Neues Datenschutzrecht

in der Reihe:

Bearbeitungs- und Prüfungsleitfaden

Prozesse prüfen * Risiken vermeiden * Fehler aufdecken
→ Handlungsempfehlungen ableiten

Finanz Colloquium Heidelberg, 2019

Bearbeitungs- und Prüfungsleitfaden

Neues Datenschutzrecht

Mike Bona-Stecki
Manager/Auditor Informationssicherheit
DekaBank
Frankfurt am Main

Dr. Martin Andreas Duncker (Hrsg.)
Dr. Martin Andreas Duncker Rechtsanwalt und Fachanwalt für Bank- und Kapitalmarktrecht Zertifizierter Compliance-Beauftragter (IHK & TÜV) Schlatter Rechtsanwälte Steuerberater PartGmbB

Thomas Göhrig
Berater für Informationssicherheit und Datenschutz
FCH Compliance GmbH

Dr. Ulrich Hallermann (Hrsg.)
Dr. Ulrich Hallermann Rechtsanwalt und Fachanwalt für Arbeitsrecht Datenschutzbeautragter Investitions- und Strukturbank Rheinland-Pfalz (ISB)

Dr. Markus Lang
Dr. Markus Lang Rechtsanwalt Externer Datenschutzbeauftragter

Christian Maull (Hrsg.)
Spezialist Compliance
FCH Compliance GmbH
Heidelberg

Dr. Stephanie Müller
Referentin beim Bundesbeauftragten
für den Datenschutz und die Informationsfreiheit

Denise Primus
Rechtsanwältin
Schlatter Rechtsanwälte Steuerberater PartG mbB
Heidelberg

Jürgen Ranger
Projektleiter Strategische Projektportfoliosteuerung
Creditplus Bank AG
Stuttgart

Finanz Colloquium Heidelberg, 2019

Inhaltsübersicht

Inhaltsverzeichnis

A.

Vorwort

A. Vorwort

Zum 25. Mai 2018 trat die Europäische Datenschutz-Grundverordnung (EU-DSGVO) in Kraft und ersetzte das bisherige Bundesdatenschutzgesetz (BDSG) als maßgebende Rechtsvorschrift in Sachen Datenschutz. Parallel zur EU-DSGVO trat das neue Bundesdatenschutzgesetz in Kraft und konkretisiert die für die EU-Mitgliedsstaaten in der EU-DSGVO enthaltenen Öffnungsklauseln. 1

Im Jahre 1970 verabschiedete Hessen das erste Datenschutzgesetz der Welt und schuf somit den ersten Meilenstein des deutschen Datenschutzrechts. Seitdem folgten zahlreiche technische und rechtliche Entwicklungen und der Schutz personenbezogener Daten gewann zunehmend an Bedeutung. Aufgrund dieser Historie verwundert es nicht, dass auch in der Neuregelung des Datenschutzrechts altbekannte Themen in mehr oder minder bekanntem Umfang wiederzufinden sind. Trotz alledem ist die EU-DSGVO mehr als alter Wein in neuen Schläuchen, denn ihre Einführung brachte umfangreiche Änderungen und Herausforderungen mit sich, welche Verantwortliche Stellen noch heute beschäftigen. Die Spannbreite der Handlungsfelder reicht von Dokumentations- und Nachweispflichten, über die Umsetzung von Betroffenenrechten und technisch-organisatorischen Maßnahmen, bis hin zu Sonderkonstellationen bei Datenübermittlungen innerhalb und außerhalb eines Unternehmens oder einer Unternehmensgruppe, sowohl im europäischen In- als auch im Ausland. 2

Die Summe der einzelnen Themen und deren Verknüpfung untereinander erforderte die Einführung eines Datenschutzmanagements zur rechtskonformen Umsetzung regulatorischer Anforderungen und der gleichzeitig möglichst hohen Effektivität getroffener Maßnahmen. In seiner neuen Ausrichtung unter der EU-DSGVO wurde die Datenschutzfunktion mehr und mehr an bestehende Compliance-Funktionen angepasst und verortet sich nunmehr als Bestandteil der zweiten Verteidigungslinie im Modell der three-lines-of-defense. 3

Dieses Buch dient sowohl als Arbeitsunterlage für Datenschutzbeauftragte, Syndikusrechtsanwälte, Rechtsanwälte, Berater und Wissenschaftler, sowie als Prüfungshilfe für Revisoren und Datenschutzauditoren. Es befasst sich sowohl mit den Grundlagen des Datenschutzes als auch themenspezifischen Herausforderungen, sowie aktuellen rechtlichen Entwicklungen und Erfahrungen der Aufsichtsbehörden und unterstützt durch zahlreiche praxisorientierte Checklisten im Alltag. 4

B.

Aufsichtliche Würdigung

B. Aufsichtliche Würdigung

I. Inhalte und Bedeutung des Datenschutzmanagements

Auf Grund des bereits im 17. Jahrhundert bekannten Bankgeheimnisses werden die von den Kreditinstituten vorgehaltenen und generierten Kundendaten seit jeher mit großer Sorgfalt verwahrt. 5

Kreditinstitute speichern naturgemäß sehr viele personenbezogene Daten. Sowohl die Kontaktinformationen als auch die mit dem Zahlungsverkehr verbundenen Informationen enthalten personenbezogene Daten. Informationen des Zahlungsverkehrs können besonders schützenswerte personenbezogene Daten enthalten, da sich beispielsweise aus Arztrechnungen, Gewerkschaftsmitgliedsbeiträgen oder Spenden an Parteien Rückschlüsse ziehen lassen. Fragen des Datenschutzes sind beim operationellen Risiko zu berücksichtigen. Datenschutzverletzungen können auch Folgen für die Reputation eines Kreditinstituts haben. Da die Verstöße gegen datenschutzrechtliche Regelungen auch sehr hohe Bußgelder nach sich ziehen können, ist ein effektives Datenschutzmanagementsystem für den Verantwortlichen von großer Bedeutung. 6

Die Verantwortung für die Einhaltung von Datenschutzregelungen ist die Aufgabe des Verantwortlichen, auch wenn die Geschäftsleitung diese Aufgabe gelegentlich beim Datenschutzbeauftragten sieht. Die DS-GVO und die nationalen Vorschriften enthalten eine klare Aufgabenzuweisung beim Verantwortlichen. Der Datenschutzbeauftragte berät die Geschäftsleitung hinsichtlich der Einhaltung von datenschutzrechtlichen Vorschriften und führt ggf. entsprechende Kontrollen durch. Darüber hinaus ist die Beratungsfunktion des Datenschutzbeauftragten sowohl für Mitarbeiter als auch für Externe von großer Bedeutung. Datenschutzaufsichtsbehördlicher Sicht ist der Datenschutzbeauftragte neben dem Verantwortlichen selbst der Ansprechpartner bei datenschutzrechtlichen Fragestellungen. Durch regelmäßige Schulungen der Mitarbeiter können diese für die Fragen des Datenschutzes im Arbeitsalltag sensibilisiert werden. Erfahrungsgemäß lassen sich mittels Hinweisen und einfachen Hilfestellungen einige Datenschutzverstöße vermeiden. Eine regelmäßige Überprüfung der internen Vorgaben und deren Handhabung ist ratsam, damit der Verantwortliche bei einer Kontrolle durch die Aufsichtsbehörde diesbzgl. gut vorbereitet ist. 7

II. Zuständigkeiten und Zusammenspiel der Behörden

8 Die DS-GVO enthält in ihrem sechsten Kapitel (Art. 51 bis 59 DS-GVO) Regelungen für die unabhängigen Aufsichtsbehörden. Diese werden durch die nationalen Regelungen des BDSG ergänzt.

9 Die Aufsichtsbehörden sind in jedem Mitgliedsstaat der EU bis zum 25. Mai 2018 einzurichten gewesen. Die Aufsichtsbehörden bilden ein Netzwerk bei einem materiell weitgehend harmonisierten Datenschutzrecht[1]. Dabei ist in das Netzwerk auf der Ebene der EU-Mitgliedsstaaten und das föderale System in der Bundesrepublik Deutschland zu unterscheiden. Die Datenschutzaufsichtsbehörden sind unabhängige Kontroll- und Aufsichtsstellen, Art. 52 Abs. 1 DS-GVO[2].

1. Bundesrepublik Deutschland

10 Auf Grund des Föderalismus in der Bundesrepublik Deutschland ist die Datenschutzaufsicht föderal organisiert. Jedes Land verfügt über mindestens eine Datenschutzaufsichtsbehörde, darüber hinaus hat auch der Bund eine eigene Datenschutzaufsichtsbehörde. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit ist zuständig für die Einrichtungen des Bundes sowie die Post- und Telekommunikationsunternehmen. Im Fall der Bundesgerichte erstreckt sich die Zuständigkeit nur auf Verwaltungstätigkeiten und nicht die Aufgaben der Justiz[3]. Darüber hinaus ist er auch im Bereich der Finanzbehörden im Anwendungsbereich der Abgabenordnung zuständig, durch Landesgesetz können im Bereich der Finanzbehörden weitere Aufgaben übertragen werden. Bislang hat hiervon lediglich die Freie und Hansestadt Hamburg Gebrauch gemacht. Für die Rundfunkanstalten und Religionsgemeinschaften[4] existieren gesonderte Datenschutzbeauftragte, auf die hier nicht eingegangen wird. Die Landesbeauftragten sind für die Aufsicht über die Landesbehörden und im Regelfall auch für den nichtöffentlichen Bereich zuständig, also die Privatwirtschaft[5].

1 Von Lewinski, Datenschutzaufsicht als Netzwerk in Europa, NVwZ 2017, 1483.
2 So bereits zur Richtlinie 95/46/EG Urteil des EuGH (Große Kammer) vom 9. März 2010, C-518/07, Kommission/Deutschland.
3 Vgl. § 9 Abs. 2 BDSG.
4 Dies ermöglichen Art. 85 und 91 DS-GVO.
5 In Bayern wurde entschieden, die Datenschutzaufsicht für den öffentlichen und nichtöffentlichen Bereich auf zwei Behörden aufzuteilen.

Die Datenschutzaufsichtsbehörden unterstützen sich u. a. im Wege der Amtshilfe. Hierzu dürfen auch personenbezogene Daten übermittelt werden, §§ 16 Abs. 5 S. 2, 40 Abs. 3 S. 1 Hs. 2 BDSG. 11

Damit die deutschen Datenschutzaufsichtsbehörden das Recht gleich auslegen, existieren nationale Koordinierungsgremien, in denen datenschutzrechtliche Fragen diskutiert werden. Im Arbeitskreis Kreditwirtschaft, einem Arbeitskreis der Datenschutzkonferenz, tauschen sich die deutschen Aufsichtsbehörden zu datenschutzrechtlichen Fragen der Kreditwirtschaft aus. An diesen Treffen nehmen auch regelmäßig Vertreter der Kreditwirtschaft teil. 12

Darüber hinaus existiert die sogenannte zentrale Anlaufstelle beim Bundesbeauftragen für den Datenschutz und die Informationsfreiheit. Diese Stelle ist jedoch organisatorisch von diesem getrennt[6]. Sie ist die Anlaufstelle für Aufsichtsbehörden anderer Mitgliedsstaaten, den Europäischen Datenschutzausschuss und die Kommission[7], um eine schnelle und reibungslose Zusammenarbeit mit den deutschen Aufsichtsbehörden zu gewährleisten. Durch die zentrale Anlaufstelle müssen außerhalb der Bundesrepublik Deutschland nicht die innerstaatlichen Zuständigkeiten bekannt sein. Auch die deutschen Aufsichtsbehörden können sich der zentralen Anlaufstelle bedienen, wenn sie mit den Aufsichtsbehörden oder europäischen Institutionen in Kontakt treten möchten[8]. 13

Der zentralen Anlaufstelle kommt folglich eine Unterstützungsfunktion zu und ist besonders bei den sog. Kohärenzverfahren von Bedeutung. Hoheitliche Befugnisse hat die zentrale Anlaufstelle nicht[9]. 14

2. EU

Auch auf EU-Ebene sind die Datenschutzaufsichtsbehörden der Mitgliedsstaaten miteinander vernetzt und koordinieren die Auslegung der DS-GVO. In Kapitel VII der DS-GVO (Art. 60 bis Art. 76 DS-GVO) sind die Zusammenarbeit und das Kohärenzverfahren geregelt. 15

Neben der Zusammenarbeit zwischen federführender und anderer betroffener Aufsichtsbehörde (Art. 60 DS-GVO) und der Amtshilfe (Art. 61 DS-GVO) gibt es die gemeinsamen Maßnahmen der Aufsichtsbehörden (Art. 62 16

6 BT-Drs. 18/11325, S. 90.
7 EG 119 der DS-GVO und § 17 Abs. 1 BDSG.
8 BT-Drs. 18/11325, S. 89.
9 BT-Drs. 18/11325, S. 89.

DS-GVO). Zu den gemeinsamen Maßnahmen gehören u. a. gemeinsame Untersuchungen und gemeinsame Durchsetzungsmaßnahmen.

17 In der Praxis ist wohl die Zusammenarbeit zwischen der federführender und anderen betroffenen Aufsichtsbehörden bei grenzüberschreitenden Sachverhalten gem. Art. 60 DS-GVO der häufigste Fall. Auf Grund des One-Stop-Shop-Prinzips ist die Behörde, an dem die Hauptniederlassung eines Unternehmens seinen Sitz hat, grundsätzlich die federführende Behörde. Betroffene Behörde ist die Aufsichtsbehörde bei der ggf. eine Niederlassung in einem anderen Mitgliedsstaat besteht oder an die sich ein Bürger wegen eines etwaigen Datenschutzverstoßes des Unternehmens wendet. Die federführende Aufsichtsbehörde koordiniert das Vorgehen gegen den Verantwortlichen. Können sich die federführende und die betroffene Aufsichtsbehörde auf ein Vorgehen einigen, so erlässt die federführende Aufsichtsbehörde den Entscheid gegenüber dem Unternehmen (Art. 60 Abs. 7 DS-GVO). Die Kommunikation mit der betroffenen Person obliegt der Behörde, an die sich der Bürger gewendet hat. Kommt es zu keiner Einigung, kommt es zum Kohärenzverfahren.

18 Das Kohärenzverfahren ist in Art. 63 ff. DS-GVO geregelt. Das Verfahren dient der einheitlichen Anwendung der DS-GVO in den Mitgliedsstaaten. Das Kohärenzverfahren wird durch den Europäischen Datenschutzausschuss durchgeführt. Mit Hilfe dieses Verfahrens sollen bei grenzüberschreitenden Sachverhalten widersprüchliche Entscheidungen der Datenschutzaufsichtsbehörden vermieden werden[10].

19 Plant die zuständige Aufsichtsbehörde eine im Katalog des Art. 64 Abs. 1 S. 2 DS-GVO aufgeführte Entscheidung zu treffen, so ist der Entwurf des Beschlusses dem Europäischen Datenschutzausschuss zu übermitteln. Da eine entsprechende Entscheidung von allgemeiner Bedeutung sein kann, auch wenn kein grenzüberschreitender Bezug gegeben ist, gibt der Europäische Datenschutzausschuss eine entsprechende Stellungnahme ab. Der Europäische Datenschutzausschuss sieht von einer Stellungnahme ab, wenn er in einer solchen Angelegenheit bereits schon einmal eine Stellungnahme abgegeben hat (Art. 64 Abs. 3 DS-GVO).

20 Empfehlende Stellungnahmen gibt der Europäische Datenschutzausschuss auch ab, wenn er von der zuständigen Aufsichtsbehörde, der Kommission oder dem eigenen Vorsitzenden einen entsprechenden Antrag erhalten hat,

10 Selmayr/Ehmann, in: Ehmann/Selmayr (Hrsg.), DS-GVO, Einführung Rn. 71.

Art. 64 Abs. 2 DS-GVO. Es muss sich dann um eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkung in einem Mitgliedsstaat handeln.

Stellungnahmen sind zwar nicht binden, aber werden sie nicht befolgt, so können sie Anlass für einen bindenden Beschluss sein, vgl. Art. 65 Abs. 1 lit. c DS-GVO. 21

Die bindenden Beschlüsse sind in Art. 65 DS-GVO geregelt. Sie sind ein Mittel der Streitbeilegung. Sie finden Anwendung, wenn sich die federführende und die betroffene Datenschutzaufsichtsbehörde nicht einigen können, unklar ist, welcher Aufsichtsbehörde die Federführung obliegt oder im Fall des Art. 64 Abs. 1 DS-GVO keine Stellungnahme eingeholt wurde oder die Aufsichtsbehörde der Stellungnahme nicht folgen möchte, Art. 65 Abs. 1 DS-GVO. 22

Das bisherige EU-weite Abstimmungsgremium zu datenschutzrechtlichen Fragestellungen Art.-29-Gruppe wurde am 25. Mai 2018 durch den Europäischen Datenschutzausschuss ersetzt. Der Europäische Datenschutzausschuss handelt unabhängig, Art. 69 DS-GVO. Seine Aufgaben sind in Art. 70 DS-GVO klar festgelegt. 23

Die Art.-29-Gruppe hatte lediglich beratende Funktion, der Europäische Datenschutzausschuss berät u. a. die Kommission und kann Leitlinien und Stellungnahmen veröffentlichen. Seine Beschlüsse sind gegenüber den mitgliedsstaatlichen Aufsichtsbehörden verbindlich[11]. Sie können vor dem EuGH angegriffen werden. 24

Regelungen zum Europäischen Datenschutzausschuss finden sich in den Art. 68 ff. DS-GVO. Er verfügt über eine eigene Rechtspersönlichkeit und besteht aus den Leitern der Datenschutzaufsichtsbehörden der Mitgliedsstaaten sowie dem Europäischen Datenschutzbeauftragten. Verfügt ein Mitgliedsstaat – wie Deutschland – über mehr als eine Datenschutzaufsichtsbehörde, so wird ein gemeinsamer Vertreter benannt. Für Deutschland ist dies der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit[12]. Der Stellvertreter wird durch den Bundesrat aus dem Kreis der Landesdatenschutzbeauftragten gewählt[13]. Die Kommission kann an den Sitzungen und Tätigkeiten des Europäischen Datenschutzausschusses teilnehmen, verfügt jedoch nicht über ein Stimmrecht. Die Kommission wird über die Tätigkeiten des Europäischen Datenschutzausschuss durch dessen Vorsitzenden unterrichtet. 25

11 Albrecht, in: Ehmann/Selmayr (Hrsg.), DS-GVO, Art. 68 Rn. 1.
12 § 17 Abs. 1 S. 1 BDSG.
13 § 17 Abs. 1 S. 2 BDSG.

3. Zusammenarbeit mit anderen Staaten

26 Denkbar ist, dass an der Klärung eines Falles Aufsichtsbehörden in mehreren Mitgliedsstaaten zuständig sind. Grenzüberschreitende Fälle treten auf Grund von international tätigen Unternehmen vermehrt auf und erfordern eine Zusammenarbeit der Aufsichtsbehörden, da diese nur im Hoheitsgebiet ihres Mitgliedsstaates tätig werden können. Auch die Mobilität der Menschen und die Regelungen der DS-GVO tragen dazu bei, denn es ist möglich, dass sich eine betroffene Person bei einer Datenschutzaufsichtsbehörde beschwert, obwohl sich der Sachverhalt in einem anderen Mitgliedsstaat zugetragen hat. Die DS-GVO sieht eine Beschwerdemöglichkeit unabhängig vom Wohnsitz der betroffenen Person auch in einem anderen Mitgliedsstaat ausdrücklich vor. Eine Aufsichtsbehörde ist nach Art. 4 Nr. 22 DS-GVO immer betroffen, wenn der Verantwortliche oder Auftragsverarbeiter im Hoheitsgebiet dieser Aufsichtsbehörde niedergelassen ist, die Verarbeitung erhebliche Auswirkungen auf betroffenen Personen mit Wohnsitz im Mitgliedsstaat dieser Aufsichtsbehörde hat oder eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde.

27 Für den Fall, dass mehrere Aufsichtsbehörden betroffen sind, ist grundsätzlich die Aufsichtsbehörde am Sitz der Hauptniederlassung des Verantwortlichen oder des Auftragsverarbeiters die federführende Aufsichtsbehörde[14].

28 Die Aufsichtsbehörden arbeiten dann nach den Regelungen des Art. 60 DS-GVO zusammen und bemühen sich um eine konsensuale Entscheidungsfindung. Die betroffenen Aufsichtsbehörden leisten Amsthilfe[15] und führen gemeinsame Maßnahmen[16] durch. Die federführende Behörde teilt die ihr vorliegenden zweckdienlichen Informationen mit den betroffenen Behörden und erarbeitet einen Beschlussentwurf. Die betroffenen Behörden können zu diesem Entwurf Stellung nehmen. Die federführende Behörde trägt diesen Stellungnahmen gebührend Rechnung[17]. Die federführende Behörde setzt den Verantwortlichen oder Auftragsverarbeiter über die Entscheidung in Kenntnis, die Kommunikation mit der betroffenen Person bzw. dem Beschwerdeführer ist Aufgabe der beteiligten Aufsichtsbehörde[18].

14 Nach dem One-Stop-Shop-Prinzip ist die Aufsichtsbehörde am Sitz des Unternehmens die zuständige Aufsichtsbehörde.
15 Art. 61 DS-GVO.
16 Art. 62 DS-GVO.
17 Art. 60 Abs. 3 DS-GVO.
18 Art. 60 Abs. 7, 8 DS-GVO.

Konnten sich die beteiligten Aufsichtsbehörden nicht einigen, leitet die federführende Aufsichtsbehörde das Kohärenzverfahren ein[19]. Der Europäische Datenschutzausschuss entscheidet darin mittels eines verbindlichen Entschlusses den Streit zwischen den Aufsichtsbehörden[20]. Dieser Entschluss liegt dann der Entscheidung zu Grunde, die die Aufsichtsbehörden treffen und dem Verantwortlichen/Auftragsverarbeiter und Beschwerdeführer gegenüber bekanntgeben. Die Entscheidung des Europäischen Datenschutzausschusses wird publiziert. 29

4. Aufgaben und Befugnisse der Aufsichtsbehörden

Art. 57 DS-GVO enthält einen Katalog an Aufgaben, für die die Datenschutzaufsichtsbehörden zuständig sind. Sie können in Untersuchungs-, Abhilfe-, Genehmigungsaufgaben und Beratung sowie etwaige Aufgaben nach nationalem Recht[21] unterteilt werden. Darüber hinaus haben die unabhängigen Aufsichtsbehörden auch die Aufgabe, die DS-GVO einheitlich anzuwenden, Art. 51 Abs. 2 DS-GVO. 30

Für betroffene Personen und für Datenschutzbeauftrage ist das Tätigkeitwerden der Datenschutzaufsichtsbehörde grds. kostenlos. Gebühren dürfen nur bei offenkundig unbegründeten oder exzessiven Anfragen erhoben werden, Art. 57 Abs. 4 S. 1 DS-GVO. Unternehmen können sich von ihrer zuständigen Aufsichtsbehörde ebenfalls beraten lassen. 31

Aus den Aufgaben lassen sich entsprechende Befugnisse ableiten. Diese sind in Art. 58 DS-GVO festgelegt. Neben den Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen kommt den Aufsichtsbehörden auch die Möglichkeit zu, gegen Entscheidungen der Kommission und des EDSA zu klagen. 32

In der Praxis von Bedeutung ist für das einzelne Institut sind die Möglichkeiten der Datenschutzaufsichtsbehörde der Möglichkeit der Durchführung von Kontrollen, wobei der Aufsichtsbehörde Zutritt zu sämtlichen Räumen zu gewähren ist und Informationen bereitzustellen sind. Darüber hinaus sind in der Praxis auch die Abhilfebefugnisse der Aufsichtsbehörden von großem Interesse, wie etwa die Verwarnung, die Anordnung, das Verhängen von Bußgeldern sowie die Untersagung von Datenverarbeitungen und Datentransfers in Drittstaaten, Art. 58 Abs. 2 DS-GVO. 33

19 Art. 60 Abs. 4 DS-GVO.
20 Art. 65 Abs. 2 DS-GVO.
21 Bei diesen Vorschriften handelt es sich um die Umsetzung von Art. 46 DSRL-JI.

III. Datenschutzkontrollen und Zertifizierungen

34 Kontrollen sind eine effektive Möglichkeit, um die Einhaltung datenschutzrechtlicher Vorgaben und Empfehlungen zu überprüfen. Sie ermöglichen die Begutachtung wie der Datenschutz vor Ort gelebt und umgesetzt wird. Darüber hinaus geben die Aufsichtsbehörden bei Kontrollen Hinweise zu gesetzlichen Neuerungen und sprechen Best-Practice-Empfehlungen aus. Der Besuch der Aufsichtsbehörde gibt auch Raum für die Klärung von Fragen des Verantwortlichen. Fragen beantworten die Datenschutzaufsichtsbehörden auch außerhalb von Prüfungen, es ist der gesetzliche Auftrag an die Aufsichtsbehörden beratend tätig zu sein.

35 Denkbar ist, dass ein Verantwortlicher ein Verarbeitungsverfahren nach Art. 42 DS-GVO zertifizieren lässt. Die Zertifizierung dient dem Nachweis der Einhaltung datenschutzrechtlicher Vorschriften. Zertifizierungen haben einen präventiven Charakter[22]. Es handelt sich hierbei um eine freiwillige Überprüfung und erfolgt in einem transparenten Verfahren[23]. Die Datenschutzaufsichtsbehörden sind nicht durch die Zertifizierung gebunden, auch wenn sie diese fördern. Die Zertifizierung gilt für drei Jahre und kann verlängert sowie widerrufen werden[24]. Trotz Zertifizierung besteht die Verantwortung für den Verarbeitungsprozess weiterhin[25]. Die Zertifizierung ist nur durch eine akkreditierte Stelle möglich[26]. Für Verantwortliche außerhalb der EU eignet sich die Zertifizierung zum Nachweis eines angemessenen Datenschutzniveaus[27]. Die erteilten Zertifizierungsverfahren werden in ein Register beim Europäischen Datenschutzausschuss aufgenommen und in geeigneter Weise veröffentlicht[28].

22 Will, in: Ehmann/Selmayr, DS-GVO, Art. 42 Rn. 2.
23 Art. 42 Abs. 3 DS-GVO.
24 Art. 43 Abs. 7 DS-GVO.
25 Art. 42 Abs. 4 DS-GVO.
26 Vgl. Art. 43 DS-GVO.
27 Vgl. Art. 46 Abs. 1 lit. f DS-GVO.
28 Art. 42 Abs. 8 DS-GVO.