker
Apotheker	Betrieb eines Fitness-Centers (auch mit Eingangs-Gesundheitscheck)
Betrieb eines Krankenhauses	Betrieb einer Beratungsstelle nach den §§ 3 und 8 des Schwangerschaftskonfliktgesetzes
Betrieb einer Reha-Einrichtung	Betrieb eines Dentallabors
Physiotherapeut	Diätassistent
Betrieb eines Seniorenheimes	Hörgeräteakustiker
Betrieb eines Pflegeheimes	
Ergotherapeut	Orthopädieschuhmacher

Heilpraktiker	
Hebamme	Podologe
Logopäde	Versicherungsvertreter / Versicherungsagentur (wenn auch regelmäßig andere Versicherungen als z.B. Lebens-, Kranken- und Pflegeversicherungen vermittelt werden)
Betrieb eines medizinischen Labors	Zahntechniker
Betrieb eines privaten (ambulanten) Pflegedienstes (Kranken- und Altenpflege)	
Psychologe	
	
<u>Weiterprüfung</u> unter Abschnitt 3. c) notwendig	**<u>Keine Pflicht</u>** zur Benennung eines Datenschutzbeauftragten nach Art. 37 Abs. 1 Buchst. c DS-GVO mangels entsprechender Kerntätigkeit

c) Umfangreiche Verarbeitung

Auch wenn die Verarbeitung von besonderen Kategorien personenbezogener Daten als Kerntätigkeit bejaht wird, muss noch als 3. Kriterium die **umfangreiche Bearbeitung** dieser besonderen Datenarten als Kerntätigkeit hinzukommen. Somit stellt sich die Frage, was unter einer „umfangreichen Verarbeitung“ konkret zu verstehen ist.

Ob eine umfangreiche Verarbeitung vorliegt, ergibt sich aus den nachfolgenden Kriterien des ErwGr 91 der DS-GVO:

- (große) Menge(n) an personenbezogenen Daten (Volumen);
- Verarbeitung auf regionaler, nationaler oder supranationaler Ebene (geografischer Aspekt);
- Anzahl der betroffenen Personen (absolute Zahl oder in Prozent zur relevanten Bezugsgröße);

- Dauer der Verarbeitung (zeitlicher Aspekt).

Können **zwei oder mehr Kriterien bejaht** werden, ist von einer umfangreichen Verarbeitung auszugehen. Hierbei kommt es stets auf den Einzelfall an. In der Regel ist aber nicht von einer umfangreichen, sondern einer normalen, durchschnittlichen Bearbeitung auszugehen.

Liegt eine umfangreiche Datenverarbeitung vor, ist ohnehin nach Art. 35 Abs. 3 Buchst. b DS-GVO eine Datenschutz-Folgenabschätzung durchzuführen, was wiederum nach § 38 Abs. 1 BDSG die Pflicht zur Benennung eines DSB auslöst.

Gesetzliche Regelvermutung („Privilegierung"): Keine umfangreiche Verarbeitung bei einzeln praktizierenden Ärzten, Angehörigen eines Gesundheitsberufs und Rechtsanwälten

ErwGr 91 der DS-GVO (der an sich zur Notwendigkeit einer Datenschutz-Folgenabschätzung Stellung nimmt, aber in seiner Bewertung auch hier herangezogen werden kann) ist zu entnehmen:

> *„Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt."*

Der europäische Gesetzgeber hat also die Datenverarbeitung durch einen **einzelnen** Arzt, einen einzelnen Angehörigen eines Gesundheitsberufs und einen einzelnen Rechtsanwalt vom Anwendungsbereich der Vorschrift ausgenommen, weil er davon ausgeht, dass deren jeweilige Datenverarbeitung in diesem Fall **nicht umfangreich** ist.

d) DSK-Beschluss zur DSB-Bestellpflicht bei Angehörigen von Gesundheitsberufen

Ausgehend von diesem rechtlichen Rahmen hat die

Datenschutzkonferenz (DSK)

am 26. April 2018 folgenden Beschluss gefasst:

Datenschutzbeauftragten-Bestellpflicht
nach Artikel 37 Abs. 1 Buchst. c Datenschutz-Grundverordnung
bei Arztpraxen, Apotheken und sonstigen Angehörigen eines Gesundheitsberufs

1. Betreibt ein **einzelner** Arzt, Apotheker oder sonstiger Angehöriger eines Gesundheitsberufs eine Praxis, Apotheke oder ein Gesundheitsberufsunternehmen und sind dort einschließlich seiner Person in der Regel mindestens 10 Personen ständig mit der (*automatisierten, Ergänzung des LfDI BW*) Verarbeitung personenbezogener Daten beschäftigt, besteht eine gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten (DSB).

2. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu **mehreren** in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, ist in der Regel nicht von einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne von Art. 37 Abs. 1 Buchst. c DS-GVO auszugehen – in diesen Fällen ist unter Berücksichtigung von Punkt 3 dann kein DSB zu benennen, wenn weniger als 10 Personen mit der Verarbeitung personenbezogener Daten beschäftigt sind.

3. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, bei denen **ein hohes Risiko für die Rechte und Freiheiten bei der Verarbeitung** personenbezogener Daten zu erwarten ist, ist eine Datenschutzfolgenabschätzung vorgeschrieben und damit zwingend ein Datenschutzbeauftragter zu benennen. Dies kann neben einer umfangreichen Verarbeitung (z.B. große Praxisgemeinschaften), die ohnehin nach Art. 37 Abs. 1 Buchst. c DS-GVO zu einer Benennungspflicht führt, beispielsweise beim Einsatz von neuen Technologien, die ein hohes Risiko mit sich bringen, der Fall sein. Der Datenschutzbeauftragte ist damit auch dann zu benennen, wenn weniger als 10 Personen ständig mit der Verarbeitung personenbezogener Daten zu tun haben.

4. Der **Begriff „Gesundheitsberuf“** ist im Sinne der Aufzählung nach § 203 Abs. 1 StGB auszulegen und umfasst die in § 203 Abs. 1 Nr. 1, 2, 4 und 5 StGB aufgezählten Berufsbilder.

Dieser Beschluss ist hinsichtlich der Ziffern 1 bis 3 entsprechend auch auf **Rechtsanwälte** anzuwenden.

4. Regelmäßig sind mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt (§ 38 Abs. 1 S. 1 BDSG).

Neben die Bestellpflicht gemäß DS-GVO tritt diejenige des BDSG: § 38 Abs. 1 S. 1 BDSG[4] schafft eine zusätzliche Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz für alle nicht-öffentlichen Stellen, die in der Regel mehr als 19 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Gezählt werden nicht nur die abhängig Beschäftigten bzw. Mitarbeiter, sondern **alle Personen** beim Verantwortlichen oder Auftragsverarbeiter, also auch der Chef oder die Partner oder der/die Kanzlei- oder Praxisinhaber.

a) Was ist unter dem Begriff „Personen“ zu verstehen?

Das Wort „Personen“ soll deutlich machen, dass aus datenschutzrechtlicher Sicht allein die Anzahl der mit der automatisierten Verarbeitung personenbezogener Daten Beschäftigten – unabhängig von ihrem arbeitsrechtlichen Status als Arbeitnehmer, freie Mitarbeiter oder Auszubildende – entscheidend ist.

Es sind also beispielsweise hinzuzurechnen: Voll- und Teilzeitkräfte, Leiharbeitnehmer, Auszubildende, Volontäre und Praktikanten sowie Beschäftigte in Telearbeit.

b) Was bedeuten „ständig“ und „in der Regel“?

Diese beiden Kriterien stellen auf die hinzuzuzählenden Beschäftigungsverhältnisse ab, nicht auf die Art der Tätigkeit innerhalb eines Beschäftigungsverhältnisses.

„In der Regel“ soll unterstreichen, dass gewisse Schwankungen in der Anzahl der Personen, die automatisiert Daten verarbeiten, unbeachtlich sind, wenn „in der Regel“ die Anzahl unter 20 Personen bleibt. Dadurch soll vermieden werden, dass Unternehmen nur deshalb einer anderen Kategorie (DSB-Bestellpflicht) zugeordnet werden, weil sie die maßgebliche Personengrenze für die Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz **kurzzeitig** überschreiten. Entscheidend ist der **auf ein Jahr zu betrachtende, durchschnittliche Personalbestand**.

„Ständig“ soll klarstellen, dass Personen, die nur **gelegentlich**, z. B. als Urlaubsvertretung, mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, nicht mitgezählt werden. Maßgeblich ist danach, dass die Datenverarbeitung zu den

[4] Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU - 2. DSAnpUG-EU), am 26.11.2019 in Kraft getreten.

(arbeitsvertraglich/weisungsgemäß) zugeordneten Aufgaben zählt und nicht nur ausnahmsweise und ad hoc ohne dauerhafte Zuordnung erfolgt.

c) Die Person muss automatisiert Daten verarbeiten

Es sind aber **nur die Personen** hinzuzuzählen, die im Unternehmen (Verein usw.) **automatisiert Daten verarbeiten**. Eine automatisierte Datenverarbeitung liegt vor, wenn für die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten von der Person Datenverarbeitungsanlagen wie z.B. PCs, Tablets oder Smartphones eingesetzt werden. Das BDSG weicht hinsichtlich der Bestellpflicht daher vom Verarbeitungsbegriff des Art. 4 Nr. 2 DS-GVO ab.

Personen (Beschäftigte), die **mit anderen (z. B. technischen/handwerklichen) Aufgaben** betraut sind und keine automatisierte Datenverarbeitung durchführen, sind **nicht zu berücksichtigen**.

Nicht hinzuzuzählen sind damit z. B. angestellte Handwerker, Reinigungskräfte, LKW-Fahrer, Monteure, Lager-Mitarbeiter, Arbeiter an Produktionsstätten und auf Baustellen etc., die ihre Aufträge intern **nur auf Papier** bekommen und nicht automatisiert personenbezogene Daten verarbeiten. Bekommen sie ihre Aufträge via Smartphone oder Tablet, sind sie hinzuzuzählen.

Trainer, Betreuer und Übungsleiter in Vereinen verfügen auch zumeist über Namens- oder Adresslisten ihrer jeweiligen Mannschaften oder Gruppen, die sie auch nutzen. Soweit dies ohne technische Geräte (z.B. Smartphones) geschieht, ist auch in diesen Fällen nicht von einer automatisierten Datenverarbeitung auszugehen. Diese Personen zählen dann ebenfalls nicht hinzu.

5. Es ist eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen (§ 38 Abs. 1 S. 2 1. HS BDSG)

Die Pflicht zur Benennung eines Datenschutzbeauftragten wird nach § 38 Abs. 1 S. 2 1. HS BDSG auch ausgelöst, wenn im Unternehmen (in der Kanzlei / im Verein / in der Praxis) wegen eines (oder mehrerer) Datenverarbeitungsverfahrens eine sog. **Datenschutz-Folgenabschätzung (DSFA) nach Art. 35 DS-GVO** durchzuführen ist.

Eine solche DSFA ist durchzuführen, wenn die **Form der Verarbeitung**, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des **Umfangs**, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein **hohes Risiko** zur Folge hat. Sie befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann (Art. 35 Abs. 1, 7 DS-GVO sowie ErwGr 84, 90).

Eine DSFA bezieht sich auf einzelne, konkrete Verarbeitungsvorgänge. Unter Verarbeitungsvorgängen ist die Summe von Daten, Systemen (Hard- und Software) und Prozessen zu verstehen. Sofern mehrere ähnliche Verarbeitungsvorgänge voraussichtlich ein ähnliches Risiko aufweisen, können diese zusammen bewertet werden (Art. 35 Abs. 1 DS-GVO). Ähnliche Risiken können beispielsweise dann gegeben sein, wenn ähnliche Technologien zur Verarbeitung vergleichbarer Daten(-kategorien) zu gleichen Zwecken eingesetzt werden (vgl. auch ErwGr 92 DS-GVO). Bei einer gemeinsamen Bewertung von ähnlichen Verarbeitungsvorgängen sind die im Folgenden dargestellten Vorgehensweisen ggf. anzupassen.

Ob eine DSFA durchzuführen ist, ergibt sich aus einer Abschätzung der Risiken der Verarbeitungsvorgänge („Schwellwertanalyse“). Ergibt diese ein **voraussichtlich hohes Risiko**, dann ist eine DSFA durchzuführen. Wird festgestellt, dass der Verarbeitungsvorgang kein hohes Risiko aufweist, dann ist eine DSFA nicht erforderlich. In jedem Fall ist die Entscheidung über die Durchführung oder Nichtdurchführung der DSFA mit Angabe der maßgeblichen Gründe für den konkreten Verarbeitungsvorgang schriftlich zu dokumentieren. Eine DSFA ist **vor** der Aufnahme der zu betrachtenden Verarbeitungsvorgänge durchzuführen.

Art. 35 Abs. 3 DS-GVO benennt einige Fallgruppen, die regelmäßig zu einem hohen Risiko i. S. d. Art. 35 Abs. 1 DS-GVO und damit zur Pflicht führen, eine DSFA durchzuführen – was wiederum für Sie die Pflicht auslöst, einen Datenschutzbeauftragten zu benennen.

Die Datenschutzaufsichtsbehörde hat zur Konkretisierung eine nicht-abschließende Liste mit Verarbeitungstätigkeiten, bei denen stets eine DSFA durchzuführen ist, veröffentlicht (sog. „Muss-Liste“). Diese finden Sie auch auf unserer Internetseite:
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Liste-von-Verarbeitungsvorgängen-nach-Art.-35-Abs.-4-DS-GVO-LfDI-BW.pdf

Der Europäische Datenschutzausschuss hat zur DSFA Leitlinien beschlossen:
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/06/Leitlinien-zur-Datenschutz-Folgenabschätzung.pdf

Bei **Angehörigen von Gesundheitsberufen und Rechtsanwälten** greift **Art. 35 Abs. 3 Buchst. b DS-GVO**…

> *Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:*
> *(…)*
> *b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10*
> *(...)*

… regelmäßig **nicht**. Hier kommt, diesmal in direkter Anwendung, wieder **ErwGr 91 der DS-GVO** ins Spiel. Die gesetzliche Regelvermutung („Privilegierung“), dass bei einzeln praktizierenden Ärzten, Angehörigen eines Gesundheitsberufs und Rechtsanwälten keine umfangreiche Verarbeitung stattfindet, führt dazu, dass in diesen Fällen **keine DSFA durchzuführen und daher auch kein Datenschutzbeauftragter zu bestellen ist**.
Es kann daher auf die Ergebnisse unter **Abschnitt II. 3.** verwiesen werden, insbesondere auch auf die oben dargestellte Übersicht.

Informationen zur DSFA finden Sie im entsprechenden DSK-Kurzpapier Nr. 5:
https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2013/02/DSK-Kurzpapier-5-DSFA.pdf

6. Es werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet (§ 38 Abs. 1 S. 2 2. HS BDSG)

Wie schon im BDSG-alt sind diejenigen Stellen verpflichtet, einen DSB zu benennen, die geschäftsmäßig personenbezogene Daten erheben und verkaufen oder vermieten.

Dies betrifft insbesondere **Adresshändler, Wirtschaftsauskunfteien** und, wie der Gesetzestext selbst schon namentlich aufführt, **Markt- und Meinungsforschungsinstitute**. Allerdings ist bei den Instituten festzustellen, dass diese immer seltener selbst mit personenbezogenen Daten arbeiten.

III. Freiwillige Benennung

Art. 37 Abs. 4 DS-GVO stellt übrigens klar, dass die **freiwillige Benennung** von Datenschutzbeauftragten immer möglich ist. Wenn eine Einrichtung einen DSB auf freiwilliger Basis ernennt, so unterliegen dessen Benennung, Stellung und Aufgabenbereich den Anforderungen wie bei einer obligatorischen Benennung (Art. 37 bis 39 DS-GVO).

Einer Einrichtung, die zur Benennung eines DSB nicht gesetzlich verpflichtet ist und die nicht gewillt ist, einen solchen auf freiwilliger Basis zu benennen, steht es frei, Mitarbeiter oder externe Berater/Beraterinnen mit Aufgaben zu betrauen, die mit dem Schutz personenbezogener Daten in Zusammenhang stehen. In einem solchen Fall gilt es jegliche Unklarheit hinsichtlich ihrer Funktionsbezeichnung, ihres Status, ihrer Stellung und ihres Aufgabenfelds zu vermeiden.

Daher sollte aus allen Mitteilungen innerhalb des Unternehmens und gegenüber Datenschutzbehörden, betroffenen Personen und der breiten Öffentlichkeit klar hervorgehen, dass die Funktionsbezeichnung der natürlichen Person bzw. des Beraters/der Beraterin nicht die eines Datenschutzbeauftragten ist.

Und weiter mit Teil II des Praxisratgebers, der u.a. folgende Themen behandelt:

Persönliche Voraussetzungen
Durchführung der Benennung
Stellung und Aufgaben
Beendigung der Benennung