Positionspapier des BvD zum Entwurf der EU-Datenschutzgrundverordnung vom 25.01.2012

Stand: 18.10.2012

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Inhalt

I. Vorstellung BvD 3

II. Einleitung 3

1. Positive und zukunftsfähige Weichenstellung für den Datenschutz durch die EU-DSGVO 4

2. Verbot mit Erlaubnisvorbehalt 4

3. Betriebliche Datenschutzbeauftragte 5

III. Sieben Hinweise zur Unterstützung der Ziele der EU-DSGVO 6

1. Hinweis: Klarstellung des Anwendungsbereichs der EU-DSGVO 6

2. Hinweis: Einführung der Pseudonymisierung 8

3. Hinweis: Benennung eines Datenschutzbeauftragten entsprechend dem Schutzbedürfnis der Daten anstatt der Unternehmensgröße sowie Erfordernis der Fachkunde und Unabhängigkeit des Datenschutzbeauftragten 8

   a) Pflicht zur Benennung eines Datenschutzbeauftragten 8

   b) Fachkunde / Zuverlässigkeit / Weiterbildungsanspruch 13

   c) Bestelldauer / Kündigungsschutz 14

   d) Überblick: Vorteile für den für die Verarbeitung Verantwortlichen bei Benennung eines Datenschutzbeauftragten 14

4. Hinweis: Rechtssicherheit durch Klarstellung der Verantwortung des für die Verarbeitung Verantwortlichen bei der Auftragsverarbeitung 16

5. Hinweis: Gleichstellung von Sozialdaten mit Gesundheitsdaten in Art. 81 EU-DSGVO 17

6. Hinweis: Bagatellklausel bei Security Breach Notification 17

7. Hinweise zum Dialog 18

IV. Bereitschaft des BvD zum Dialog 18

I. Vorstellung BvD

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. ist die Berufsorganisation der Datenschutzbeauftragten. Die satzungsgemäße Aufgabe des BvD besteht darin, die Interessen der betrieblichen und behördlichen Datenschutzbeauftragten im Sinne einer dem Stand der Technik angemessenen Realisierung von Datenschutz und Datensicherheit zu fördern.

Die über 790 Datenschutzbeauftragten im BvD betreuen mehrere tausend Unternehmen, Behörden und Institutionen und sind die direkten Ansprechpartner für mehr als fünf Millionen Beschäftigte und noch deutlich mehr Kunden dieser Unternehmen. In den Arbeitskreisen und Ausschüssen des BvD wurden die wesentlichen Änderungen des Entwurfs der Verordnung des europäischen Parlaments und Rats zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.01.2012 (KOM (2012) 11) (http://ec.europa.eu/justice/data-rotection/document/review2012/com_2012_11_de.pdf), nachfolgend EU-DSGVO-E, für die tägliche Praxis überprüft. Die Kommentierung des EU-DSGVO-E bezieht sich daher zunächst nur auf die Teile, welche sich unmittelbar auf die Tätigkeit der Datenschutzbeauftragten auswirken bzw. bei denen offensichtliche Klarstellungen bzw. Verbesserungsmöglichkeiten aus Sicht der Praktiker angezeigt sind.

II. Einleitung

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. begrüßt die Initiative der EU-Kommission, das Datenschutzrecht, entsprechend dem Wandel der Zeit seit der EU-Richtlinie 95/46/EG, zu modernisieren und in Europa zu vereinheitlichen. Es besteht damit die Chance, 20 Jahre nach dem Inkrafttreten der EU-Richtlinie 95/46/EG im europäischen Datenschutz einen neuen Meilenstein zu setzen.

Im Zuge der immer weitergehenden Verarbeitung personenbezogener Daten durch staatliche Stellen und viel mehr noch durch private Wirtschaftsunternehmen sind die Betroffenen heute sensibler denn je und erwarten einen besseren Schutz durch den Staat und mehr Aktivitäten ihres Datenschutzbeauftragten. Dies gilt in Europa, aber längst auch in den USA oder in Asien. Die Akzeptanz neuer Angebote der Wirtschaft und der Industrie im digitalen Umfeld haben nur dann eine Chance sich durchzusetzen, wenn sie auch hinsichtlich der Anforderungen an den Schutz der Persönlichkeitsrechte und der Datensicherheit das Vertrauen der Bürger und Kunden genießen: Vertrauen ist die Grundlage innovativer Technologien!

Der BvD befasst sich in dieser Stellungnahme entsprechend seiner Rolle als Berufsverband zunächst im Wesentlichen mit der Rolle des Datenschutzbeauftragten und weist darüber hinaus auf Aspekte aus der Praxis des „gelebten Datenschutzes“ der Datenschutzbeauftragten hin.

1. Positive und zukunftsfähige Weichenstellung für den Datenschutz durch den EU-DSGVO-E

Die EU-Kommission hat dies erkannt und legt dazu einen Entwurf zu einer Datenschutzgrundverordnung vor, der den zahlreichen Anforderungen aller Beteiligten gerecht werden muss. Das dies nicht in allen Teilen gelingen kann, liegt auf der Hand. Es ist daher zu begrüßen, dass die Kommission sich trotzdem dieser gewaltigen Aufgabe angenommen und diesen Entwurf vorgelegt hat.

Zwei wesentliche und besonders begrüßenswerte Elemente des Entwurfs der EU-Kommission sind

- das **Verbot mit Erlaubnisvorbehalt** als sicher handhabbare Bewertungsgrundlage des Umgangs mit personenbezogenen Daten sowie
- das **Institut „betrieblicher Datenschutzbeauftragter“** als Kernelement der Selbstregulierung und Entlastung der Aufsichtsbehörden.

Beides zusammen – Verbot mit Erlaubnisvorbehalt als materiell-rechtliche Entscheidungsregelung und der betriebliche Datenschutzbeauftragte als Verfahrenssicherung – bilden die Grundlage für den Schutz der Persönlichkeitsrechte der Betroffenen. Darüber hinaus sind sie auch eine Stütze der Rechtssicherheit für diejenigen, die für die Verarbeitung verantwortlich sind.

2. Verbot mit Erlaubnisvorbehalt

Das Verbot mit Erlaubnisvorbehalt beinhaltet die Pflicht des für die Verarbeitung Verantwortlichen, eine Verarbeitung personenbezogener Daten zunächst zu hinterfragen und sodann begründbar die Zulässigkeit zu bewerten, denn er muss einem Betroffenen die Zulässigkeit darlegen können. Der Verzicht auf das Verbot mit Erlaubnisvorbehalt würde den Betroffenen dazu zwingen, gegenüber dem für die Verarbeitung Verantwortlichen die Unzulässigkeit einer Verarbeitung seiner Daten darzulegen und zu beweisen. In der Praxis kann ein Betroffener dies weder in rechtlicher noch in tatsächlicher Hinsicht leisten, denn den Betroffenen werden weit überwiegend die Möglichkeiten zur Aufklärung der Hintergründe fehlen und auch das Wissen zur datenschutzrechtlichen Bewertung. Gleichzeitig verdeutlicht dies dem für die Verarbeitung Verantwortlichen, dass er Technologie, die er nicht versteht, nicht zur Verarbeitung personenbezogener Daten einsetzen kann. Wenn er diese nicht versteht, kann er diese auch nicht bewerten. Was nicht bewertet werden kann, muss als unzulässig betrachtet werden. Auch die Aufsichtspraxis ist damit erleichtert, da auch die Aufsichtsbehörden damit nicht die tatsächlichen und rechtlichen Voraussetzungen selbst aufklären müssen, sondern eine entsprechende Aufklärung durch den für die Verarbeitung Verantwortlichen fordern können. Gerade in Anbetracht der Finanzlage und Personaldecke der Datenschutzaufsichtsbehörden lässt nur das Verbot mit Erlaubnisvorbehalt eine Aufsichtspraxis realistisch erscheinen.

3. Betriebliche Datenschutzbeauftragte

Der betriebliche Datenschutzbeauftragte ist ein Institut der Selbstregulierung, das staatlichen „Aufsichtsdruck“ auf den für die Verarbeitung Verantwortlichen reduziert. Gleichzeitig entlastet dieses Institut der Selbstregulierung auch die staatlichen Aufsichtsbehörden und die Wirtschaft, da in gewissem Umfang die „Aufsicht“ durch den betrieblichen Datenschutzbeauftragten als Ausdruck einer regulierten Selbstregulierung wahrgenommen wird. Darüber hinaus ist er in der deutschen Datenschutzaufsichtspraxis auch vermittelnder Ansprechpartner der Datenschutzaufsichtsbehörden, wenn sie im Rahmen der Aufsicht an den für die Verarbeitung Verantwortlichen herantreten. Hier zeigen sich die Vorteile des Instituts betrieblicher Datenschutzbeauftragter auch für den für die Verarbeitung Verantwortlichen. Diese Art der Aufsicht ist in der Praxis deutlich weniger konfrontativ. Ebenso stellt sich auch das Verhältnis zwischen den für die Verarbeitung Verantwortlichen und der Betroffenen dar. Der betriebliche Datenschutzbeauftragte ist häufig „Konflikt entschärfend“ dazwischen geschaltet. Darüber hinaus unterstützt er als sachkompetenter Funktionsträger den für die Verarbeitung Verantwortlichen bei der Einhaltung der gesetzlichen Pflichten des Datenschutzrechts.

Die Übernahme des Erfolgsmodells der Einrichtung eines Datenschutzbeauftragten in Deutschland zeigt also auch die Weitsicht, mit welcher der Vorschlag bewährte Konzepte aus den Mitgliedsstaaten im gesamten europäischen Wirtschaftsraum implementieren will. Die Einbindung eines fachlich qualifizierten Ansprechpartners, der sowohl die Belange und Prozesse derjenigen, die für die Verarbeitung verantwortlich sind, als auch die normativen Anforderungen an Datenschutz und Datensicherheit kennt und beherrscht, gewährleistet einen bürokratie-minimalen Einsatz, um die Ziele der Wahrung der Persönlichkeitsrechte der betroffenen Personen und die Möglichkeit des freien Datenverkehrs in angemessener Weise zu sichern und bei widerstreitenden Interessen eine vertretbare Lösung zu ermöglichen. Der BvD begrüßt die Entscheidung des Gesetzgebers, durch die Einführung eines Datenschutzbeauftragten auch in anderen Mitgliedsländern praxisnahe Entscheidungen in Unternehmen und Verwaltungen fachlich begleiten zu lassen und damit einen wesentlichen Beitrag zum Bürokratieabbau zu leisten. Die Berücksichtigung der positiven Erfahrungen aus einem Mitgliedsland sind Garanten einer umfassenden Reform der datenschutzrechtlichen Grundlage einer europaweit einheitlichen Lösung. Dies gilt für die Stellung des Datenschutzbeauftragten (Art. 36 EU-DSGVO-E), wie für dessen Aufgaben (Art. 37 EU-DSGVO-E).

III. Sieben Hinweise zur Unterstützung der Ziele des EU-DSGVO-E

Mit sieben Hinweisen möchte der BvD die EU-Kommission bei der Erreichung der mit dem EU-DSGVO-E gesteckten Ziele unterstützen:

1. Hinweis: Klarstellung des Anwendungsbereichs der EU-DSGVO-E

Das entscheidende Kriterium für die Anwendung des Datenschutzrechts ist der **Personenbezug einer Information**. Der Datenschutz muss eingreifen, wenn Informationen einer natürlichen Person zugeordnet werden können. Dann ist auch das Datenschutzrecht anwendbar. Da das Datenschutzrecht selbst seinen Anwendungsbereich über den Personenbezug von Informationen definiert (Art. 1 Abs. 1 i. V. m. Art. 4 Abs. 2), geht der EU-DSGVO-E offensichtlich davon aus, dass es auch Informationen gibt, auf welche das Datenschutzrecht nicht zur Anwendung kommt.

Die Grenzziehung ist daher für die Anwendung des Datenschutzrechts von entscheidender Bedeutung. Dies lässt sich wie folgt verdeutlichen: Der Betreiber einer Internetseite erhebt die dynamische IP-Adresse des Besuchers seiner Internetseite. Er selbst kann diese Information keiner natürlichen Person zuordnen, denn er weiß nicht, welchem Nutzer der Internet-Access-Provider diese (dynamische) IP-Adresse temporär zugeordnet hat. Wird für den Personenbezug nur auf den Betreiber der Webseite abgestellt, liegt kein Personenbezug vor und das Datenschutzrecht ist nicht anwendbar (sog. relativer Ansatz). Wird dem Betreiber der Internetseite allerdings das Wissen des Internet-Access-Providers zugerechnet, ist von einem Personenbezug und der Anwendung des Datenschutzrechts auszugehen (sog. absoluter Ansatz). Dabei ist allerdings auch zu beachten, dass der Internet-Access-Provider sich nach deutschem Recht strafbar machen würde, wenn er diese Information über den Nutzer an den Betreiber der Webseite ohne rechtliche Grundlage weitergeben würde.

In Deutschland ist diese Frage derzeit rechtlich umstritten. Während die deutschen Datenschutzaufsichtsbehörden den Personenbezug von IP-Adressen generell bejahen, verneint die überwiegende Meinung in der Literatur und – soweit ersichtlich – auch die Rechtsprechung den Personenbezug.

Für den Betreiber der Internetpräsenz ist es von entscheidender Bedeutung klar zu wissen, ob das Datenschutzrecht anwendbar ist oder nicht. Zur Unterscheidung von klaren Fällen der Bejahung des Personenbezugs: Die dynamische IP-Adresse wird – aber erst dann – auch für den Betreiber der Webseite zu einem personenbezogenen Datum, wenn sich der Nutzer gegenüber dem Betreiber der Webseite identifiziert (sei es durch eine Bestellung, sei es durch ein Log-In). Daher besteht auch keine Schutzlücke, denn der

Datenschutz greift jedenfalls dann, wenn der Verarbeitende selbst einen Zusammenhang zur Person herstellen kann. Die (dynamische) IP-Adresse ist für den Internet-Access-Provider stets ein personenbezogenes Datum, da er sie seinem Nutzer zuteilt.

Es wäre sehr zu begrüßen, wenn diese Frage durch den EU-DSGVO-E abschließend geklärt wird. Bisher ist dies nicht der Fall. Denn Erwägungsgrund 24 spricht für den sog. relativen Ansatz, während Art. 4 Abs. 1 EU-DSGVO-E für den sog. absoluten Ansatz spricht.

Zu beachten ist bei der Festlegung auch, dass der sog. absolute Ansatz in der Praxis weitgehend dazu führen wird, dass auf alle Informationen das Datenschutzrecht zur Anwendung kommt und der Anwendungsbereich keine begrenzende Funktion mehr hat. Denn durch das „Hinzuziehen" der Kenntnis sonstiger Personen lässt sich praktisch jede Information einer Person zuordnen. Alternativ werden sich in der Praxis Überlegungen ergeben, wie weit der Kreis der „hinzuziehenden" Dritten ist, was aber im Ergebnis das bereits bestehende Problem „in neuem Gewand" nur an einen anderen „Aufhänger" verlagert.

Der EU-DSGVO-E kennt die **Anonymisierung** nicht. Das Anonymisieren ist entscheidend, um das Ende der Anwendung des Datenschutzrechts zu bestimmen. Denn wenn eine Information durch Anonymisieren ihren Personenbezug verloren hat, ist es interessengerecht, die Anwendung des Datenschutzrechts zu beenden. Als Anonymisieren kann beispielsweise verstanden werden (in Anlehnung an § 3 Abs. 6 deutsches Bundesdatenschutzgesetz): das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Allein die Erwähnung der Anonymisierung im Erwägungsgrund 23 reicht nicht aus. Es ist erscheint daher geboten, den Begriff der Anonymisierung in den EU-DSGVO-E einzuführen und eindeutig zu definieren.

Gerade für die kleinen und mittleren Unternehmen (KMU), welche durch den Entwurf der EU-DSGVO von Pflichten befreit werden sollten (vgl. Erwägungsgrund 130 sowie Art. 8 Abs. 3, Art.12 Abs. 8, Art. 14 Abs. 7, Art. 22 Abs. 4, Art. 28 Abs. 4 lit. b, Art. 33 Abs. 6 EU-DSGVO-E) bedarf es einer einfachen und eindeutigen Entscheidungsregel, ob das Datenschutzrecht anzuwenden ist oder nicht.

2. Hinweis: Einführung der Pseudonymisierung

Der EU-DSGVO-E kennt nicht die Pseudonymisierung. Die Pseudonymisierung ist ein „Instrument“ zur Verringerung von datenschutzrechtlichen Eingriffen.

Im Rahmen der Zulässigkeitsprüfung anhand Interessenabwägung nach Art. 6 Abs. 1 lit. f EU-DSGVO-E führt die Verwendung pseudonymisierter Daten zu einer anderen Bewertung als die Verwendung nicht pseudonymisierten Daten, denn bei der Verwendung von Pseudonymen sind die Interessen der Betroffenen weniger belastet. Die Unterscheidung nach der Pseudonymisierung schafft daher die Möglichkeit zu einer datenschutzfreundlicheren Differenzierung im Rahmen der Rechtmäßigkeitsprüfung.

Als Pseudonymisieren kann beispielsweise verstanden werden (in Anlehnung an § 3 Abs. 6a deutsches Bundesdatenschutzgesetz): Das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

Im Interesse des Datenschutzes erscheint es sinnvoll, den Begriff Pseudonymisieren explizit in den EU-DSGVO-E als Verarbeitungsschritt einzuführen und explizit zu definieren, um die Berücksichtigung einer Pseudonymisieren im Rahmen der Interessensabwägung zu ermöglichen.

3. Hinweis: Benennung eines Datenschutzbeauftragten entsprechend dem Schutzbedürfnis der Daten anstatt der Unternehmensgröße sowie Erfordernis der Fachkunde und Unabhängigkeit des Datenschutzbeauftragten

a) Pflicht zur Benennung eines Datenschutzbeauftragten

Art. 35 Abs. 1 lit. b und c EU-DSGVO-E sehen für den nicht-öffentlichen Bereich eine Pflicht zur Bestellung eines Datenschutzbeauftragten unter zwei Voraussetzungen vor:

> *„b) die Bearbeitung durch ein Unternehmen erfolgt, das 250 oder mehr Mitarbeiter beschäftigt, oder*
>
> *c) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen.“*

Diese Gestaltung wird der Bedeutung des Datenschutzbeauftragten für den Datenschutz nicht gerecht. Es ist zwar zu begrüßen, dass im Fall einer regelmäßigen und systematischen Beobachtung eine Bestellpflicht unabhängig von der Anzahl der Beschäftigten besteht. Allerdings ist das Kriterium der Beobachtung nicht – jedenfalls nicht hinreichend – deutlich geeignet, die besonders gefährdenden Verarbeitungen zu erfas-

sen. Das weitere Kriterium der Anzahl der Beschäftigten ist zwar zur Ausgrenzung von KMU geeignet. Allerdings ist die reine Betriebsgröße keine datenschutzspezifische „Größe“. Dies würde aus der Sicht des Datenschutzes zu kuriosen Ergebnissen führen: Ein Unternehmen, das Auskunft über die Bonität und Kreditwürdigkeit von Verbraucher gibt, kommt gerade dann, wenn eine intelligente IT eingesetzt wird, mit deutlich weniger als 250 Mitarbeitern aus. Eine Bestellpflicht besteht dann nicht, obgleich das Bedürfnis nach einem Datenschutzbeauftragten auf der Hand liegt. Ein metallverarbeitendes Unternehmen aus der Zulieferungsbranche, das über 250 Arbeiter an Maschinen zur Produktion im Einsatz hat, aber nicht einmal Marketing gegenüber Verbrauchern betreibt, muss einen Datenschutzbeauftragten bestellen.

Entsprechend dem Ansatz, den Betroffenen durch den Schutz seiner Daten zu schützen (Art. 1 Abs. 1, Art. 4 Abs. 1 und Abs. 2 EU-DSGVO-E), müssen die betroffenen Daten das entscheidende Kriterium für die Bestellpflicht sein. Sei es die Masse der verarbeiteten Daten (bspw. 4 Mio. Datensätze im Bereich Adresshandel), die Art der Verarbeitung der Daten (bspw. Data Mining zur Bewertung des Kaufverhaltens) oder sei es die Art der verarbeiteten Daten (bspw. Daten über Gesundheit).

Vor diesem Hintergrund schlägt der BvD folgende Regelung vor:

*Artikel 35_**(neu)** EU-DSGVO-E*

Benennung eines Datenschutzbeauftragten

1. *Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen einen Datenschutzbeauftragten, falls*

   a) die Verarbeitung durch eine Behörde oder eine öffentliche Einrichtung erfolgt;

   oder

   b) die Verarbeitung durch ein Unternehmen erfolgt.

2. *Die Pflicht zur Benennung gilt für Unternehmen, deren Haupttätigkeit die Verarbeitung personenbezogener Daten ist, uneingeschränkt.*

3. *Unternehmen, die personenbezogene Daten als Hilfstätigkeit zur Haupttätigkeit verarbeiten, sind von der Pflicht zur Bestellung eines Datenschutzbeauftragten ausgenommen, sofern*

   a) der Umfang der Verarbeitung personenbezogener Daten, oder

   b) die Art der verarbeiteten personenbezogener Daten oder

   c) die Art der Verarbeitung personenbezogener Daten oder

   d) eine Kombination der vorgenannten Aspekte

   die Bestellung eines Datenschutzbeauftragten nicht erforderlich macht.

4. *Unternehmen mit drei oder mehr Tätigen zeigen binnen Monatsfrist die Benennung eines Datenschutzbeauftragten oder den Grund für die*

Ausnahme von der Bestellung gegenüber der Datenschutzaufsichtsbehörde an.

5. *Bis zur Vorlage eines Standardformulars durch die EU-Kommission sind die zuständigen Aufsichtsbehörden zur Vorgabe eines Standardformulars zur Meldung nach vorstehendem Absatz 4 befugt.*

6. *Unabhängig von der Pflicht zur Bestellung gilt für die Verarbeitung Verantwortlichen, die einen Beauftragten für den Datenschutz nach Maßgabe dieses Art. 35 benannt haben, dass*

   a) *anstelle der Zurateziehung der Aufsichtsbehörde nach Art. 34 Abs. 2 und Abs. 3 eine vorherige Bewertung mit Vorschlägen durch Datenschutzbeauftragten des für die Verarbeitung Verantwortlichen erfolgt; hat der für die Verarbeitung Verantwortliche nach der Zurateziehung des Datenschutzbeauftragten Zweifel an der Vereinbarkeit mit dieser Verordnung zieht er die Aufsichtsbehörde nach Maßgabe von Art. 34 zu Rate.*

   b) *für besonders gefährdende Verarbeitungen die Aufsichtsbehörde in Ausnahmen von der Regelung des Art. 35 Abs. 6 lit.a vorsehen kann."*

Erläuterung zu Art. 35 Abs. 3:

Der „*Umfang der Verarbeitung personenbezogener Daten"* adressiert Konstellationen, in denen allein schon aufgrund der Masse der verarbeiteten personenbezogenen Daten ein ergänzender Schutz durch die Benennung eines Datenschutzbeauftragten geboten erscheint. Mit der *„Art der verarbeiteten personenbezogener Daten"* ist insbesondere die Verarbeitung sensibler personenbezogener Daten erfasst, wohingegen sich im Fall „*Art der Verarbeitung personenbezogener Daten*" das Schutzbedürfnis aufgrund des Umgangs mit den personenbezogenen Daten und nicht schon aus den Daten selbst ergibt. Die Einbeziehung „*Kombination der vorgenannten Aspekte*" trägt dem Umstand Rechnung, dass Konstellationen in Betracht kommen, in den zwar keine der vorgenannten Schwellen für sich überschritten ist, aber die Kombination der Fälle dennoch eine Benennung eines Datenschutzbeauftragten geboten erscheinen lässt. So kann z.B. ein Unternehmen mit 50 Mitarbeitern, das sich nur mit Baumaterialien beschäftigt datenschutzrechtlich als weniger kritisch betrachtet werden, als ein Unternehmen mit 10 Mitarbeitern, das im Auftrag Data Mining betreibt oder einem anderen, welches mit 8 Mitarbeitern Persönlichkeitstests erstellt oder Gesundheitsdaten verarbeitet.

Erläuterung zu Art. 35 Abs. 6:

Gerade in der Konstellation des Art. 34 EU-DSGVO-E kann der Datenschutzbeauftragte seine Rolle als Instrument der Selbstregulierung wahrnehmen. Es erscheint daher angemessen, im Fall der Benennung eines Datenschutzbeauftragten diesen bei der Bewertung nach Art. 34 EU-DSGVO-E einzubeziehen. Dies führt auch zu einer Entlastung der Datenschutzaufsichtsbehörden und damit Effektuierung deren Tätigkeit in Fällen, in denen sie mangels Datenschutzbeauftragten selbst zum Schutz der betroffenen Person aktiver werden müssen. Bei verbleibenden Zweifeln über die Verwertung ist dennoch

die Datenschutzaufsichtsbehörde hinzuziehen. Aber auch in diesen Fällen ist sie entlastet, da sie auf die Vorarbeiten des Datenschutzbeauftragten zur Arbeitserleichterung zugreifen kann. Für den für die Verarbeitung Verantwortlichen stellt dieses Vorgehen auch ein effizienteres Vorgehen dar, da der Datenschutzbeauftragte ohnehin stärker in die betrieblichen Abläufe eingebunden ist, sodass eine Vorbewertung durch den Datenschutzbeauftragten für den für die Verarbeitung Verantwortlichen weniger aufwendig ist, als bei einer Darstellung gegenüber der Datenschutzaufsichtsbehörde. Auch der Schutz des Betroffenen wird dadurch nicht beschränkt.

Im Vergleich ergibt sich folgende Gegenüberstellung:

Artikel 35 EU-DSGVO-E *Benennung eines Datenschutzbeauftragten*	*Artikel 35_**(neu)** EU-DSGVO-E* *Benennung eines Datenschutzbeauftragten*
1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen einen Datenschutzbeauftragten, falls a) die Verarbeitung durch eine Behörde oder eine öffentliche Einrichtung erfolgt; oder b) die Bearbeitung durch ein Unternehmen erfolgt, das 250 oder mehr Mitarbeiter beschäftigt, oder c) die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen.	*1. Der für die Verarbeitung Verantwortliche und der Auftragsverarbeiter benennen einen Datenschutzbeauftragten, falls* *a) die Verarbeitung durch eine Behörde oder eine öffentliche Einrichtung erfolgt;* *oder* *b) die Verarbeitung durch ein Unternehmen erfolgt.* *2. Die Pflicht zur Benennung gilt für Unternehmen, deren Haupttätigkeit die Verarbeitung personenbezogener Daten ist, uneingeschränkt.* *3. Unternehmen, die personenbezogene Daten als Hilfstätigkeit zur Haupttätigkeit verarbeiten, sind von der Pflicht zur Bestellung eines Datenschutzbeauftragten ausgenommen, sofern* *a) der Umfang der Verarbeitung personenbezogener Daten, oder* *b) die Art der verarbeiteten personenbezogener Daten oder* *c) die Art der Verarbeitung personenbezogener Daten oder* *d) eine Kombination der vorgenannten Aspekte*

	die Bestellung eines Datenschutzbeauftragten nicht erforderlich macht. *4. Unternehmen mit drei oder mehr Tätigen zeigen binnen Monatsfrist die Benennung eines Datenschutzbeauftragten oder den Grund für die Ausnahme von der Bestellung gegenüber der Datenschutzaufsichtsbehörde an.* *5. Bis zur Vorlage eines Standardformulars durch die EU-Kommission sind die zuständigen Aufsichtsbehörden zur Vorgabe eines Standardformulars zur Meldung nach vorstehendem Absatz 4 befugt.* *6. Unabhängig von der Pflicht zur Bestellung gilt für die Verarbeitung Verantwortlichen, die einen Beauftragten für den Datenschutz nach Maßgabe dieses Art. 35 benannt haben* *a) anstelle der Zurateziehung der Aufsichtsbehörde nach Art. 34 Abs. 2 und Abs. 3 erfolgt eine vorherige Bewertung mit Vorschlägen durch Datenschutzbeauftragten des für die Verarbeitung Verantwortlichen; hat der für die Verarbeitung Verantwortliche nach der Zurateziehung des Datenschutzbeauftragten Zweifel an der Vereinbarkeit mit dieser Verordnung zieht er die Aufsichtsbehörde nach Maßgabe von Art. 34 zu Rate.* *b) für besonders gefährdende Verarbeitungen kann die Aufsichtsbehörde in Ausnahmen von der Regelung des Art. 35 Abs. 6 lit.a vorsehen."* *(nachfolgende Absätze verschieben sich in der Nummerierung)*

b) Fachkunde / Zuverlässigkeit / Weiterbildungsanspruch

Der Entwurf der EU-DSGVO äußert sich in Art. 35 allgemein zur beruflichen Qualifikation und zum Fachwissen des Datenschutzbeauftragten und verweist lediglich darauf, dass der Datenschutzbeauftragte die zur Aufgabenerfüllung erforderlichen Fähigkeiten besitzen muss. In 2010 legte die Konferenz der deutschen Aufsichtsbehörden über den nichtöffentlichen Bereich die Anforderungen an die Fachkunde eines Datenschutzbeauftragten in einem Beschluss fest (http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/24112010-MindestanforderungenAnFachkunde.pdf?__blob=publicationFile). Im Artikel 37 EU-DSGVO-E werden die umfangreichen Aufgaben des Datenschutzbeauftragten beschrieben. Neben konkreten Aufgaben wie z.B. Verfahrensdokumentation (Art. 28 EU-DSGVO-E) oder Ansprechpartner für die Aufsichtsbehörde, soll der Datenschutzbeauftragten die verantwortliche Stelle bei allen Pflichten, die sich für diese aus dem EU-DSGVO-E ergeben, beraten, unterstützen und überwachen. Daher benötigt der Datenschutzbeauftragte umfassende Fachkunde, angefangen bei Rechtskenntnissen, IT-Kenntnissen bis hin zu Management-Fähigkeiten, damit er z.B. Strategie-Planung, Datenschutz-Folgenabschätzung, Kontroll- und Beratungstätigkeiten wahrnehmen kann.

Zu den Grundkenntnissen im Rechtsbereich gehören umfassende Kenntnisse des Persönlichkeitsrechts, des europäischen und nationalen Datenschutzrechts, des Telekommunikationsrechts, des Arbeitnehmerdatenschutzrechts, des Strafrechts sowie des Rechts bei besonderen Verarbeitungsvorgängen oder Daten, wie z.B. personenbezogene Daten besonderer Kategorien oder Werbung. Je nach Art des Unternehmens und Art der Daten benötigt der Datenschutzbeauftragte zusätzliche Rechtskenntnisse, z.B. aus den Bereichen internationales Datenschutzrecht, Adresshandel und Marketing, Medizin oder dem Berufsrecht.

Datenschutz durch Technik, datenschutzfreundliche Voreinstellung, Datensicherheit, Prüfung und Beratung beim Einsatz von Verarbeitungsvorgängen erfordern grundlegende und umfassende IT-Kenntnisse. Mit der Funktionsweise von Netzwerktechnologien, Betriebssystemen und Datenbanksystemen muss sich der Datenschutzbeauftragte ebenso auskennen wie mit Hardware-Architektur, Firewall, Verschlüsselung, physischer Sicherheit, Datensicherung, etc., alles Themen aus dem klassischen Bereich der IT-Sicherheit. Er benötigt Kenntnisse, um bei Berechtigungskonzepten, Protokollierung und IT-Konzepten beraten und überwachen zu können. Auch im IT-Bereich ist es je nach Art des Unternehmens oder Art der Daten notwendig, zusätzliches Fachwissen zu besitzen.

Da der Datenschutzbeauftragte beraten und überwachen soll, sind Management-Fähigkeiten Voraussetzung, die Aufgabe überhaupt wahrnehmen zu können. Projekt- und Risikomanagement, Entwicklung von Konzepten, Durchführung von Audits und Kontrollen erfordern gute Fachkenntnisse in diesen Bereichen. Für Schulungen, die Beratungstätigkeit sowie Konfliktmanagement benötigt der Datenschutzbeauftragte kommunikative Methodik und Didaktik. Ergänzt wird sein Fachwissen durch betriebswirtschaftliche Grundkenntnisse.

Nur mit diesem erforderlichen Fachwissen kann er seine Aufgaben zuverlässig wahrnehmen. Das Fachwissen muss der Datenschutzbeauftragte daher auch durch Fort- und Weiterbildung ständig aktuell halten.
Zuverlässigkeit bedeutet auch Sicherstellung der Unabhängigkeit, Weisungsfreiheit, Kündigungsschutz und Verschwiegenheit des Datenschutzbeauftragten. Ausreichendes Zeitbudget sowie Mittel und Räumlichkeiten müssen ihm zur Verfügung gestellt werden.

c) Bestelldauer / Kündigungsschutz

Die Ausübung der Aufgaben des Datenschutzbeauftragten kann im Einzelfall entgegen den einzelnen Interessen des Arbeitgebers bzw. bei externen Datenschutzbeauftragten des Auftraggebers stehen. Hier muss der Datenschutzbeauftragte ungeachtet denkbarer Repressalien auf Schwachstellen hinweisen und seine Aufgabe ungehindert ausführen können, auch wenn er aus Sicht der für die Verarbeitung Verantwortlichen unbequem wird. Eine Befristung der Aufgabe auf mindestens 2 Jahre wie in Art. 35 Abs. 7 EU-DSGVO-E verhindert aber eine effektive und im Einzelfall kritische Wahrnehmung der Aufgaben. Angestellte Datenschutzbeauftragte müssen ihre Aufgaben ohne Befürchtungen um ihren Arbeitsplatz ausüben können. Eine Kündigung muss nur bei schwerwiegenden Verfehlungen durch den angestellten Datenschutzbeauftragten möglich sein, die eine Fortführung des Arbeitsverhältnisses für den Arbeitgeber unzumutbar werden lassen. Bei externen Datenschutzbeauftragten ist aus den gleichen Gründen eine Mindestbestelldauer angeraten, die seitens des Entwurfs angegebene Mindestdauer von 2 Jahren kann dabei nur eine Untergrenze sein. Die Wirksamkeit eines Datenschutzbeauftragten und das dadurch gewonnene Vertrauen der Bürgerinnen und Bürger in eine datenschutzkonforme Verarbeitung ihrer Daten kann nur gestärkt werden, wenn die Ausübung der Aufgaben eines Datenschutzbeauftragten uneingeschränkt wahrgenommen werden kann.

d) Überblick: Vorteile für den für die Verarbeitung Verantwortlichen bei Benennung eines Datenschutzbeauftragten

In Deutschland hat sich in jahrzehntelanger Praxis herausgestellt, dass die Unternehmen durch den Datenschutzberater auf einen kompetenten, sachnahen Ansprechpartner unmittelbar zugreifen können. Dieser ist mit den internen Prozessen, Anforderungen und Zusammenhängen, aber auch mit den konkreten gesetzlichen und technischen Anforderungen der Branche des Unternehmens vertraut und kann somit – oftmals auch kurzfristig – praxisnahe Lösungen erarbeiten und zielorientiert bei der Umsetzung beraten. Dabei umfasst das **Beratungsgebiet** sowohl die Prüfung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten als auch die Gestaltung der Einwilligungserklärungen der Betroffenen, über die Schulung und Sensibilisierung der eingesetzten Mitarbeiter bis hin zur Risikoanalyse und der Erarbeitung eines Maßnahmenkatalogs sowie der Durchführung interner Audits.

Die **Fachkunde des Datenschutzbeauftragten** verbunden mit den Fachkenntnissen der Branche des Arbeitsgebers / Auftraggebers gewährleistet eine sachgerechte, zeitnahe Beratung, die beide Interessenslagen berücksichtigt: die Persönlichkeitsrechte der Betroffenen und die wirtschaftlichen Interessen des Arbeitgebers/Auftraggebers. Abstimmungen und Beratungen in komplexen Einzelfällen mit und durch die Aufsichtsbehörden werden dadurch wesentlich beschleunigt und führen auch bei den Aufsichtsbehörden zu weniger Personalbedarf. Die Vertrauensstellung, die ein Datenschutzbeauftragter bei der Leitung der verantwortlichen Stelle genießt, wird aber ohne die Einführung einer Verschwiegenheitspflicht hinsichtlich Identität der Betroffenen, die sich an ihn wenden (Art. 35 Abs. 10 EU-DSGVO-E) nur einseitig entstehen können. Die betroffenen Personen müssen darauf vertrauen können, dass sie Nachfragen, hinter denen sich unter Umständen auch Missstände verbergen können, ohne Offenlegung ihrer Identität gegenüber dem Unternehmen, das auch als Arbeitgeber / Lieferant / Auftraggeber fungiert, befürchten zu müssen.

Der **Dokumentationsaufwand**, der für die Sicherstellung der Wahrung der Rechte der Betroffenen erforderlich ist, kann nur durch jemanden innerhalb des für die Verarbeitung Verantwortlichen erfolgen oder betreut werden, der auch die Besonderheiten der Anforderungen an einen wirksamen Persönlichkeitsschutz kennt und einfordert. Dementsprechend kann dieser Dokumentationsaufwand und die Pflicht zur Abstimmung mit den Aufsichtsbehörden für die Unternehmen auf ein erforderliches und notwendiges Maß reduziert werden, wenn ein Datenschutzbeauftragter eingebunden ist.

Die Zuweisung der Verantwortlichkeit zur Sicherstellung der Erstellung der Dokumentation an den Datenschutzbeauftragten (Art. 37 Abs. 1 lit.d EU-DSGVO-E) übersieht, dass die Verantwortlichkeit der Erstellung der Dokumentation nach Art. 28 Abs.1 EU-DSGVO-E beim für die Verarbeitung Verantwortlichen, beim Auftragsverarbeiter und beim Vertreter für die Verarbeitung Verantwortlichen liegt.

So kann bei einer **Datenschutz-Folgeabschätzung** (Art. 33 EU-DSGVO-E) die vorherige Zurateziehung der Aufsichtsbehörden (Art. 34 Abs. 1 – 6 EU-DSGVO-E) entfallen, wenn der für die Verarbeitung Verantwortliche einen unabhängigen Datenschutzbeauftragten einsetzt und dieser die Datenschutz-Folgeabschätzung durchführt. Für die Einschätzung, Abwägung und Dokumentation von bestimmten Verfahren und Prozessen ist der Datenschutzbeauftragte näher am Sachverhalt und kann sich von dem für die Verarbeitung Verantwortlichen zuarbeiten lassen. Dies entlastet die Aufsichtsbehörden, aber auch die Unternehmen, die aufwändige Abstimmungen mit Aufsichtsbehörden über Zweifelsfälle durch den Datenschutzbeauftragten begrenzen können.

4. Hinweis: Rechtssicherheit durch Klarstellung der Verantwortung des für die Verarbeitung Verantwortlichen bei der Auftragsverarbeitung

Durch Art. 26 EU-DSGVO-E wird auf europäischer Ebene der Auftragsverarbeiter etabliert. Die Auftragsverarbeitung zeichnet sich durch die vertragliche Gebundenheit des Auftragsverarbeiters (Art. 26 Abs. 2 EU-DSGVO-E) und insbesondere die Bindung des Auftragsverarbeiters an die Weisungen des Auftraggebers (Art. 26 Abs. 2 lit a) EU-DSGVO-E) aus.

Diese besondere Bindung begründet eine Privilegierung der Auftragsverarbeitung gegenüber sonstigen Datenübermittlungen an Dritte und rechtfertigt eine Befreiung von der Zulässigkeitsprüfung nach Art. 6 Abs. 1 lit. f und Art. 7 EU-DSGVO-E. Wie sich aus Art. 26 Abs. 4 EU-DSGVO-E indirekt ergibt, geht die EU-DSGVO-E von einer solchen Privilegierung in der Sache auch aus. Im Interesse der Rechtssicherheit für die für die Verarbeitung Verantwortlichen, die Auftragsverarbeiter und die Betroffenen wäre eine weitergehende und explizite Klarstellung dieser Privilegierung wünschenswert.

Die nach Art. 26 Abs. 2 lit. a) und Abs. 3 EU-DSGVO-E vorgesehene strikte Weisungsgebundenheit des Auftragsverarbeiters steht im Widerspruch dazu, dass der Auftragsverarbeiter in einigen Regelungen der EU-DSGVO-E neben dem Auftraggeber in die Pflicht genommen wird. Denn aufgrund der Weisungsgebundenheit stehen dem Auftragsverarbeiter keine eigenständigen Entscheidungsbefugnisse zu. Diese Situation ist für den Auftragsverarbeiter nicht konfliktfrei zu lösen. Wir begrüßen es daher, wenn im Zuge der weiteren Konkretisierung der Auftragsverarbeitung die primäre Verantwortlichkeit des Auftraggebers klargestellt wird.

Art. 26 Abs. 4 EU-DSGVO-E betrachtet den Auftragsverarbeiter als für die Verarbeitung Verantwortlichen, wenn der Auftragsverarbeiter „personenbezogene Daten auf eine andere als die ihm von dem für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet“. Dieser Ansatz ist zur Verdeutlichung der Verantwortlichkeit gegenüber dem Auftragsverarbeiter und zum Schutz der Betroffenen begrüßenswert. Die Rechtsfolge der gemeinsamen Verantwortlichkeit nach Art. 24 EU-DSGVO-E erscheint in einer Mehrzahl der Fälle nicht adäquat. Denn Art. 26 Abs. 4 EU-DSGVO-E erfasst nicht nur die Fälle, in denen der Auftragsverarbeiter bewusst und zielgerichtet seine Rolle als Auftragsverarbeiter „verlässt“, sondern auch solche Fälle, in denen versehentlich aufgrund eines Fehlers und/oder unerkannt aufgrund eines Missverständnisses eine Überschreitung der Weisungsgebundenheit erfolgt. In diesen Fällen wird die nicht weisungsgebundene Tätigkeit mit Erkennen der Überschreitung der Weisung eingestellt, sodass die Abstimmung nach Art. 24 EU-DSGVO-E nicht sinnvoll ist.

5. Hinweis: Gleichstellung von Sozialdaten mit Gesundheitsdaten in Art. 81 EU-DSGVO-E

Im Gesundheitsbereich existiert in allen Mitgliedsländern der EU eine Vielzahl spezifischer Regelungen. Diese sind notwendig, um den besonderen Anforderungen einzelner Bereiche gerecht zu werden. Als Beispiel seien Transplantationsgesetz, Krebsregistergesetze der Länder, Ärztliche Berufsordnungen und auch das neue Patientenrechtegesetz genannt. In der jetzigen Entwurfsfassung ist nicht klar, in welchem Verhältnis diese spezifischen Regelungen und insbesondere § 203 StGB (Verletzung von Privatgeheimnissen) zur EU-DSGVO-E stehen.

In Art 81 EU-DSGVO-E werden die Gesundheitsdaten definiert. Der Artikel 81 stellt sehr stark auf den ärztlich geleiteten Versorgungsbereich mit den notwendigen behandlungsbegleiteten Maßnahmen, wie Praxis- und Klinikverwaltung oder Heilmittelverordnung ab. In der heutigen, gesundheitspolitischen gewollten und geförderten, sektorenübergreifenden Versorgung von Patienten nehmen eine Vielzahl von Personen teil, die ihre Leistung **nicht** unter ärztlicher Leitung erbringen. Die Daten, die hier erhoben werden, sind die sog. Sozialdaten, die zwar über keinen direkten Gesundheitsbezug verfügen, aber genauso viel über das tiefste Innere des Menschen aussagen. Solche Daten werden von ambulanten Diensten, Beratungsstellen oder sonstigen Versorgungsteilnehmern erhoben. Die gesundheitspolitischen Ziele und die Kostenträger forcieren den Zusammenschluss von Anbietern der stationären oder ambulanten Versorgung und der Nachsorge in verschiedenen Formen. Durch die enge Fassung des Begriffs „Gesundheit“ entsteht ein Bruch im Schutzbedarf der Daten zwischen schützenswerten Daten aus der ärztlichen Anleitung und den Daten aus der Hilfeversorgung.

Sozialdaten aus Patienten- und Klientenversorgungsprozessen sind aus Sicht des BvD zu behandeln wie Gesundheitsdaten. Daher sind Sozialdaten und Gesundheitsdaten in der EU-DSGVO-E gleich zu behandeln.

6. Hinweis: Bagatellklausel bei Security Breach Notification

Der BvD begrüßt die Einführung einer Security Breach Notification in Art. 31 und 32 EU-DSGVO-E. Diese Informationspflicht bei der Verletzung des Schutzes personenbezogener Daten ist die konsequente Fortsetzung des Gebots der Transparenz. Denn durch diese Informationspflicht wird die betroffene Person gerade dann in die Lage versetzt, sich selbst zu schützen, wenn eine Verletzung des Schutzes ihrer personenbezogenen Daten durch sie selbst nicht wahrgenommen werden kann.

Durch die zweistufige Ausgestaltung der Informationspflicht erfolgt eine differenzierte Pflicht zur Information, welche für die Verpflichteten gegenüber der Regelung in §§ 42a BDSG, 15a TMG einen Mittelweg darstellt. Denn es erfolgt eine Unterrichtung der Aufsichtsbehörde unterhalb der Schwelle zur Unterrichtung der Betroffenen. Damit kann in Abstimmung mit den Aufsichtsbehörden über das weitere Vorgehen gesprochen werden. Gleichzeitig erhalten die Aufsichtsbehörden auch unterhalb der Schwelle einer Beeinträchtigung der betroffenen Person einen Eindruck von der „Sicherheitslage“.

In Bezug auf die Unterrichtung der Betroffenen muss jedoch eine Erheblichkeitsschwelle eingefügt werden. Denn mit Blick auf die Tragweite der Information der Betroffenen muss dem Verhältnismäßigkeitsgrundsatz dadurch Rechnung getragen werden, dass nur bei Drohen „schwerer“, „schwerwiegender“ oder „erheblicher“ Beeinträchtigungen eine Informationspflicht besteht.
Eine Informationspflicht unter dieser Schwelle dient auch nicht dem Schutz der betroffenen Person. Denn ohne diese Schwelle erhält die betroffene Person eine solche Vielzahl an Hinweisen, dass sie abstumpft und die Hinweise auf die wirklich gefährdenden Verletzungen des Schutzes personenbezogener Daten aufgrund dieser „Abstumpfung“ nicht hinreichend zur Kenntnis genommen werden.
Mit Blick auf die Interessen aller Beteiligten wird daher empfohlen, eine Bagatellgrenze bzw. eine Erheblichkeitsschwelle einzufügen.

7. Hinweise zum Dialog

Die bisherigen Regelungen

- zur Einwilligung bei „erheblichem Ungleichgewicht der Beteiligten (Art. 7 Abs. 4 EU-DSGVO-E),
- das Verhältnis zu Rechtsvorschriften in Mitgliedsländern zu weiteren berufsrechtlichen Verschwiegenheitsverpflichtungen (z. B. Rechtsanwälte, Steuerberater, Amtsträger) und
- die Einführung von zwingenden Informationspflichten in Art. 31 und Art. 32 EU-DSGVO-E ohne Begrenzung auf Risikodaten und ohne ein Tatbestandmerkmal der drohenden schwerwiegenden Beeinträchtigung (wie in § 42a Deutsches Bundesdatenschutzgesetz)

bedürfen einer Anpassung, um in der Praxis ohne Einbußen für den Schutz der Persönlichkeitsrechte noch umsetzbar für die Unternehmen und öffentlichen Stellen (Behörden) zu bleiben. In diesen Fällen kann ein Datenschutzbeauftragter als Berater nur eine dem freien Datenverkehr entgegenlaufende Empfehlung geben, um seinen Arbeitgeber / Auftraggeber nicht dem Risiko einer existenzgefährdenden Sanktion auszusetzen. Mit wenigen Klarstellungen und Änderungen in den Formulierungen können hier durch Eindeutigkeit und Praxisnähe Verbesserungen für die Unternehmen und die Rechtssicherheit der Betroffenen erreicht werden.

IV. Bereitschaft des BvD zum Dialog

Der BvD steht gerne bereit, bei der Verbesserung der Ziele der EU-DSGVO zu unterstützen und behält sich vor, auch im weiteren Gesetzgebungsverfahren mit Anmerkungen und Vorschlägen beizutragen, eine neue Rechtslage zu schaffen, die den Unternehmen, Behörden und deren Datenschutzbeauftragten eine in ganz Europa einheitlich geltende, praxisnahe Rechtssicherheit vermittelnde und die Wahrung der Persönlichkeitsrechte der betroffenen Personen gewähr-leistende Datenschutzgrundlage garantiert.