Teil A Compliance

In Teil A geht es um die wichtigsten Vorkehrungen und Maßnahmen, die im Unternehmen zu treffen sind, um Konformität mit dem neuen Datenschutzrecht zu erreichen. Es geht um Technik und Organisation, um Dokumentation und unternehmensinterne Richtlinien, um Transparenz und um die grundlegenden Prinzipien des neuen Datenschutzrechts. 1

Die DSGVO hat das erklärte Ziel, dem Datenschutz in der behördlichen und betrieblichen Praxis mehr Geltung zu verschaffen. Datenschutzverstöße sind in Zukunft keine „Kavaliersdelikte" mehr. Es drohen Geldbußen bis zu 20 Mio. Euro bzw. 4 % des weltweiten Jahresumsatzes eines Unternehmens. 2

Ob und inwieweit die Datenschutzbehörden von ihren erweiterten Sanktionsrechten Gebrauch machen werden, bleibt abzuwarten. Der drastisch erweiterte Bußgeldrahmen erhöht jedenfalls den Compliance-Druck. Der Datenschutz wird in den nächsten Jahren einen Spitzenplatz unter den Compliance-Themen erobern. 3

Merke:

Mit den neun wichtigsten Compliance-Themen sollte sich jedes Unternehmen vertraut machen: 4

- Bestellung eines betrieblichen Datenschutzbeauftragten
- Dokumentation und Folgenabschätzung
- Datenschutzerklärungen und Transparenz
- Allgemeine Datenschutzprinzipien und „risikobasierter Ansatz"
- Technische und organisatorische Maßnahmen
- Meldepflichten bei Datenpannen
- Datentransfer in Drittstaaten
- Territorialer Anwendungsbereich der DSGVO
- Haftung, Rechtsbehelfe, Sanktionen

I. Betriebliche Datenschutzbeauftragte

1. Wann muss ein Datenschutzbeauftragter bestellt werden?

■ *Geltendes Recht*

Nach § 4 f Abs. 1 BDSG besteht für die meisten Unternehmen die Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten. Ausnahmen gelten nur für Unternehmen, in denen 5

- höchstens 9 Personen personenbezogene Daten *automatisiert* verarbeiten,

– weniger als 20 Personen personenbezogene Daten *nicht-automatisiert* verarbeiten,
– keine personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeitet werden und
– keine automatisierte Verarbeitung erfolgt, die einer Vorabkontrolle unterliegt.

6 Es gibt heute kaum noch ein Unternehmen ohne Computer. Jedenfalls Mitarbeiter- und Kundendaten werden in fast jedem Unternehmen automatisiert verarbeitet. Daher sind Unternehmen mit mehr als neun Beschäftigten, die Zugang zum Betriebscomputer haben, in aller Regel zur Bestellung eines betrieblichen Datenschutzbeauftragten verpflichtet.

Änderungen durch die DSGVO

7 Nach Art. 37 Abs. 1 lit. b und c DSGVO ist in einem Unternehmen immer dann ein Datenschutzbeauftragter zu bestellen, wenn zu den Kernaktivitäten des Unternehmens

– die „umfangreiche regelmäßige und systematische Überwachung" von Betroffenen oder
– die „umfangreiche Verarbeitung" sensitiver Daten zählt:

„b) 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

c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht."

8 Anders als nach § 4 f Abs. 1 BDSG kommt es nicht auf die Zahl der im Betrieb Beschäftigten an.

9 Nicht viele Unternehmen werden die Voraussetzungen des Art. 37 Abs. 1 DSGVO erfüllen. Weder das mittelständische Maschinenbauunternehmen noch der durchschnittliche Online-Händler „überwachen" in größerem Umfang die Aktivitäten ihrer Kunden oder verarbeiten sensitive Daten beispielsweise über politische Meinungen oder genetische Informationen ihrer Kunden (Art. 9 DSGVO). Selbst wenn – beispielsweise per Google Analytics – Daten über das Kundenverhalten erhoben werden, zählt dies nicht zu den „Kernaktivitäten" der meisten Unternehmen.

10 Die DSGVO macht somit die Bestellung eines betrieblichen Datenschutzbeauftragten in zahlreichen Fällen verzichtbar. Im Vergleich zum geltenden deut-

schen Recht entsteht eine erhebliche Lücke, die der deutsche Gesetzgeber allerdings jederzeit schließen kann. Denn Art. 37 Abs. 4 DSGVO enthält eine Öffnungsklausel, die es dem nationalen Gesetzgeber erlaubt, die Bestellung eines betrieblichen Datenschutzbeauftragten auch dann zur Pflicht zu erklären, wenn die Voraussetzungen des Art. 37 Abs. 1 DSGVO nicht erfüllt sind. Es ist zu erwarten, dass der deutsche Gesetzgeber von dieser Öffnungsklausel Gebrauch machen wird. Aller Voraussicht nach wird es dabei bleiben, dass in aller Regel betriebliche Datenschutzbeauftragte bestellt werden müssen.

Merke:

> Ob und unter welchen Voraussetzungen nach Inkrafttreten der DSGVO noch betriebliche Datenschutzbeauftragte bestellt werden müssen, ist derzeit offen. Der deutsche Gesetzgeber wird sich entscheiden müssen, ob er die derzeitige Regelung (§ 4 f Abs. 1 BDSG) bestehen lässt oder Änderungen vornimmt. Die DSGVO lässt dem nationalen Gesetzgeber freie Hand. 11

2. Was ist bei der Bestellung eines Datenschutzbeauftragten zu beachten?

■ *Geltendes Recht*

Weder die Geschäftsleitung noch der Betriebsinhaber können sich selbst zum Datenschutzbeauftragten bestellen. Es bedarf somit entweder der Ernennung eines fachkundigen und zuverlässigen Mitarbeiters oder der Beauftragung eines externen Beraters zum Datenschutzbeauftragten. Die Fachkunde des Datenschutzbeauftragten ist auf Verlangen der Aufsichtsbehörde durch Ausbildungs- und Schulungsbescheinigungen nachzuweisen. 12

Bei kleineren Unternehmen handelt es sich zumeist um ein Nebenamt. Dieses Nebenamt darf nicht mit anderen Aufgaben des Datenschutzbeauftragten kollidieren, um auszuschließen, dass sich der Datenschutzbeauftragte bei der Ausübung seines Amtes selbst kontrollieren muss. 13

Organisatorisch ist Folgendes zu beachten: 14

- Der Datenschutzbeauftragte ist der Geschäftsleitung organisatorisch unmittelbar zu unterstellen (§ 4 f Abs. 3 Satz 1 BDSG).
- Der Datenschutzbeauftragte agiert bei der Ausübung seines Amts weisungsfrei (§ 4 f Abs. 3 Satz 2 BDSG).
- Dem Datenschutzbeauftragten ist die Möglichkeit der Fortbildung zu geben (§ 4 f Abs. 3 Satz 7 BDSG).
- Dem Datenschutzbeauftragten sind Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist (§ 4 f Abs. 5 Satz 1 BDSG).
- Wenn der Datenschutzbeauftragte Arbeitnehmer ist, genießt er erweiterten Kündigungsschutz nach § 4 f Abs. 3 Satz 5 und 6 BDSG.

■ *Änderungen durch die DSGVO*

15 Die Bestellung des Datenschutzbeauftragten ist in Art. 37 und 38 DSGVO geregelt:

- Der Datenschutzbeauftragte ist – wie bisher – der obersten Managementebene unmittelbar zu unterstellen (Art. 38 Abs. 3 Satz 3 DSGVO).
- Die Weisungsfreiheit bei der Ausübung der Funktion ist in Art. 38 Abs. 3 Satz 1 DSGVO – unverändert – festgeschrieben.
- Dem Datenschutzbeauftragten sind die für die Erfüllung seiner Aufgaben und zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen (Art. 38 Abs. 2 DSGVO).
- Nach Art. 37 Abs. 6 DSGVO kann der Datenschutzbeauftragte Beschäftigter des Verantwortlichen bzw. Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.
- Anders als das geltende Recht sieht Art. 37 Abs. 2 DSGVO die Möglichkeit der Bestellung eines einheitlichen Datenschutzbeauftragten für einen Konzern ausdrücklich vor, sofern dessen leichte Erreichbarkeit für die konzernangehörigen Unternehmen gewährleistet ist.
- Nach Art. 38 Abs. 3 Satz 2 DSGVO darf der Datenschutzbeauftragte im Zusammenhang mit der Erfüllung seiner Aufgaben weder abberufen noch benachteiligt werden. Dies bleibt deutlich hinter dem erweiterten Kündigungsschutz nach § 4 f Abs. 3 Satz 5 und 6 BDSG zurück.

Merke:

16 Anders als nach dem BDSG kann ein Datenschutzbeauftragter nach der DSGVO auch per ordentlicher Kündigung entlassen werden. Der Ausschluss des ordentlichen Kündigungsrechts entfällt. Ausgeschlossen ist lediglich eine Kündigung, die sich auf Gründe stützt, die mit der Ausübung des Amtes zusammenhängen.

Anders als nach dem BDSG endet der besondere Kündigungsschutz des Datenschutzbeauftragten nach der DSGVO mit der Beendigung des Amtes. Das Fortwirken des besonderen Kündigungsschutzes über die Amtszeit hinaus (ein Jahr) entfällt.

Die Öffnungsklausel des Art. 37 Abs. 4 DSGVO gilt nur für die Bestellung eines Datenschutzbeauftragten, nicht jedoch für dessen Abberufung und für die Kündigung, sodass für den deutschen Gesetzgeber keine Möglichkeit besteht, an dem bisherigen, erweiterten Kündigungsschutz festzuhalten.

3. Welche Aufgaben und Befugnisse hat der Datenschutzbeauftragte?

■ *Geltendes Recht*

Die Aufgaben und Befugnisse des Datenschutzbeauftragten sind in § 4 g BDSG geregelt. Danach wirkt der Datenschutzbeauftragte darauf hin, dass die Bestimmungen des BDSG und andere datenschutzrechtliche Bestimmungen eingehalten werden. Zudem obliegt es dem Datenschutzbeauftragten, 17

– die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme zu überwachen, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen (§ 4 g Abs. 1 Satz 4 Nr. 1 BDSG), und
– die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Bestimmungen des BDSG und mit anderen datenschutzrechtlichen Vorschriften über den Datenschutz sowie mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen (§ 4 g Abs. 1 Satz 4 Nr. 2 BDSG).

Der Datenschutzbeauftragte ist nach geltendem Recht nicht zur Zusammenarbeit mit den Aufsichtsbehörden verpflichtet. Er ist auch nicht die zentrale Beschwerdestelle für Anfragen von Mitarbeitern, Kunden und Nutzern, die sich durch die betriebliche Datenverarbeitung betroffen fühlen. Nach außen beschränken sich die Aufgaben des Datenschutzbeauftragten auf die Überlassung eines externen Verfahrensverzeichnisses an jedermann für den Fall, dass dies beantragt wird (§ 4 g Abs. 2 Satz 2 BDSG). Zudem ist der Datenschutzbeauftragte zur Vorabkontrolle in den Fällen des § 4 d Abs. 5 BDSG verpflichtet (§ 4 d Abs. 6 Satz 1 BDSG). 18

■ *Änderungen durch die DSGVO*

Bestimmungen zu den Aufgaben und Befugnissen des Datenschutzbeauftragten finden sich in Art. 38 und 39 DSGVO. Anders als Art. 37 DSGVO enthalten die Art. 38 und 39 DSGVO keine Öffnungsklausel für den nationalen Gesetzgeber. Dies wird man so verstehen müssen, dass die Art. 38 und 39 DSGVO auch dann verbindlich sind, wenn die Bestellung eines Datenschutzbeauftragten nicht nach Art. 37 Abs. 1 DSGVO, sondern lediglich aufgrund des Datenschutzrechts eines Mitgliedstaates erforderlich ist (Art. 37 Abs. 4 DSGVO). 19

Art. 38 und 39 DSGVO enthalten zahlreiche Neuerungen: 20

– Zu den Aufgaben des Datenschutzbeauftragten gehört nach Art. 39 Abs. 1 lit. b DSGVO neben der Schulung von Mitarbeitern auch deren „Sensibilisierung“ für den Datenschutz.
– Nach Art. 38 Abs. 4 DSGVO wird der Datenschutzbeauftragte zum Ansprechpartner jedes Betroffenen, der Fragen zu den Datenverarbeitungsprozessen in dem jeweiligen Unternehmen hat oder Rechte geltend machen möchte, die ihm nach der DSGVO zustehen.

- Die Verpflichtung nach Art. 38 Abs. 4 DSGVO wird dadurch verstärkt, dass die DSGVO in Art. 13 Abs. 1 lit. b und Art. 14 Abs. 1 lit. b die Bekanntgabe des Namens und der Kontaktdaten des Datenschutzbeauftragten vorschreibt. Die Tragweite dieser Neuerung ist nicht zu unterschätzen. Bislang war ein Unternehmen nur gegenüber der Aufsichtsbehörde zu Angaben über den bestellten Datenschutzbeauftragten verpflichtet. Eine Verpflichtung zur Preisgabe des Namens und weiterer Informationen an Dritte gibt es nach geltendem Recht nicht.
- Art. 39 Abs. 1 lit. d und e DSGVO führt umfassende Verpflichtungen des Datenschutzbeauftragten zur Zusammenarbeit mit den Aufsichtsbehörden ein. Anders als nach bisherigem Recht wird der Datenschutzbeauftragte zum zentralen Ansprechpartner der Aufsichtsbehörden.
- Art. 39 Abs. 2 DSGVO verpflichtet den Datenschutzbeauftragten, bei allen Maßnahmen eine Angemessenheitsprüfung vorzunehmen, die sich an den Risiken des jeweiligen Verfahrensvorgangs orientiert. Verallgemeinernd lässt sich hieraus die Verpflichtung ableiten, die eigene Tätigkeit nicht ausschließlich an der bestmöglichen Durchsetzung des Datenschutzrechts auszurichten, sondern andere betriebliche Belange im Auge zu behalten. Je geringer die Risiken einer Datenverarbeitung sind, desto weniger können sie der bestimmende Maßstab für unternehmerische Entscheidungen sein.

Merke:

21 Art. 38 Abs. 4 DSGVO und die Kooperationspflichten gemäß Art. 39 Abs. 1 lit. d und e DSGVO sind konfliktträchtig für den Datenschutzbeauftragten, der bei der Zusammenarbeit mit den Aufsichtsbehörden sowie bei Auskünften, die er Kunden, Nutzern und anderen Betroffenen erteilt, nicht nur die Anforderungen des Datenschutzrechts, sondern auch die berechtigten Interessen des Unternehmens im Auge behalten muss. Art. 38 Abs. 4 DSGVO und Art. 39 Abs. 1 lit. d und e DSGVO geben dem Datenschutzbeauftragten beispielsweise keine Befugnis zur Preisgabe von Betriebs- und Geschäftsgeheimnissen (§ 17 UWG) oder zur Preisgabe von Geheimnissen, die einer Verschwiegenheitspflicht unterliegen (§ 203 StGB).

Es dürfte zumindest ratsam sein, dass sich die Geschäftsleitung mit dem Datenschutzbeauftragten über Regeln für interne Abstimmungsprozesse verständigt für den Fall, dass sich ein Bürger nach Art. 38 Abs. 4 DSGVO unmittelbar an den Datenschutzbeauftragten wendet. Auch über einige Grundregeln der Zusammenarbeit mit den Aufsichtsbehörden sollten sich die Geschäftsleitung und der Datenschutzbeauftragte verständigen.

II. Dokumentation und Folgenabschätzung (Vorabkontrolle)

4. Was wird aus den Verfahrensverzeichnissen?

■ *Geltendes Recht*

Selbst in kleineren Unternehmen ist es nicht immer einfach, den Überblick über die eigenen Datenverarbeitungsprozesse zu behalten. Dies umso mehr als einzelne Prozesse in die Cloud verlagert werden. Wenn Terminkalender und die Kundendatenbank in der Cloud geführt werden, sind die Daten auf den Unternehmensservern nicht mehr sichtbar. Bei einem Datenschutz-Audit kann es leicht passieren, dass derartige Prozesse übersehen werden. 22

Nach geltendem Recht wird die Transparenz der Datenverarbeitungsprozesse durch Verfahrensverzeichnisse gesichert. Die Führung eines Verfahrensverzeichnisses nach § 4 g Abs. 2 Satz 1 i. V. m. § 4 e Satz 1 BDSG gehört zu den Kernaufgaben des betrieblichen Datenschutzbeauftragten. 23

Bei den Verfahrensverzeichnissen geht es weniger um Software als um Prozesse, beispielsweise um Kundendatenbanken, die Verwaltung der Mitarbeiterdaten in der Personalabteilung, um den Internetauftritt, den Terminkalender und die Finanzbuchhaltung. Jeder dieser Prozesse muss in einem Verfahrensverzeichnis in Grundzügen beschrieben werden. 24

§ 4 e Abs. 1 Satz 1 BDSG schreibt folgende Angaben vor: 25

- Name oder Firma sowie Anschrift der verantwortlichen Stelle;
- Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen;
- Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung;
- Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien;
- Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können;
- Regelfristen für die Löschung der Daten;
- Datenübermittlung in Drittstaaten, falls geplant;
- eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die technischen und organisatorischen Maßnahmen nach § 9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

■ *Änderungen durch die DSGVO*

Art. 30 Abs. 1 DSGVO entspricht § 4 e Satz 1 BDSG und listet die Angaben auf, die ein Verfahrensverzeichnis enthalten muss: 26

„Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält sämtliche folgenden Angaben:

a) den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

b) die Zwecke der Verarbeitung;

c) eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;

d) die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;

e) gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

f) wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;

g) wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1."

27 Anders als nach bisherigem Recht gibt es eine (teilweise) Befreiung von der Pflicht zu Verfahrensverzeichnissen für kleinere Unternehmen (Art. 30 Abs. 5 DSGVO):

„Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, sofern die von ihnen vorgenommene Verarbeitung nicht ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich erfolgt oder nicht die Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt."

28 Unternehmen mit weniger als 250 Beschäftigten müssen somit nicht für jedes Verarbeitungsverfahren ein Verzeichnis anlegen, sondern nur für Verfahren, die

- mit einem erheblichen Risiko für die Betroffenen verbunden sind (z. B. Videoüberwachung) oder
- nicht nur gelegentlich angewendet werden oder
- sensitive Daten (z. B. Gesundheitsdaten oder Daten aus einem Strafregister) umfassen.

Merke:

> Die Ausnahme gilt nur für „gelegentliche" Verfahren. Daher gibt es für alle Grundfunktionen des Unternehmens (z. B. Finanzbuchhaltung; Personalakten; Kundendatenbank) keine Änderung. Es bleibt bei der Verpflichtung zur Führung von Verfahrensverzeichnissen. 29

Art. 30 DSGVO weist drei weitere Besonderheiten gegenüber dem geltenden Recht auf: 30

- Anders als nach der bisherigen Praxis ist die Unternehmensleitung und nicht der betriebliche Datenschutzbeauftragte für die Verfahrensverzeichnisse verantwortlich (Art. 30 Abs. 1 DSGVO).
- Auch der Auftragsverarbeiter ist nach Art. 30 Abs. 2 DSGVO zur Führung von Verfahrensverzeichnissen verpflichtet.
- Nach der DSGVO gibt es kein „Jedermanns-Recht" auf Einsicht in die Verfahrensverzeichnisse. Die Führung externer Verzeichnisse zur Erfüllung der Verpflichtung nach § 4 g Abs. 2 Satz 2 BDSG wird entbehrlich.
- Bei einem Datentransfer in einen Drittstaat auf der Grundlage des Art. 49 Abs. 1 Satz 2 DSGVO sind die Risikoabschätzung und die ergriffenen Schutzmaßnahmen nach Art. 28 DSGVO zu dokumentieren (Art. 49 Abs. 6 DSGVO). Bei einem neuen Verarbeitungsverfahren ist somit ein neues Verzeichnis zu erstellen, anderenfalls ist das bereits bestehende Verzeichnis um die durch Art. 49 Abs. 6 DSGVO vorgeschriebenen Angaben zu ergänzen.

Merke:

> Bei der Funktion der Verzeichnisse gemäß Art. 30 DSGVO lässt sich eine leichte Akzentverschiebung beobachten. Geht es in § 4 g Abs. 2 Satz 1 i. V. m. § 4 e Satz 1 BDSG maßgeblich um ein jeweils aktuelles Bild der Datenverarbeitungsverfahren, die im Unternehmen praktiziert werden, kommt durch Art. 30 DSGVO eine historische Komponente hinzu. Art. 30 DSGVO soll den Aufsichtsbehörden auch für die Vergangenheit die Möglichkeit eröffnen, Datenverarbeitungsverfahren zu untersuchen. 31
>
> Wegen der historischen Komponente erscheint es ratsam, die jeweils aktuellen Verfahrensverzeichnisse in ein umfassendes Dokumentationssystem einzubinden. Alle Änderungen und Ergänzungen sowie die Neuanlegung und Schließung von Verzeichnissen sollten lückenlos unter Verwendung von Zeitstempeln dokumentiert werden.

5. Was wird aus der Vorabkontrolle?

■ *Geltendes Recht*

32 Nach § 4 d Abs. 5 und Abs. 6 Satz 1 BDSG ist der Datenschutzbeauftragte zu einer Vorabkontrolle verpflichtet, wenn automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Dies ist insbesondere der Fall, wenn

- besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) verarbeitet werden (§ 4 d Abs. 5 Satz 2 Nr. 1 BDSG) oder
- die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens (§ 4 d Abs. 5 Satz 2 Nr. 2 BDSG).

33 Die Regelungen zur Vorabkontrolle in § 4 d Abs. 5 und 6 BDSG beantworten die Frage nach dem „Ob" einer solchen Kontrolle, lassen jedoch das „Wie" vollkommen offen. In welcher Weise der Datenschutzbeauftragte seine Pflicht nach § 4 d Abs. 6 Satz 1 BDSG zu erfüllen hat und welche Prüfungsmaßstäbe für eine Vorabkontrolle gelten, ist gesetzlich nicht geregelt. Geregelt ist lediglich, dass der Datenschutzbeauftragte „in Zweifelsfällen" die zuständige Datenschutzbehörde zu verständigen hat (§ 4 d Abs. 6 Satz 3 BDSG).

■ *Änderungen durch die DSGVO*

34 Durch die DSGVO tritt eine Folgenabschätzung an die Stelle der Vorabkontrolle. Anders als bei der Vorabkontrolle ist der Datenschutzbeauftragte nicht für die Durchführung einer Vorabkontrolle verantwortlich. Er muss lediglich hinzugezogen werden zum Zwecke der Beratung der Geschäftsleitung (Art. 35 Abs. 2 und Art. 39 Abs. 1 lit. c DSGVO).

6. Wann ist eine Folgenabschätzung erforderlich?

35 Wenn ein neues Verfahren der Datenverarbeitung eingesetzt werden soll, das mit einem „hohen Risiko" für die Betroffenen verbunden ist, ist nach Art. 35 Abs. 1 DSGVO eine Folgenabschätzung vorzunehmen:

> „Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden."

36 Art. 35 Abs. 3 DSGVO enthält Regelbeispiele, die § 4 d Abs. 5 Satz 2 BDSG ähneln: