Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg
University of Applied Sciences

HOCHSCHULE FÜR ÖFFENTLICHE VERWALTUNG UND FINANZEN LUDWIGSBURG

Die neue EU-Datenschutzgrundverordnung (EU-DSGVO) - Bußgelder und Verwaltungsstrafen gegen Behörden.

Bachelorarbeit

zur Erlangung des Grades eines
Bachelor of Arts (B.A.)
im Studiengang gehobener Verwaltungsdienst – Public Management

vorgelegt von

Nikolai Wörner

Studienjahr 2016/2017

Erstgutachter: Herr Prof. Dr. Robert Müller-Török
Zweitgutachter: Herr Arne Pautsch

Inhaltsverzeichnis

Anlagenverzeichnis ..... **III**

A. Einführung **1**

B. Die EU-Datenschutzgrundverordnung (EU-DSGVO) **4**

I. Allgemeines 4

1. Die Entstehung 4

2. Aufbau der EU-DSGVO 7

3. Ziele der Datenschutzreform 8

II. Aufsichtsbehörden 10

1. Organisation 10

2. Aufgaben und Befugnisse 11

3. Zuständigkeit 12

III. Anwendungsbereich der Datenschutzgrundverordnung 13

1. Sachlicher Anwendungsbereich 13

2. Räumlicher Anwendungsbereich 15

3. Anwendungsbereich der Richtlinie (EU) 2016/680 15

C. Sanktionsmöglichkeiten gegen Behörden **17**

I. Grundgedanke über die Sanktionierung von Behörden 17

II. Abhilfebefugnisse der Aufsichtsbehörde 19

1. Verwarnungen 20

2. Anweisungen 22

3. Sanktionen 24

III. Bußgeldvorschriften 25

1. Charakter der Bußgelder 25

2. Aufbau des Art. 83 EU-DSGVO 27

3. Verstöße gegen die Verordnung 28

a) Verstöße erster Kategorie 28
b) Verstöße zweiter Kategorie 29
c) Verstöße dritter Kategorie 30
4. Bedingungen zur Verhängung von Bußgelder 31
5. Anwendbarkeit auf den öffentlichen Bereich 34
a) Grundlegende Anwendbarkeit 34
b) Öffnungsklausel 38
c) Art. 83 Abs. 7 „Lex specialis“ zu Art. 58 Abs. 2 EU-DSGVO? 41
IV. Weitere Sanktionsmöglichkeiten 41
D. Umsetzung der EU-DSGVO in Deutschland 43
I. Gesetzgebungskompetenz 43
II. Organisation der Aufsichtsbehörden 44
1. Zentrale Aufsichtsbehörde 44
2. Mehrere Aufsichtsbehörden 46
E. Fazit 48
Literaturverzeichnis 49
Eidesstattliche Erklärung 52

Anlagenverzeichnis

Anlage 1: Amtsblatt L 119 der Europäischen Union vom 04.05.2016 (deutsche Fassung)

Anlage 2: Amtsblatt L 119 der Europäischen Union vom 04.05.2016 (englische Fassung)

Anlage 3: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen Gesamtkonzept für den Datenschutz in der Europäischen Union vom 04.11.2010

Anlage 4: Schlussfolgerungen des Rates zur Mitteilung der Kommission an das Europäische Parlament und den Rat "Gesamtkonzept für den Datenschutz in der Europäischen Union" vom 21.01.2011

Anlage 5: Vorschlag für Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) (Kommissionsentwurf) vom 25.01.2012

Anlage 6: Datenschutzpaket – Bericht über die unter zyprischem Vorsitz erzielten Fortschritte -Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 26.11.2012

Anlage 7: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)- Ergebnis der ersten Lesung des Europäischen Parlaments vom 12.03.2014

Anlage 8: Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DatenschutzGrund-

verordnung)– Vorbereitung einer allgemeinen Ausrichtung vom 11.06.2015

Anlage 9: Trilog - Synopse der DS-GVO vom 15.12.2015

Anlage 10: BfDI - Info 6

Anlage 11: Die Datenschutzreform der Europäischen Union

Anlage 12: Deutsche Bundesbank - Themen - Bundesbank: Ein wichtiger Partner vor Ort, https://www.bundesbank.de/Redaktion/DE/Themen/2015/2015_08_27_bundesbank_vor_ort.html?view=render%5BDruckversion%5D

A. Einführung

"Die Gesetzgebung ist an die verfassungsmäßige Ordnung, die vollziehende Gewalt und die Rechtsprechung sind an Gesetz und Recht gebunden." (Art. 20 Abs. 3 GG).

Die öffentliche Verwaltung hat sich an alle Gesetze zu halten, durch die sie innerhalb Deutschlands und der Europäischen Union tangiert ist. Der Vorbehalt und Vorrang des Gesetzes sind Verfassungsgrundsätze, welche für jeden Leiter und Mitarbeiter in der Verwaltung selbstverständlich sein sollten. Doch diese "Selbstverständlichkeit" ist leider nicht überall in der öffentlichen Verwaltung zu finden. Ein großes Problemfeld betrifft in diesem Zusammenhang den Datenschutz.

Das Thema Datenschutz wird in allen Bereichen der unternehmerischen und staatlichen Tätigkeiten durch die fortschreitende Digitalisierung der Arbeit und Verwaltung immer wichtiger. Im Zeitalter des "Cloud-Computing" und der "Industrie 4.0" wird der Datenschutz immer mehr an Bedeutung gewinnen. Am 27.04.2016 wurde eine neue Europäische Datenschutzgrundverordnung[1] erlassen, die den gesamten Datenschutz in der EU vereinheitlichen soll. In dieser Verordnung wurden die Sanktions- und Bußgeldvorschriften der Aufsichtsbehörden revolutioniert und verschärft.[2]

Es häufen sich Beiträge in den Tätigkeitsberichten der Landesdatenschutzbeauftragten der einzelnen Bundesländer über Datenschutzverstöße in Behörden. In einem Fall wurden Schriftstücke mit personenbezogenen Daten von Jobcenterkunden in Müllbeuteln entsorgt und unverschlossen in einer öffentlich zugänglichen Tiefgarage gelagert.[3] Desweiteren gibt es viele Verstöße gegen die Melde- und Unterstützungspflichten von Be-

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (Siehe Anlage 1).
[2] Vgl. *Spindler*, in: DER BETRIEB 16/2016, 937 (946).
[3] Vgl. *Voßhoff,* 25. Tätigkeitsbericht zum Datenschutz für die Jahre 2013 und 2014, 2015, 166.

hörden gegenüber den Aufsichtsbehörden.[4] Bei der Vielzahl an Verstößen im öffentlichen und nicht-öffentlichen Bereich, ist es daher wichtig, die Verantwortlichen zu sanktionieren und das Datenschutzbewusstsein in den Fachbereichen zu stärken. Doch es zeigt sich eher ein anderer Trend. Die Durchführung von Ordnungswidrigkeits-, und Strafverfahren der Vorschriften des Bundesdatenschutzgesetzes (BDSG) gegen Unternehmen verliefen in den letzten Jahren mehr als schleppend.[5] Manche zuständige Aufsichtsbehörden sind sogar der Meinung, dass es wichtiger ist, die Unternehmen mehr zu beraten und zu sensibilisieren, als dass sie für die Vergehen bestraft werden sollten.[6] Der Datenschutz wird in Deutschland mittlerweile schon als "Schreckgespenst" wahrgenommen, den man nicht mehr ernst zu nehmen braucht.[7] Die Möglichkeit durch einen Datenschutzverstoß verurteilt zu werden ist in Deutschland "äußerst gering".[8] Im Zehnjahresverlauf gab es im Schnitt eine Verurteilung bei 52 Verdächtigten.[9] Ein Grund hierfür ist der ständige Personalmangel in den Aufsichtsbehörden, der sogar schon von der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit Andrea Voßhoff beklagt wird.[10] In den letzten Jahren ist die Anzahl an Mitarbeitern sogar geschrumpft.[11]

Über die Sanktionierung von Behörden und öffentlichen Stellen wird kaum nachgedacht, obwohl es in den meisten Datenschutzgesetzen der Länder Ordnungswidrigkeitsvorschriften gibt. Doch in den meisten Fällen werden "nur" Beanstandungen durchgeführt, ohne dass dies weitere Konsequenzen für die Verantwortlichen hat.

In dieser Abschlussarbeit werden die verschiedenen Möglichkeiten der Sanktionierung von Behörden und öffentlichen Stellen durch die neue Europäische Datenschutzgrundverordnung (EU-DSGVO) erörtert. Zunächst soll sie einen kurzen Überblick über die EU-DSGVO verschaffen und die

[4] Ebenda, 170.
[5] Vgl. *Schulzki-Haddouti*, in: c't 10/2016, 162 (163).
[6] Ebenda, 162.
[7] Vgl. *Schulzki-Haddouti*, in: c't 12/2015, 66.
[8] Vgl. *Schulzki-Haddouti*, in: c't 10/2016, 162 (163).
[9] Ebenda.
[10] Vgl. *Schulzki-Haddouti*, in: c't 12/2015, 66.
[11] Ebenda.

wichtigsten themenbezogenen Regelungen erläutern. Hierzu zählen die Ziele, der Anwendungsbereich, die Rechte der betroffenen Personen sowie die Pflichten der Verantwortlichen und die Vorschriften über die Aufsichtsbehörden. Im dritten Teil wird direkt auf die Sanktionsmöglichkeiten und deren Anwendung gegenüber der öffentlichen Verwaltung eingegangen. Dies bildet den Hauptteil der Arbeit. Der letzte Teil nimmt Bezug darauf, wie die Bundesrepublik Deutschland die Regelungen der neuen Aufsichtsbehörden umsetzen könnte, damit eine effektive Durchsetzung und Kontrolle des europäischen Datenschutzrechts gewährleistet werden kann.

B. Die EU-Datenschutzgrundverordnung (EU-DSGVO)

In diesem Teil der Arbeit sollen die allgemeinen wichtigen Bestimmungen zur EU-DSGVO erläutert werden, die für das weitere Verständnis benötigt werden.

I. Allgemeines

Im folgenden Kapitel werden das Gesetzgebungsverfahren und die Ziele der Datenschutzreform beschrieben.

1. Die Entstehung

Die Europäische Kommission brachte mit Schreiben von 04.11.2010 die europäische Datenschutzreform "ins Rollen".[12] In der Mitteilung stellte sie ein gesamtes Paket mit Vorschlägen und Anregungen, für ein einheitliches Datenschutzrecht in der EU, vor. Als Hauptargument für eine Novellierung der Datenschutzvorschriften, nannte die Kommission den rasanten technologischen Fortschritt in den letzten Jahrzehnten,[13] wodurch die Richtlinie 95/46/EG (Datenschutzrichtlinie) in vielen Teilen nicht mehr zeitgemäß war. Dennoch sollen die wichtigsten Ziele der Datenschutzrichtlinie, wie der Schutz der Grundrechte und Grundfreiheiten der Bürgerinnen und Bürger vor rechtswidriger Verarbeitung ihrer personenbezogenen Daten und die Harmonisierung des Datenschutzes zur Vollendung des Binnenmarktes im Rahmen des freien Datenverkehrs, weiterhin gelten.[14] Dieser Grundgedanke wurde direkt in die Erwägungsgründe zur EU-DSGVO aufgenommen.[15] Weitere Punkte der Kommission waren u.a. die Schaffung eines hohen europaweiten Schutzniveaus für die personenbezogenen Da-

[12] Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, 2010. (Siehe Anlage 3).
[13] Ebenda, 2.
[14] Ebenda.
[15] Vgl. Erwägungsgrund Nr. 9 zur EU-DSGVO.

ten, sowie eine wirksamere Durchsetzung des Datenschutzrechts innerhalb und außerhalb der EU.[16]

Eine Reaktion des Europäischen Rates lies nicht lang auf sich warten. Mit Schreiben vom 21.01.2011 wurde den Beteiligten die Schlussfolgerungen der Gruppe "Informationsaustausch und Datenschutz" (DAPIX) des Rates vorgelegt.[17] Aus den Schlussfolgerungen ist zu entnehmen, dass der Rat der Europäischen Union das grundlegende Vorhaben der Kommission und die Ziele der Datenschutzreform unterstützt.[18] Ebenso ist der Rat der Auffassung, dass für eine effektive Durchsetzung der Vorschriften und des Erhalts eines hohen Datenschutzniveaus die zukünftigen Datenschutzaufsichtsbehörden von zentraler Bedeutung sind.[19]

Der Kommissionsentwurf zur EU-DSGVO erschien am 25.01.2012. In diesem Vorschlag wurde bereits die Möglichkeit eingeräumt, dass gegenüber Behörden und öffentlichen Stellen Bußgelder verhängt werden können. In den Erwägungsgründen des Kommissionsentwurfs wurde festgehalten, dass gegen jede öffentliche oder private Person Sanktionen erlassen werden sollte, sofern ein Datenschutzverstoß vorliegt.[20] Die Formulierung im Erwägungsgrund Nr. 119 "Gegen jede - privatem oder öffentlichem Recht unterliegende - Person [...]" kann man so verstehen, dass hierunter nicht nur natürliche Personen fallen, sondern auch juristische Personen des privaten und öffentlichen Rechts.[21] Die Höhe des höchstmöglichen Bußgelds war damals noch im Vergleich zur Endfassung mit den Stufen 250.000 Euro, 500.000 Euro und 1 Mio. Euro (Art. 79 Kommissionsentwurf) erheblich geringer, obwohl diese Geldbußen bereits das Niveau des BDSG mit 300.000 Euro überschritten hatte.

[16] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, 2010, 4. (Siehe Anlage 3).
[17] Schlussfolgerungen des Rates zur Mitteilung der Kommission an das Europäische Parlament und den Rat "Gesamtkonzept für den Datenschutz in der Europäischen Union", 2011. (Siehe Anlage 4).
[18] Ebenda, 7.
[19] Ebenda, 6.
[20] Vgl. Erwägungsgrund Nr. 119 zum Kommissionsentwurf zur EU-DSGVO. (Siehe Anlage 5).
[21] Vgl. Erwägungsgrund Nr. 89 zur Richtlinie 2016/680/EG. (Siehe Anlage 1).

Am 12.03.2014 hat der LIBE-Ausschuss (Ausschuss für bürgerliche Freiheiten, Justiz und Inneres) des Europaparlaments, nach zweijährigen Verhandlungen, mit über 4000 Änderungsanträgen, einen Parlamentsentwurf zum Vorschlag einer Europäischen Datenschutzgrundverordnung beschlossen.[22] In diesem Parlamentsentwurf wurden die Sanktionierungsmaßnahmen gegen die Verantwortlichen erheblich verschärft. Der LIBE-Ausschuss sieht, gem. Art. 79 Abs. 2a lit. c des Parlamentsentwurfs, für eine Bußgeldverhängung einen Höchstbetrag in Höhe von 100 Mio. Euro oder im Falle eines Unternehmens 5 % seines weltweiten erzielten Jahresumsatzes vor. Das Parlament schlug ein 100 mal höheres Bußgeld, ohne eine Herabstufung nach Art des Verstoßes, vor, als die Kommission. Für die Aushandlung dieses Entwurfes bekam der Berichterstatter Jan Phillip Albrecht viel Bewunderung und Lob zugesprochen[23] , da viele ein Scheitern der Datenschutzreform während der Verhandlungen vermuteten.[24]

Der Rat der Europäischen Union hatte zum 11.06.2015 schlussendlich seinen Vorschlag für das bevorstehende Trilog-Verfahren[25] unterbreitet.[26] Der Ministerrat hat sich in Bezug auf die Sanktionierung des öffentlichen Sektors geeinigt, dass es eine Öffnungsklausel im Art. 79 Abs. 3a für die Mitgliedstaaten geben soll. Diese Öffnungsklausel wurde im weiteren Trilog-Verfahren zwischen dem Europaparlament, der Kommission und dem Rat letztendlich in den endgültigen Entwurf in den Art. 79 Abs. 7 EU-DSGVO verankert.

Am 27.04.2016 wurde die Datenschutzgrundverordnung im Europaparlament verabschiedet und am 04.05.2016 im Amtsblatt der Europäischen

[22] Vgl. Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) - Ergebnis der ersten Lesung des Europäischen Parlaments, 2014, 2. (Siehe Anlage 7).
[23] Vgl. *Schaar*, in: ZD 3/2014, 113.
[24] Vgl. *Forgó*, in: ZD 2/2014, 57.
[25] Trilog - Synopse der DS-GVO, 2015. (Siehe Anlage 9).
[26] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DatenschutzGrundverordnung) – Vorbereitung einer allgemeinen Ausrichtung, 2015. (Siehe Anlage 8).

Union Nr. L119 veröffentlicht. Das Datenschutzpaket enthielt neben der Datenschutzgrundverordnung noch die Richtlinie 2016/680[27] und die Richtlinie 2016/680[28].

2. Aufbau der EU-DSGVO

Die Datenschutzgrundverordnung setzt sich aus 100 Artikeln in 11 Kapiteln zusammen. Kapitel I regelt die "Allgemeine Bestimmungen". Dort werden die Ziele und Zwecke (Art. 1 EU-DSGVO), der sachliche und räumliche Anwendungsbereich (Art. 2 und 3 EU-DSGVO) sowie die wichtigsten Begriffsbestimmungen der Verordnung geregelt. Einige Definitionen, wie die des Verantwortlichen und Auftragsverarbeiters, wurden zum Teil komplett von der Datenschutzrichtlinie 95/46/EG übernommen. In Kapitel II werden die Grundsätze und Bedingungen für die Verarbeitung personenbezogener Daten erläutert. Darauf folgend werden in Kapitel III die Rechte der betroffenen Personen und in Kapitel IV die Pflichten der Verantwortlichen und Auftragsverarbeiter aufgeführt. Die Möglichkeiten der Datenübermittlung an Drittländer und internationale Organisationen werden in Kapitel V erläutert. Die Regelungen zu den zukünftigen Datenschutzaufsichtsbehörden, ihrer Aufgaben, Organisation und über die Zusammenarbeit mit den anderen Aufsichtsbehörden, dem Europäischen Datenschutzausschuss und der Europäischen Kommission sind in den Kapiteln VI und VII enthalten. Im Kapitel VIII sind die Bestimmungen zu den Rechtsbehelfen, Sanktionen und Bußgeldvorschriften geregelt. In den restlichen Kapiteln sind Vorschriften für besondere Verarbeitungssituationen, wie der Beschäftigtendatenschutz und über Meinungs- und Informationsfreiheit (Kapitel IX), Regelungen zu delegierten Rechtsakten und

[27] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates.

[28] Richtlinie (EU) 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität.

Durchführungsrechtsakten der Europäischen Kommission (Kapitel X) und die Schlussvorschriften (Kapitel XI) enthalten.

3. Ziele der Datenschutzreform

Laut der Gesetzesbegründung zur EU-DSGVO sind die Hauptziele der Verordnung:

- Die Stärkung der Datenschutzrechte natürlicher Personen,
- der freie Verkehr personenbezogener Daten im Binnenmarkt,
- die Verringerung des Verwaltungsaufwands.[29]

Die Stärkung der Rechte der Betroffenen wird in der Verordnung durch mehrere Regelungen geprägt. Zum einen erhalten die betroffenen Personen durch die umfangreichen Transparenzpflichten eine bessere Position gegenüber den Verantwortlichen.[30] Zum anderen wird durch die Zuständigkeitsregelungen der Aufsichtsbehörden sichergestellt, dass betroffene Personen sich bei Beschwerden oder Verstößen an ihre örtliche Aufsichtsbehörde wenden können (Art. 77 Abs. 1 EU-DSGVO).[31] Die Aufsichtsbehörden sind dann verpflichtet, die Beschwerde an die zuständige Aufsichtsbehörde weiterzuleiten. Desweiteren sind die Verantwortlichen verpflichtet, die erforderlichen Informationen zu den Betroffenenrechten durch eine "einfache Sprache" den Personen bereitzustellen und die Ausübung dieser Rechte bestmöglich zu erleichtern.[32]

Durch die kommende europaweite Harmonisierung des Datenschutzes, werden ebenso die Rechte aller EU-Bürgerinnen und Bürger gestärkt, da in den einzelnen Mitgliedstaaten verschiedene Datenschutzniveaus herrschen.[33] Dadurch ist es auch möglich, das Datenschutzrecht europaweit konsequenter durchzusetzen. Durch die verstärkten Befugnisse der Auf-

[29] Vgl. EU-Datenschutz-Grundverordnung, Gesetzestext mit eingereihten Erwägungsgründen, 2016, 141.
[30] Vgl. *Wybitul*, in: ZD 5/2016, 203 (204).
[31] Vgl. *Albrecht,* Die Datenschutzreform der Europäischen Union, 2015, 25. (Siehe Anlage 11).
[32] Vgl. EU-Datenschutz-Grundverordnung, Gesetzestext mit eingereihten Erwägungsgründen, 2016, 149.
[33] Vgl. Erwägungsgrund Nr. 9 zur EU-DSGVO.

sichtsbehörden, die hohen Bußgelder und die zukünftige sehr enge Zusammenarbeit zwischen den Aufsichtsbehörden, haben diese die Möglichkeit, gegenüber den Verantwortlichen mehr Druck auszuüben, damit diese die Vorschriften einhalten.[34] Die EU legte bei der Gesetzgebung daher einen großen Wert darauf, dass die für die Datenverarbeitung Verantwortlichen sich bewusst werden, dass Verstöße gegen den Datenschutz nicht harmloser Natur sind.[35]

In Artikel 1 Abs. 3 EU-DSGVO ist aufgeführt, dass der freie Verkehr personenbezogener Daten in der Union weder eingeschränkt noch verboten werden darf. In dieser Formulierung wird ein weiteres Hauptziel deutlich, die Harmonisierung und Stärkung des Binnenmarkts. Der freie Verkehr personenbezogener Daten ist für den Europäischen Binnenmarkt von wichtiger Bedeutung, da im Zeitalter des Internets Waren und Dienstleistungen von zu Hause aus erworben werden können. Durch die Datenschutzgrundverordnung sollten in Zukunft gleiche (oder ähnliche) Datenschutzstandards in der Europäischen Union herrschen, wodurch die Unternehmen mehr Rechtssicherheit bei ihrer Datenverarbeitung erhalten.[36]

Ein weiterer wichtiger Punkt war für die Europäische Kommission und die Unternehmen die Verringerung des Verwaltungsaufwands. Die vollständige Harmonisierung des Datenschutzrechts, durch eine Verordnung mit verbindlichem Charakter, soll dafür Sorge tragen, dass internationale Unternehmen mit Niederlassungen in mehreren Mitgliedstaaten, es einfacher haben, die Datenschutzvorschriften umzusetzen. So können sich die Unternehmen auf nur eine Datenschutzregelung konzentrieren und diese effizient umsetzen, anstatt dass mehrere unterschiedliche Datenschutzge-

[34] Vgl. *Klingbeil,* 32. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Baden-Württemberg 2014/2015, 2016, 18.
[35] Vgl. *Albrecht,* Die Datenschutzreform der Europäischen Union, 2015, 25. (Siehe Anlage 11).
[36] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, 2010, 11. (Siehe Anlage 3).

setze beachtet werden müssen.[37] Dadurch kann es auch zu Kosteneinsparungen in den Unternehmen kommen.[38]

II. Aufsichtsbehörden

In der Datenschutzgrundverordnung sind die Regelungen zu den zukünftigen Aufsichtsbehörden in den Artikeln 51 bis 59 geregelt. Ihre Arbeitsweise und Organisation entscheiden in Zukunft, wie effektiv die Datenschutzgrundverordnung in der EU umgesetzt wird.[39]

1. Organisation

Der EU-Gesetzgeber hat die Gestaltung der Aufsichtsbehörden durch Art. 54 EU-DSGVO komplett den Mitgliedstaaten überlassen. Die EU schreibt den Mitgliedstaaten nur einige organisatorische Regelungen vor. Eines der wichtigsten Merkmale ist die Unabhängigkeit der Aufsichtsbehörden. Die Aufsichtsbehörden müssen frei von jeder Art der Beeinflussung ihren Aufgaben nachkommen, um den bestmöglichen Schutz der personenbezogenen Daten zu sichern.[40] Die Mitarbeiter der Aufsichtsbehörden dürfen keinerlei mit ihrem Amt unvereinbare Tätigkeiten wahrnehmen und sich weder von innen noch von außen beeinflussen lassen, um sicherzustellen, dass es zu keinem Interessenkonflikt kommt.[41]

Als erfreulich ist anzusehen, dass die EU den Mitgliedstaaten in Art. 52 Abs. 4 EU-DSGVO nun vorschreibt, dass die Aufsichtsbehörden mit genügend "personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastruktur" ausgestattet werden müssen.[42] Somit könnten sich die aktuellen Landesdatenschutzbeauftragten und die Bundesdatenschutzbeauftragte über neues Personal freuen, sofern die Regierungen bereit sind, die notwendigen Mittel bereit zu stellen. Die Mitgliedstaaten

[37] Ebenda.
[38] Ebenda, 12.
[39] Vgl. Schlussfolgerungen des Rates zur Mitteilung der Kommission an das Europäische Parlament und den Rat "Gesamtkonzept für den Datenschutz in der Europäischen Union", 2011, 6. (Siehe Anlage 4).
[40] Vgl. Erwägungsgrund Nr. 117 zur EU-DSGVO; Art. 51 Abs. 1 EU-DSGVO; Art. 52 Abs. 1 EU-DSGVO.
[41] Art. 52 Abs.2 und 3 EU-DSGVO.
[42] Vgl. Erwägungsgrund Nr. 120 S. 1 zur EU-DSGVO.

müssen ebenso durch nationales Recht bestimmen, welche Qualifikationen die Mitarbeiter der Aufsichtsbehörden benötigen und wie das Einstellungsverfahren abzulaufen hat.[43]

Als weitere Behörde müssen die Mitgliedstaaten Finanzkontrollen für die Aufsichtsbehörden einführen,[44] da die Aufsichtsbehörden über ihren eigenen Finanzetat selbstständig bestimmen können.[45]

2. Aufgaben und Befugnisse

Die Aufgaben und Befugnisse der Aufsichtsbehörden sind in den Artikeln 57 und 58 EU-DSGVO aufgeführt. Zur Hauptaufgabe gehören die Überwachung und Durchsetzung der EU-DSGVO und die Sicherstellung des Schutzes der personenbezogenen Daten und der Grundrechte und Grundfreiheiten. [46] Desweiteren leisten die Aufsichtsbehörden gem. Art. 51 Abs. 2 EU-DSGVO einen Beitrag für eine einheitliche Anwendung der Datenschutzgrundverordnung. Der Aufgabenkatalog in Art. 57 EU-DSGVO enthält insbesonders folgende Aufgaben:

- Überwachung und Durchsetzung der EU-DSGVO,
- Öffentlichkeitsarbeit,
- Beratung von Regierungen und Parlamenten über Datenschutzmaßnahmen,
- Sensibilisierung der Verantwortlichen,
- Bürgerberatung,
- Bearbeitung von Beschwerden,

und vieles mehr. Nach Art. 59 EU-DSGVO müssen die Aufsichtsbehörden außerdem jedes Jahr den nationalen Parlamenten einen Tätigkeitsbericht,

[43] Vgl. Erwägungsgrund Nr. 121 zur EU-DSGVO.
[44] Vgl. Art. 52 Abs. 6 EU-DSGVO; Erwägungsgrund Nr. 118 zur EU-DSGVO.
[45] Vgl. Erwägungsgrund Nr. 120 S. 2 zur EU-DSGVO.
[46] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, 2010, 19–20. (Siehe Anlage 3); Art. 51 Abs. 1 EU-DSGVO; Art. 57 Abs. 1 lit. a EU-DSGVO.

über die Datenschutzverstöße , durchgeführten Maßnahmen und weitere datenschutzrelevante Themen, vorlegen.

Den Aufsichtsbehörden stehen für die Kontrollaufgaben umfangreiche Befugnisse zur Verfügung. In Art. 58 Abs. 1 EU-DSGVO sind die Untersuchungsbefugnisse aufgeführt, mit denen die Aufsichtsbehörden ihre Ermittlungsersuchen bei den Verantwortlichen rechtsverbindlich durchsetzen können. Art. 58 Abs. 2 EU-DSGVO enthält die Abhilfebefugnisse, auf die ausführlich im Teil C. II. eingegangen werden. Die Genehmigung- und Beratungsbefugnisse sind in Art. 58 Abs. 3 geregelt. Die Mitgliedstaaten haben durch Art. 58 Abs. 6 das Recht, den nationalen Aufsichtsbehörden weitere Befugnisse zu erteilen.

3. Zuständigkeit

Die Zuständigkeitsregelungen werden durch die EU-DSGVO ebenso neu geregelt. Durch das neue System der zentralen Anlaufstelle, oder auch "One-Stop-Shop" genannt, ist nur die Aufsichtsbehörde, in dem Mitgliedstaat zuständig, in dem der Verantwortliche seine Hauptniederlassung hat.[47] Diese Regelung kommt vor allem den Unternehmen mit mehreren Niederlassungen in der EU entgegen, da sie selbst die Hauptniederlassung bestimmen können.[48] Bei länderübergreifenden Datenverarbeitungen können gem. Art. 56 EU-DSGVO mehrere Aufsichtsbehörden zuständig sein. Die Aufsichtsbehörde, die für die Hauptniederlassung zuständig ist, ist demnach die federführende Aufsichtsbehörde. In diesem Fall arbeiten die betroffenen Aufsichtsbehörden gem. Art. 60 ff. EU-DSGVO zusammen. Für die Zusammenarbeit zwischen den Aufsichtsbehörden und um eine einheitliche Vorgehensweise sicherzustellen, kann das Kohärenzverfahren zur Anwendung kommen.[49] Gem. Art. 55 Abs. 2 EU-DSGVO sind die Aufsichtsbehörden für Behörden und öffentliche Stellen allein zustän-

[47] Vgl. EU-Datenschutz-Grundverordnung, Gesetzestext mit eingereihten Erwägungsgründen, 2016, 143; Art. 56 Abs. 1 EU-DSGVO.
[48] Vgl. *Caspar*, in: ZD 12/2012, 555 (556).
[49] Vgl. Erwägungsgrund Nr. 135 zur EU-DSGVO; Art. 63 EU-DSGVO.

dig und die Vorschriften über die federführende Aufsichtsbehörde und das Kohärenzverfahren kommen nicht zur Anwendung.[50]

III. Anwendungsbereich der Datenschutzgrundverordnung

Die Regelungen zum sachlichen und räumlichen Anwendungsbereich sind in den Artikeln 2 und 3 der EU-DSGVO geregelt. Da Teile der öffentlichen Verwaltung von der Richtlinie 2016/680/EG betroffen sind, muss auch auf den Anwendungsbereich der Richtlinie für die Strafverfolgung eingegangen werden.

1. Sachlicher Anwendungsbereich

Nach Art. 2 Abs. 1 EU-DSGVO, gilt diese Verordnung für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten, sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Vom Anwendungsbereich der Verordnung ausgeschlossen sind datenverarbeitende Tätigkeiten personenbezogener Daten gem. Absatz 2, wenn

- sie sich außerhalb des Anwendungsbereichs des Unionsrechts befinden (lit. a),
- die gemeinsamen Außen- und Sicherheitspolitik (Titel V Kap. 2 EUV) betroffen ist (lit. b),
- es sich um persönliche oder familiäre Angelegenheiten natürlicher Personen handelt (lit. c),
- der Anwendungsbereich der Richtlinie 2016/680/EG tangiert wird (lit. d).

Da die Vorschrift des Art. 2 nicht definiert, welche Bereiche der Datenverarbeitung betroffen sind, kann indiziert werden, dass sowohl der privatrechtliche wie auch der öffentlich-rechtliche Tätigkeitsbereich miteinbegriffen sind. Relevant für den öffentlich Bereich, für die Klärung, ob die Da-

[50] Vgl. Erwägungsgrund Nr. 128 zur EU-DSGVO; Art. 55 Abs. 2 EU-DSGVO; EU-Datenschutz-Grundverordnung, Gesetzestext mit eingereihten Erwägungsgründen, 2016, 162-163.

tenschutzgrundverordnung zur Anwendung kommt, ist Art. 2 Abs. 2 lit. d EU-DSGVO. In ihm heißt es, dass Behörden für die Zwecke der Strafverfolgung und Strafvollstreckung, sowie für die Gefahrenabwehr, nicht in diesen Anwendungsbereich fallen. Hierfür wurde mit dem Datenschutzpaket die Richtlinie 2016/680/EG verabschiedet, die den Datenschutz des Bereichs der Strafverfolgung abdeckt. Es ist immer auf den Zweck der Datenverarbeitung abzustellen, und nicht auf die Tatsache, ob es sich um eine Polizeibehörde handelt. Dies wurde mit dem Ausdruck "durch die zuständige Behörden zum Zwecke[...]" klar gestellt.

Für den öffentlichen Bereich gibt es jedoch wiederum eine Sonderregelung, die den Anwendungsbereich der EU-DSGVO aushebeln könnte. In Art. 6 Abs. 2 EU-DSGVO wird den Mitgliedstaaten das Recht eingeräumt, für den öffentlichen Bereich spezifischere nationale Regelungen zu erlassen. Diese Öffnungsklausel gilt für die Verarbeitung personenbezogener Daten für die Wahrnehmung von Aufgaben des öffentlichen Interesses oder die in Ausübung öffentlicher Gewalt erfolgt (Art. 6 Abs. 1 lit. e EU-DSGVO), sowie zur Erfüllung von rechtlichen Verpflichtungen (Art. 6 Abs. 1 lit. c EU-DSGVO). Durch diese Bestimmungen könnten viele Aufgabenbereiche der öffentlichen Verwaltung, die in nationalen Regelungen vorgeschrieben sind, in vielen Teilen nationalgesetzlich geregelt werden. Jedoch bleibt der Anwendungsbereich der EU-DSGVO für diese Aufgaben trotzdem berührt. In der Öffnungsklausel wird ausdrücklich erwähnt, dass nationalgesetzliche Regelungen für die Spezifizierung und besondere Anpassung dieser Verordnung für die Zwecke des Art. 6 Abs. 1 lit. c und e EU-DSGVO erfolgen kann.[51] Durch die Bedingungen der Vorschriften des Art. 6 Abs. 2 und 3 EU-DSGVO werden die spezifischeren nationalen Regelungen in Abhängigkeit mit der Datenschutzgrundverordnung gebracht, sodass sie trotzdem noch für diese datenverarbeitenden Zwecke in den Grundzügen verbindlich ist.

[51] Vgl. *Benecke/Wagner*, in: DVBl 10/2016, 600 (601).

2. Räumlicher Anwendungsbereich

Für den räumlichen Anwendungsbereich der Datenschutzgrundverordnung ist relevant, ob sich der Verantwortliche in der EU befindet und ob personenbezogene Daten von Bürgerinnen und Bürger der EU verarbeitet werden. Der Ort der tatsächlichen Datenverarbeitung ist demnach nicht von Bedeutung.

Nach Art. 3 Abs. 1 EU-DSGVO gilt die Verordnung für alle Verantwortlichen und Auftragsverarbeiter, die eine Niederlassung in der EU besitzen und dort personenbezogene Daten verarbeiten; auch "Marktortprinzip"[52] genannt. Desweiteren gilt die Verordnung gem. Abs. 2 für Verantwortliche, die personenbezogene Daten von EU-Bürgerinnen und Bürgern verarbeiten und keine Niederlassungen in der EU besitzen. Durch diese neue Regelung können die personenbezogenen Daten auch vor Verantwortlichen von Drittstaaten geschützt werden. Die gesamten Regelungen der Datenschutzgrundverordnung können sich demnach theoretisch weltweit erstrecken. Da Behörden der Mitgliedstaaten als Verantwortliche in der Regel nur in Ihrem Hoheitsgebiet tätig werden, sind sie unmittelbar in den räumlichen Anwendungsbereich nach Absatz 1 mit inbegriffen.

3. Anwendungsbereich der Richtlinie (EU) 2016/680

Die Richtlinie zur Strafverfolgung hat gem. Art. 1 Abs. 2 die Ziele, die justizielle Zusammenarbeit zwischen den Strafverfolgungsbehörden sicherzustellen und den Schutz der personenbezogenen Daten der betroffenen Personen zu schützen. Der Zweck der Datenverarbeitung ergibt sich unmittelbar aus Art. 1 Abs. 1. Die Richtlinie soll die Verarbeitung personenbezogener Daten zum Zwecke der Strafverfolgung und der Gefahrenabwehr regeln. Dieser Zweck ist identisch mit der Regelung des Art. 2 Abs. 2 lit. d EU-DSGVO. Der Anwendungsbereich nach Art. 2 Abs. 1 der Richtlinie zur Strafverfolgung, bezieht sich direkt auf diesen Zweck aus Art. 1. Demnach ist für die Anwendbarkeit der Richtlinie nicht die Tatsache entscheidend, ob es sich um eine Polizeibehörde handelt, sondern ob die

[52] Vgl. *Caspar*, in: ZD 12/2012, 555 (556).

Behörde die Datenverarbeitung nach den Zwecken des Art. 1 durchführt. Sollte eine Polizeibehörde personenbezogene Daten verarbeiten, die nicht mit den Zwecken der Richtlinie übereinstimmen, so gilt für diesen Datenverarbeitungsvorgang die Datenschutzgrundverordnung.[53] Diese Schlussfolgerung wurde ebenso in die Erwägungsgründe (Nr. 19) der Datenschutzgrundverordnung mit aufgenommen. Demnach kann es vorkommen, dass Polizeibehörden die Regelungen der Richtlinie zur Strafverfolgung und die Datenschutzgrundverordnung gleichzeitig beachten müssen. Vor allem im Bereich der Sanktionierung gibt es entscheidende Unterschiede. Daher wird es in Zukunft wichtig sein, die Datenverarbeitungsvorgänge in den Polizei- und Strafverfolgungsbehörden genau zu definieren und die Zwecke, für die die personenbezogenen Daten verarbeitet werden, eindeutig aufzuführen. Da es sich hierbei um eine Richtlinie der EU handelt, muss diese erst in nationales Recht umgesetzt werden. Hier könnte der Gesetzgeber entsprechende Regelungen einführen, um diesen problematischen Bereich zu entschärfen.

[53] Vgl. EU-Datenschutz-Grundverordnung, Gesetzestext mit eingereihten Erwägungsgründen, 2016, 240.

C. Sanktionsmöglichkeiten gegen Behörden

In diesem Hauptteil der Arbeit werden zunächst die Abhilfebefugnisse der Aufsichtsbehörden beschrieben und danach speziell die Bußgeldvorschriften des Art. 83 EU-DSGVO. In den folgenden Ausführungen wird nicht immer direkt von den Behörden, sondern auch von den Verantwortlichen gesprochen, da die Datenschutzgrundverordnung für den öffentlichen und den privaten Bereich gilt.

I. Grundgedanke über die Sanktionierung von Behörden

Sanktionen sind ein wichtiges Mittel, um die Durchsetzung der EU-DSGVO sicherzustellen. Es ist zwar fraglich, ob sie auch die gewünschte Wirkung erzielen, dennoch sollen sie eingesetzt werden, um für die Verantwortlichen als Anreiz für die Einhaltung der EU-DSGVO zu dienen.[54] Der EU-Gesetzgeber sieht die Verschärfung der Sanktionen auch als wichtiges Instrument für die Gewährleistung eines gleichmäßigen hohen Datenschutzniveaus für die personenbezogenen Daten in der EU. Daher bedarf es gleichwertiger Sanktionen in allen Mitgliedstaaten.[55] Die Sanktionen haben somit den Zweck, die Grundrechte und Grundfreiheiten, insbesonders das Grundrecht auf Datenschutz (Art. 8 GRCh) und das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) zu gewährleisten.

Damit diese Grundrechte auch in allen Bereichen im Anwendungsbereich der EU-DSGVO geschützt werden können, müssen die Sanktionsbefugnisse, insbesondere die Geldbußen, auch für den öffentliche Bereich gelten. Der öffentliche Bereich verarbeitet seit Jahren zunehmend Daten in umfangreichen Mengen.[56] Daher ist es besonders wichtig, den Schutz personenbezogener Daten in Behörden besser zu überwachen und bei Verstößen rechtsverbindlich durchsetzen zu können.

[54] Ebenda, 143.
[55] Vgl. Erwägungsgrund Nr. 13 zur EU-DSGVO.
[56] Vgl. Erwägungsgrund Nr. 6 zur EU-DSGVO.

Die öffentliche Verwaltung ist durch den Verfassungsgrundsatz des Vorbehaltes des Gesetzes (Art. 20 Abs. 3 GG) desweiteren besonders verpflichtet, sich an die Gesetze und Vorschriften zu halten. Die Behörden sind dadurch an alle förmlichen Gesetze, Rechtsverordnungen und Satzungen gebunden.[57] Da es sich bei der Datenschutzgrundverordnung um eine Verordnung der Europäischen Union handelt, ist sie unmittelbar anzuwendendes Recht.[58]

Ein weiterer grundrechtlicher Aspekt, der für die Sanktionierung von Behörden spricht, ergibt sich aus dem Art. 1 Abs. 3 GG. Durch das Volkszählungsurteil des Bundesverfassungsgerichts von 1983[59], wurde das Grundrecht auf informationelle Selbstbestimmung geschaffen, dass sich aus dem Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG schließen lässt. Da die Grundrechte des Grundgesetzes für die vollziehende Gewalt gem. Art. 1 Abs. 3 GG bindend ist, sollten Behörden nicht ohne Konsequenzen gegen das Grundrecht auf informationelle Selbstbestimmung verstoßen können.

In manchen Bundesländern gibt es bereits Ordnungswidrigkeits- und Strafvorschriften in den jeweiligen Landesdatenschutzgesetze, die für die öffentliche Verwaltung gelten.[60] Diese kommen jedoch so gut wie nie zur Anwendung. Gründe hierfür sind vor allem der Personalmangel in den Aufsichtsbehörden und der politische Wille, diese durchzusetzen. In den meisten Fällen werden Beanstandungen erstellt und an die Behördenleitung weitergegeben.[61] Oftmals werden die Datenschutzkontrollen nur wegen Einzelfällen durchgeführt, bei denen eine konkrete Beschwerde vorliegt, anstatt dass eine umfangreiche Kontrolle durchgeführt wird.[62] Typische Datenschutzverstöße der Behörden sind zum Beispiel die Speicherdauer und die Menge von personenbezogenen Daten.[63] In vielen Fällen ist

[57] Vgl. *Jarass/Pieroth,* 2016, Art. 20 GG Rn. 53.
[58] Vgl. *Hetmeier,* in: Lenz/Borchardt/u.a., 2013, Art. 288 AEUV Rn. 8.
[59] BVerfG Urteil vom 15. Dezember 1983 Az. 1 BvR 209/83, 1 BvR 484/83, 1 BVR 440/83, 1 BvR 362/83, 1 BvR 269/83.
[60] Z.B. § 40 LDSG (BW); Art. 37 BayDSG; § 41 HDSG.
[61] Vgl. *Caspar,* 25. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2014 / 2015, 2015, 21.
[62] Vgl. *Schulzki-Haddouti*, in: c't 13/2016, 154 (155).
[63] Ebenda.

auch die Kommunikation zwischen den Behörden ein Problem, in denen personenbezogene Daten unverschlüsselt[64] oder ohne gesetzliche Grundlage weitergegeben werden. Die Behörden verstoßen vermutlich nicht vorsätzlich gegen die Datenschutzvorschriften, sondern eher fahrlässig, um sich die Arbeit zu erleichtern.[65] Es kommt jedoch auch vor, dass von den Behörden die Verstöße gegen den Datenschutz verharmlost werden.[66] Daher begrüßen einige Landesdatenschutzbeauftragte die neuen Kompetenzen und Befugnisse, die sie in Zukunft durch die Datenschutzgrundverordnung erhalten haben.[67] Fraglich ist nur , ob die zuständigen Regierungen in Deutschland die Verwirklichung der neuen Aufgaben und Befugnisse der zukünftigen Aufsichtsbehörden unterstützen und umsetzen werden. Die Aufsichtsbehörden haben zwar nun das Recht, mit den notwendigen Ressourcen ausgestattet zu werden, jedoch zeigte sich schon in der Vergangenheit, dass es kaum Interesse daran gibt, die Aufsichtsbehörden mit genügend Personal und finanziellen Mitteln auszustatten.[68]

Gründe die gegen eine Sanktionierung von Behörden sprechen, ist Tatsache, dass die Behörden keine Gewinnerzielungsabsicht hegen, wie die private Wirtschaft. Die Datenverarbeitung in den Behörden erfolgt durch Rechtsvorschriften im öffentlichen Interesse. So könnte argumentiert werden, dass die öffentliche Verwaltung eine Sonderstellung gegenüber der privaten Wirtschaft inne hat und daher nicht sanktioniert werden sollte. Jedoch ist es nach Abwägung aller Gründe zu empfehlen, die öffentliche Verwaltung gleich oder ähnlich, wie die anderen datenverarbeitenden Unternehmen zu behandeln.

II. Abhilfebefugnisse der Aufsichtsbehörde

Wie bereits vorher erwähnt, haben die Aufsichtsbehörden durch die Regelung des Art. 58 EU-DSGVO umfangreiche Befugnisse erhalten, die sie für die Rechtsdurchsetzung anwenden können. Eine signifikante Rolle spielen

[64] Ebenda, 154.
[65] Ebenda, 155.
[66] Ebenda.
[67] Vgl. *Smoltczyk,* Datenschutz und Informationsfreiheit Bericht 2015 Berlin, 2016, 30.
[68] Vgl. *Schulzki-Haddouti*, in: c't 13/2016, 154 (157).

dabei die Abhilfebefugnisse nach Art. 58 Abs. 2 EU-DSGVO. Die Abhilfebefugnisse lassen sich in drei Stufen einordnen. Die Verwarnungen (lit. a und b), die Anweisungs- und Anordnungsbefugnisse (lit. c, d, e, g und h) und die Sanktionsbefugnisse (lit. f, h, i und j).[69] Alle Befugnisse des Art. 58 (mit Ausnahme des Art. 58 Abs. 2 lit. i EU-DSGVO) richten sich nach dem Wortlaut an die Verantwortlichen und Auftragsverarbeiter. Gemäß des Art. 4 Nr. 7 EU-DSGVO zählen zu den Verantwortlichen alle natürlichen oder juristische Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden (Art. 4 Nr. 7 EU-DSGVO). Da die Behörden explizit in dieser Definition mit aufgeführt sind, gelten die Befugnisse auch gegenüber der öffentlichen Verwaltung. Dies ist bereits eine Neuerung gegenüber dem alten Datenschutzrecht, in dem die Aufsichtsbehörden keinerlei Anordnungsbefugnisse gegenüber den Behörden hatten.[70]

Damit eine effektive Durchführung dieser Befugnisse erfolgen kann, sollte der Europäische Datenschutzausschuss Richtlinien und Leitfäden erstellen.[71] Dies wird jedoch noch einige Zeit in Anspruch nehmen, nach dem die EU-DSGVO gilt, da erst durch die Auslegung von unbestimmten Rechtsbegriffen und Rechtsprechung durch den Europäischen Gerichtshof Rechtssicherheit in der Umsetzung entstehen kann.[72]

1. Verwarnungen

Die Warnung und die Verwarnung sind in Art. 58 Abs. 2 lit. a und b EU-DSGVO geregelt. Sie haben den Zweck, den Verantwortlichen klar zu signalisieren, dass ihr Verhalten nicht den Datenschutzvorschriften entspricht. Die erste Stufe ist die Warnung, bei der die Aufsichtsbehörde anzeigt, dass der Verarbeitungsvorgang voraussichtlich gegen Datenschutzbestimmungen verstößt. Somit wird den Verantwortlichen noch die Gele-

[69] Vgl .Erwägungsgrund Nr. 129 zur EU-DSGVO.
[70] Vgl. *Voßhoff,* BfDI - Info 6, 2016, 16.
[71] Vgl. EU-Datenschutz-Grundverordnung, Gesetzestext mit eingereihten Erwägungsgründen, 2016, 165.
[72] Vgl. *Ashkar*, in: DuD 12/2015, 796 (799-800).

genheit gegeben , den betroffenen Verarbeitungsvorgang zu überarbeiten, damit erst gar keine Verstöße begangen werden. Sie soll demnach präventiv Sorge tragen, dass kein Verstoß eintritt.

Die nächste Stufe der einfachen Sanktionierung ist die Verwarnung. Bei der Verwarnung muss bereits ein Datenschutzverstoß eingetreten sein, um diese auszusprechen. Sie ähnelt dem Beanstandungsrecht des/der Bundesbeauftragten für den Datenschutz in Deutschland nach § 25 BDSG; das bisher einzige Mittel der Sanktionierung gegen Behörden auf Bundesebene. Die Maßnahme der Verwarnung nach Art. 58 Abs. 2 lit. b EU-DSGVO könnte in Deutschland demnach ähnlich angewandt werden wie die Beanstandung. Mit der Verwarnung könnten die Aufsichtsbehörden den Verantwortlichen Hinweise geben, wie sie die rechtswidrige Datenverarbeitung rechtskonform gestalten können und gleichzeitig darstellen, welche weiteren Schritte von der Aufsichtsbehörde eingeleitet werden, falls der Datenschutzverstoß nicht beseitigt wird. Die Aufsichtsbehörden könnten die Verantwortlichen auch zu einer Stellungnahme auffordern, wie es ebenso im § 25 Abs. 1 BDSG geregelt ist. Sollte eine Verwarnung keinen Erfolg haben und die rechtswidrige Verarbeitung weiterhin betrieben werden, kommen die nächsten Maßnahmen zum Zug. Doch die Praxis zeigt, dass die Verwarnung ein effektives Mittel für die Beseitigung von Datenschutzverstößen ist.[73] Bevor die Aufsichtsbehörden mit Sanktionen mit Regelungscharakter einschreiten, sollte daher unbedingt eine Warnung oder Verwarnung erfolgen, mit der die Folgen bei einer andauernden Datenschutzverletzung aufgezeigt werden, um den Verantwortlichen zum Umdenken anzuregen. Bei einem schwerwiegenden Verstoß sollte aber zu der Verwarnung bereits ein Bußgeld verhängt werden, damit die Verantwortlichen diesen Umstand, eine zweite Chance zu erhalten, nicht ausnutzen können.

Da die Warnung und Verwarnung keinen Regelungscharakter aufzeigen, handelt es sich hierbei um keine Verwaltungsakte, so dass gegen sie kein verwaltungsrechtlicher Rechtsbehelf wirksam ist. Als Mittel gegen diese

[73] Vgl. *Smoltczyk,* Datenschutz und Informationsfreiheit Bericht 2015 Berlin, 2016, 165.

Maßnahme der Aufsichtsbehörde könnten nur Beschwerden oder Aufforderungen zur Rücknahme, ohne rechtliche Wirkung, sein.

2. Anweisungen

Die Anweisungsbefugnisse der Aufsichtsbehörden haben den Zweck, dass die Aufsichtsbehörden selbst einstreiten und den Verantwortlichen direkt auffordern können, um die rechtswidrige Datenverarbeitung zu stoppen. Im Gegenzug zu der Warnung und Verwarnung, haben die verwaltungsrechtlichen Anordnungen einen rechtsverbindlichen Regelungscharakter, damit die EU-DSGVO rechtlich durchgesetzt werden kann. Die Anweisungen bedürfen nun der Schriftform und es sollten in den Mitgliedstaaten verwaltungsrechtliche Rechtsbehelfe eingeführt werden bzw. vorhanden sein.[74] Die Anordnungsbefugnisse umfassen insbesondere folgende Maßnahmen: Die Aufsichtsbehörden können den Verantwortlichen oder Auftragsverarbeiter anweisen, dass

1. den Anträgen von betroffenen Personen entsprochen werden soll (lit. c),
2. rechtswidrige Verarbeitungsvorgänge in Einklang mit der EU-DSGVO gebracht werden sollen (lit. d),
3. personenbezogene Daten berichtigt oder gelöscht werden und diese Maßnahmen der betroffenen Person mitgeteilt werden sollen (lit. g).

Desweiteren können die Aufsichtsbehörden nach Art. 58 Abs. 2 EU-DSGVO den Zertifizierungsstellen anordnen, eine Zertifizierung zu widerrufen oder diese nicht zu erteilen (lit. h). Mit diesen Anordnungsbefugnissen haben die Aufsichtsbehörden in Deutschland zum allerersten Mal die Möglichkeit, auch gegen Behörden verbindliche Rechtsakte zu erlassen.[75] Durch das Beanstandungsrecht kann der/die Bundes- und die Landesdatenschutzbeauftagte/n nur hoffen, dass die Behördenleitung ihre Empfehlungen umsetzen, die sie in ihrer Beanstandung vorgeschlagen haben. Durch diese neuen Instrumente könnte der Datenschutz in Behör-

[74] Vgl. Erwägungsgrund Nr. 129 zur EU-DSGVO.
[75] Vgl. *Schulzki-Haddouti*, in: c't 13/2016, 154 (156).

den signifikant verbessert werden. Doch dadurch wird es neue Herausforderungen für die Fachbereiche in den Behörden geben, die die Organisationsstrukturen und Arbeitsabläufe datenschutzgerecht gestalten müssen.[76] Dies könnte erheblichen Mehraufwand und Mehrkosten in der öffentlichen Verwaltung entstehen lassen. Daher ist es wichtig, dass die Anordnungen der Aufsichtsbehörden verhältnismäßig sind. In den Erwägungsgründen zur EU-DSGVO ist explizit genannt worden, dass auf die Kosten und weiterführende Folgen einer etwaigen Anordnung geachtet werden soll.[77] In Deutschland gibt es bereits die Möglichkeit gegen Unternehmen Anordnungsbefugnisse durchzuführen (§ 38 Abs. 5 BDSG). In den letzten Jahren wurden diese jedoch wenig in Anspruch genommen, da sie für die Unternehmen sehr komplex zum Umsetzen sind.[78] Dennoch stellen sie eine sinnvolle Methode, für eine wirksame Durchsetzung der EU-DSGVO, dar.

Bei den Anträgen von betroffenen Personen, handelt es sich um die Geltendmachung der Rechte der EU-DSGVO. Sollte eine Behörde den betroffenen Personen nicht entgegen kommen, kann die zuständige Aufsichtsbehörde die Behördenleitung anweisen, dass sie dem Antrag abhelfen. Vor allem das Auskunftsrecht gem. Art. 15 EU-DSGVO könnte die Behörden betreffen, da viele Bürgerinnen und Bürger sich für ihre bei den Behörden gespeicherten Daten interessieren. Vor allem im Bereich der Sozialverwaltung, in der Massen an sensiblen personenbezogene Daten gespeichert werden, muss in Zukunft darauf geachtet werden, dass nur die für den Zweck erforderlichen Daten gespeichert werden.

Desweiteren können die Aufsichtsbehörden nach Art. 58 Abs. 2 EU-DSGVO den Zertifizierungsstellen anordnen, eine Zertifizierung zu widerrufen oder diese nicht zu erteilen (lit. h).

[76] Vgl. *Ashkar*, in: DuD 12/2015, 796.
[77] Vgl. Erwägungsgrund Nr. 129 zur EU-DSGVO.
[78] Vgl. *Ehmann*, in: ZD 10/2014, 493 (494).

3. Sanktionen

Die letzten Mittel der Aufsichtsbehörden für die Durchsetzung der Verordnung gem. § 58 Abs. 2 EU-DSGVO, sind die Sanktionsbefugnisse. Die Sanktionen sollen aufzeigen, dass der Datenschutz in der Europäischen Union einen hohen Stellenwert hat und nicht ohne Folgen verletzt werden kann.[79] In der Vorschrift des Artikel 58 Abs. 2 EU-DSGVO kommen folgende Sanktionen in Betracht:

1. Beschränkung und Verbot der Datenverarbeitung (lit. f),
2. Widerruf eines Zertifikates nach Art. 42 EU-DSGVO (lit. h),
3. Verhängung von Geldbußen nach Art. 83 EU-DSGVO (lit. i).

Die Beschränkung oder das Verbot von Datenverarbeitungsvorgängen, stellt wahrscheinlich die höchste Strafe für einen Verantwortlichen oder Auftragsverarbeiter dar. Durch ein Verbot der Datenverarbeitung in einem Unternehmen oder in einer Behörde, könnte die gesamte Betriebstätigkeit eingestellt werden, was zu einem hohen Verlust für den Verantwortlichen führen könnte. Ein Verbot der Datenverarbeitung in einer Behörde würde ebenso verheerende Konsequenzen mit sich ziehen; nicht nur für die Mitarbeiterinnen und Mitarbeiter, sondern auch für die Bürgerinnen und Bürger. Da die öffentliche Verwaltung rechtlich verpflichtende Aufgaben zu erfüllen hat, von denen Bürgerinnen und Bürger auch betroffen sind, würde ein Verbot der Datenverarbeitung in vielen Bereichen in der Praxis nicht in Frage kommen. Dennoch könnte eine Beschränkung von bestimmten Datenverarbeitungsvorgängen in Betracht kommen, die nicht essenziell für die pflichtgemäße Aufgabenerfüllung notwendig sind. So könnte die Aufsichtsbehörde z.B. in Jobcentern Anfragen und Auskünfte bei Banken über Konten von Leistungsempfängern verbieten oder bestimmen, dass bestimmte Informationen und Unterlagen (wie Kontoauszüge) in den Akten der Leistungsempfänger nicht mehr abgelegt werden

[79] Vgl. *Albrecht,* Die Datenschutzreform der Europäischen Union, 2015, 25. (Siehe Anlage 11).

dürfen. Der Verhältnismäßigkeitsgrundsatz spielt auch hier eine wichtige Rolle.

Der Widerruf eines Datenschutzsiegels oder eines Datenschutzzertifikates kann für den Verantwortlichen negative Auswirkungen haben. Durch diesen Entzug könnte das Unternehmen eine Rufschädigung erleiden, so dass Kundinnen und Kunden die Dienste nicht mehr in Anspruch nehmen möchten. Vor allem für große Internetfirmen wie PayPal, Amazon oder Facebook, die Massen an personenbezogene Daten verarbeiten, könnte eine derartige Rufschädigung einen hohen Verlust verursachen. Für Behörden wäre diese Art der Sanktionierung wenig sinnvoll, da sie in der "normalen" Verwaltungstätigkeit nicht auf Umsatzerlöse und Kunden, die ihre Dienste in Anspruch nehmen, angewiesen sind. Es wäre höchstens für privatrechtliche wirtschaftliche Tätigkeiten von Gemeinden, wie Versorgungsbetriebe eine Alternative, mit denen Kommunen Gewinne erwirtschaften können.

Bei der letzten Sanktion handelt es sich um Bußgelder gem. Art. 58 Abs. 2 lit. i i.V.m. Art. 83 EU-DSGVO. Auf das Bußgeldverfahren der EU-DSGVO wird im nächsten Kapitel genauer eingegangen.

III. Bußgeldvorschriften

In den folgenden Kapiteln wird auf die Bußgeldvorschriften des Art. 83 EU-DSGVO eingegangen. Es soll danach erörtert werden, inwiefern Behörden und öffentliche Stellen dem Grunde nach von diesen Bußgeldvorschriften erfasst werden.

1. Charakter der Bußgelder

Die EU erhofft sich durch die neuen schärferen Sanktionsvorschriften, dass der Datenschutz in den Mitgliedstaaten konsequenter und pflichtbewusster von den Verantwortlichen umgesetzt wird.[80] In der ehemaligen Datenschutzrichtlinie 95/46/EG hat der EU-Gesetzgeber in Art. 24 den

[80] Vgl. Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen, 2010, 10. (Siehe Anlage 3).

Mitgliedstaaten freie Hand über die Art der Sanktionierung gelassen. Da unter anderem auch in Deutschland keine wirkungsvollen Sanktionen geschaffen wurden bzw. diese nur zögerlich von den Aufsichtsbehörden umgesetzt wurden,[81] bestand für die Verantwortlichen keine große Gefahr bestraft zu werden[82].

Die neuen Bußgeldvorschriften sollen diesen Umstand ändern. In Art. 83 Abs. 1 EU-DSGVO werden die Bußgelder als wirksam, verhältnismäßig und abschreckend charakterisiert. Letzteres wurde durch die hohen Beträge in den Absätzen 4 bis 6 verwirklicht. Doch die Gefahr ist groß, dass der "Abschreckungseffekt" der neuen Bußgelder schnell abklingt, wenn die Aufsichtsbehörden diese nicht konsequent zum Einsatz bringen.[83]

Das Ziel des Bußgeldverfahren ist es, die Täter zu maßregeln und sie zu sensibilisieren, dass sie in Zukunft die Datenschutzregeln einzuhalten haben. [84] Als weiteren Effekt soll die Geldbuße eingesetzt werden, um den Gewinn des Verantwortlichen abzuschöpfen, der durch den Datenschutzverstoß erlangt wurde.[85] Die Verantwortlichen müssen spüren, dass in keinerlei Hinsicht ein Vorteil durch den Datenschutzverstoß entsteht. Da Behörden und öffentliche Einrichtungen keinen Gewinn erwirtschaften dürfen (mit Ausnahme der wirtschaftlichen Unternehmen), ist diese Methode für den öffentlichen Bereich begrenzt anwendbar. Es könnten Methoden entwickelt werden, in denen der eingesparte Personalaufwand oder Sachaufwand in den Behörden, aufgrund des Datenschutzverstoßes, zur Bußgeldhöhe angerechnet wird, da Datenschutzverstöße in Behörden vor allem aus Zeit- und praktikablen Gründen begangen werden.

Für eine dauerhafte Steigerung des Schutzniveaus und Einhaltung der Datenschutzvorschriften sind die Bußgelder jedoch nicht geeignet.[86] Das Bußgeldverfahren kommt erst zur Anwendung, wenn bereits ein Verstoß gegen die Verordnung begangen wurde. Es hat daher keinen präventiven

[81] Vgl. *Hansen-Oest/Heidrich*, in: c't 9/2016, 166 (169).
[82] Vgl. *Schulzki-Haddouti*, in: c't 10/2016, 162 (163).
[83] Vgl. *Holländer,* in: Wolff/Brink/u.a., 2013, § 43 BDSG Rn. 43.
[84] Vgl. *Ronellenfitsch,* Dreiundvierzigster Tätigkeitsbericht, 2014, 148.
[85] Vgl. *Holländer,* in: Wolff/Brink/u.a., 2013, § 43 BDSG Rn. 70.
[86] Vgl. *Holländer,* in: Wolff/Brink/u.a., 2013, § 43 BDSG Rn. 76.

Charakter. Hierfür sind die Verwarnungen und Anweisungsbefugnisse sinnvoller, da die Aufsichtsbehörden bereits vor dem Eintritt eines Verstoßes handeln können, um diesen zu verhindern.

Vom Charakter her können die Bußgeldvorschriften der EU-DSGVO mit denen des Allgemeinen Gleichbehandlungsgesetzes (AGG) verglichen werden. Das AGG entstand durch die EU-Richtlinie 2000/78/EG und wurde durch den deutschen Gesetzgeber im Jahr 2006 umgesetzt. Die Sanktionen des AGG sollen gem. Art. 17 der Richtlinie bei den Arbeitgebern einen präventiven und abschreckenden Effekt bewirken.[87] Die Sanktionen sind u. a. in § 15 AGG geregelt. Durch dieses Gesetz können ebenso öffentliche Arbeitgeber für rechtswidrige Handlungen von anderen Behörden sanktioniert werden.

2. Aufbau des Art. 83 EU-DSGVO

Der Art. 83 EU-DSGVO umfasst neun Absätze. Der erste Absatz gibt kurz Klarheit über den Charakter der zu verhängenden Bußgelder. Die Geldbußen müssen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Absatz 2 enthält einen ausführlichen Katalog an Bestimmungen, die in einem Bußgeldverfahren geprüft werden müssen. Diese stellen jedoch keine Tatbestandsvoraussetzung dar, sondern sind vielmehr relevant für die Prüfung, wenn ein Ordnungswidrigkeitstatbestand bereits erfüllt wurde. Desweiteren gibt Absatz 2 nochmals den Hinweis, dass die Bußgelder zusätzlich zu oder anstelle von Maßnahmen nach Art. 58 Abs. 2 EU-DSGVO verhängt werden können. In Absatz 3 befindet sich die Regelung, dass bei mehreren Datenschutzverstößen nur das höchstmögliche Bußgeld verhängt werden kann und nicht mehrere auf einmal. Über die verschiedenen Tatbestände und Verstöße geben die Absätze 4 bis 6 Auskunft. In jedem der 3 Absätze sind die Höhe der Geldbuße und die Vorschriften, die bußgeldrelevant sind, aufgeführt.

In Absatz 7 ist die Öffnungsklausel für die Mitgliedstaaten enthalten; darin können die Mitgliedstaaten entscheiden, ob und inwieweit Behörden und

[87] Vgl. Erwägungsgrund Nr. 35 zur Richtlinie 2000/78/EG.

öffentliche Stellen von den Bußgeldvorschriften betroffen sind. Die Regelung über die Rechtsbehelfe und gerichtliche Verfahren sind in Absatz 8 enthalten. Dieser sagt aus, dass in den Mitgliedstaaten angemessene Rechtsmittel für das Bußgeldverfahren zur Verfügung stehen müssen. Der letzte Absatz regelt die Möglichkeit, dass durch die Gerichte Bußgelder verhängt werden können, wenn sich ein Mitgliedstaat dazu entschließt, dass keine Sanktionen in Form der Bußgelder erlassen werden können.

3. Verstöße gegen die Verordnung

Der Art. 83 EU-DSGVO enthält für das Bußgeldverfahren 3 Kategorien an Verstößen:

a) Verstöße erster Kategorie

Bei den Verstößen der ersten Kategorie, handelt es sich gem. Art. 83 Abs. 4 EU-DSGVO um Verstöße gegen die Pflichten der Verantwortlichen und Auftragsverarbeiter. Desweiteren können durch diesen Absatz ebenso die Zertifizierungsstellen und Überwachungsstellen sanktioniert werden, wenn sie ihrer Verpflichtungen nach den Artikeln 42 und 43 bzw. Art. 41 Abs. 4 EU-DSGVO nicht nachkommen.

Die Verstöße nach Absatz 4 werden mit einer Geldbuße von höchstens 10 Mio. Euro geahndet oder, wenn es sich um ein Unternehmen handelt, bis zu 2 Prozent seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs. Die Bußgeldbeträge sind demnach für "sonstige Personen" auf 10 Mio. Euro begrenzt; Unternehmen können dagegen mit weitaus höheren Geldbußen sanktioniert werden. Bei allen Bußgeldverfahren sind die Verhältnismäßigkeit und die Ermessenskriterien nach Absatz 2 zu prüfen. Es ist im Bußgeldverfahren irrelevant, ob die Ordnungswidrigkeit vorsätzlich oder fahrlässig begangen wurde. Dieser Gesichtspunkt kann jedoch entweder mildernde oder verschärfende Umstände herbeiführen.

Durch diese Vorschrift werden die Verantwortlichen angehalten, alle ihre Verpflichtungen wahrzunehmen und ordnungsgemäß durchzuführen. Vor

allem die Themen Datenschutzmanagement (Art. 24, 25 EU-DSGVO) und Datenschutz-Folgenabschätzung (Art. 35 EU-DSGVO) werden in Zukunft wichtig für die Unternehmen und Behörden werden, da diese Verpflichtungen durch die Verordnung neu geschaffen wurden und in den 2 Jahren, bis die Verordnung gilt, umgesetzt werden müssen. Jedoch ist es problematisch in Deutschland, ob die Verantwortlichen diesen Verpflichtungen tatsächlich nachkommen. In den letzten Jahren wurden viele Verantwortliche, vor allem aus Gründen des Personalmangels in den Aufsichtsbehörden,[88] kaum sanktioniert. Dadurch wurde der Datenschutz in den Unternehmen dementsprechend nicht ernst genommen.[89] Daher ist es wichtig, die Verantwortlichen bestmöglich zu sensibilisieren und über die neuen Regelungen, in der Zeit bis die Datenschutzgrundverordnung gilt, aufzuklären. Vor allem die Regelung des Art. 37 EU-DSGVO, dass jede Behörde und alle Unternehmen, für die Datenverarbeitungsvorgänge zu der Kerntätigkeit gehören, einen Datenschutzbeauftragten benennen müssen, wird sehr praxisrelevant werden. Ein innerbetrieblicher Datenschutzbeauftragter kann Sensibilisierungsmaßnahmen und Umstrukturierungsmaßnahmen für sein Unternehmen oder seine Behörde in die Wege leiten, damit die Datenschutzgrundverordnung befolgt werden kann.

b) Verstöße zweiter Kategorie

Die Verstöße zweiter Kategorie sind im Absatz 5 geregelt. Bei diesen Verstößen handelt es sich hauptsächlich um Verstöße gegen die Grundsätze der Datenverarbeitung und die Rechte von betroffenen Personen. Ebenso werden Verstöße gegen die Vorschriften für besondere Verarbeitungstätigkeiten, nach dem neunten Kapitel der EU-DSGVO und die Datenübertragung in Drittstaaten, bußgeldbewährt.

Diese Ordnungswidrigkeiten werden bereits mit einem Bußgeld von bis zu 20 Mio. Euro oder bei Unternehmen bis zu 4 Prozent des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet.

[88] Vgl. *Schulzki-Haddouti*, in: c't 10/2016, 162.
[89] Vgl. *Schulzki-Haddouti*, in: c't 12/2015, 66.

Bei dieser Verdopplung der Obergrenze der Geldbußen spürt man den Charakter der Datenschutzgrundverordnung, der auf den verstärkten Schutz von betroffenen Personen gerichtet ist. Es wird den Verantwortlichen signalisiert, dass die Betroffenenrechte und die Grundsätze der Verordnung eine sehr wichtige Position inne haben und besondere Aufmerksamkeit bei der Datenverarbeitung bedürfen. Da für die betroffenen Personen das Recht der Beschwerde bei den Aufsichtsbehörden durch die erleichterten Umstände (neue Zuständigkeitsregeln der Aufsichtsbehörden, keine Verwaltungsgebühren, online Formulare) gestärkt wurde,[90] könnten sich die Beschwerden in den nächsten Jahren häufen. Dadurch erhöht sich das Risiko für die Behörden und Unternehmen, von den Aufsichtsbehörden kontrolliert zu werden. Interessante Themenfelder werden für die Verantwortlichen die neuen Transparenzpflichten nach Art. 12 Abs. 1 EU-DSGVO (vor allem die Einführung der" einfachen Sprache"), die erweiterten Informationspflichten gegenüber den betroffenen Personen (Art. 13, 14, 34 EU-DSGVO), das neue Einwilligungsverfahren (Art. 7, 8 EU-DSGVO) und das "Recht auf Vergessenwerden" (Art. 17 EU-DSGVO).

c) Verstöße dritter Kategorie

Als letzte Bußgeldvorschriften kommen die Verstöße nach Art. 83 Abs. 6 EU-DSGVO. Bei diesen Verstößen, handelt es sich um die Nichteinhaltung von Anweisungen der Aufsichtsbehörde nach Art. 58 Abs. 2 EU-DSGVO. Falls ein Verantwortlicher eine Anweisung der zuständigen Aufsichtsbehörde nicht befolgt, kann ein Bußgeld von bis zu 20 Mio. Euro verhängt werden und bei Unternehmen ebenso bis zu 4 Prozent des letzten Jahresumsatzes.

Durch diese Bußgeldvorschrift haben die Aufsichtsbehörden ein weiteres Druckmittel zur Durchsetzung ihrer Anweisungsbefugnisse und eine weitere Aufwertung ihrer Stellung erhalten. So könnte es sein, dass ein Verantwortlicher zusätzlich zu einem Verbot der Datenverarbeitung nach Art. 58 Abs. 2 lit. f EU-DSGVO eine Geldbuße nach Art. 58 Abs. 2 lit. i i.V.m. Art.

[90] Art. 57 Abs. 2 EU-DSGVO.

83 Abs. 6 EU-DSGVO verhängt bekommt. Die Verantwortlichen könnten bei Nichteinhaltung der datenschutzrechtlichen Anordnungen demnach in einen "Teufelskreis" geraten, den sie nur durch die Befolgung der Anweisungen oder durch einen erfolgreichen verwaltungsrechtlichen Rechtsbehelf verlassen können. Die Möglichkeit, dass bei einer Nichtbezahlung eines Bußgeldes nach Art. 58 Abs. 2 lit. i EU-DSGVO nochmal ein Bußgeld nach Art. 83 Abs. 6 EU-DSGVO verhängt werden kann, wurde durch die Regelung des Art. 58 Abs. 2 Satz 1 EU-DSGVO ausgeschlossen.

Bei Durchführung dieser Vorschrift muss, ebenso wie bei den anderen, die Verhältnismäßigkeit beachtet werden.[91] Es soll nicht Sinn und Zweck sein, die Verantwortlichen durch diese Regelung zu "drangsalieren". Es sollte vielmehr ein zusätzlicher Anreiz sein, damit die Verantwortlichen kooperativ mit den Aufsichtsbehörden zusammen arbeiten und den Schutz der personenbezogenen Daten ihrer Kundinnen und Kunden sicherstellen.

4. Bedingungen zur Verhängung von Bußgelder

Bereits in Art. 83 Abs. 1 EU-DSGVO wird darauf hingewiesen, dass die Bußgelder in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein sollen. In dieser Vorschrift sind mehrere Punkte enthalten, die essentiell für die Bearbeitung sind. Es bedarf auf jeden Fall:

- einer Einzelfallprüfung,
- einer Verhältnismäßigkeitsprüfung[92],
- eines wirkungsvollen und effektiven Bußgeldes,
- des abschreckenden Charakters des Bußgeldes.

Der Bußgeldbescheid muss außerdem verwaltungsrechtliche Formvorschriften erfüllen. Hierfür müssen die Regelungen der Datenschutzgrundverordnung und das Verwaltungsrecht des jeweiligen Mitgliedstaates beachtet werden.[93] In dem Erwägungsgrund Nr. 129 zu Art. 58 EU-DSGVO

[91] Vgl. *Albrecht,* Die Datenschutzreform der Europäischen Union, 2015, 25. (Siehe Anlage 11).
[92] Vgl. Erwägungsgrund Nr. 129 zur EU-DSGVO.
[93] Ebenda.

wird auf die formalen Voraussetzungen eingegangen. Jede rechtsverbindliche Maßnahme der Aufsichtsbehörden bedarf der Schriftform (mit Unterschrift des Leiters), einer klaren und eindeutigen Ausdrucksweise (Bestimmtheit) und es sollte darauf die zuständige Aufsichtsbehörde und das Datum der angeordneten Maßnahme angegeben sein.[94]

Die materiellen Voraussetzungen ergeben sich aus den jeweiligen Bußgeldvorschriften, deren Tatbestandsvoraussetzungen und den Abwägungskriterien nach Art. 58 Abs.2, die in jedem Einzelfall zu prüfen sind. In Absatz 2 wird zuerst die Möglichkeit für die Aufsichtsbehörden eingeräumt, dass Geldbußen zu oder anstelle von Maßnahmen nach Art. 58 Abs. 2 lit. a bis h und j[95] verhängt werden können. Die Prüfungskriterien umfassen 11 Punkte (von a bis k) und sind im Erwägungsgrund 148 Satz 3 folgendermaßen zusammengefasst:

> "Folgendem sollte jedoch gebührend Rechnung getragen werden: der Art, Schwere und Dauer des Verstoßes, dem vorsätzlichen Charakter des Verstoßes, den Maßnahmen zur Minderung des entstandenen Schadens, dem Grad der Verantwortlichkeit oder jeglichem früheren Verstoß, der Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, der Einhaltung der gegen den Verantwortlichen oder Auftragsverarbeiter angeordneten Maßnahmen, der Einhaltung von Verhaltensregeln und jedem anderen erschwerenden oder mildernden Umstand."[96]

Fraglich ist, wie man diese Abwägungskriterien tatsächlich überprüfen kann. Anhaltspunkte, um die Art, Schwere und Dauer des Verstoßes nachzuweisen, könnten sich durch die Dokumentation der Datenverarbeitungsvorgänge ergeben. Gem. Art. 30 EU-DSGVO sind die Verantwortlichen dazu verpflichtet, Verzeichnisse über die Verarbeitungstätigkeiten zu führen. Durch das Verzeichnis ist ersichtlich, welche Art von personenbezogenen Daten, für welchen Zweck verarbeitet wurden.

Um die Vorsätzlichkeit eines Verstoßes nachzuweisen, könnten Dienstanweisungen zu bestimmten Arbeitsschritten, direkte schriftliche Anwei-

[94] Ebenda.
[95] Hier wird auf die englische Fassung der EU-DSGVO verwiesen. In der deutschen Fassung steht in Art. 83 Abs. 2 S. 1: "a bis h und i". Dies würde jedoch keinen Sinn ergeben, da in Art. 58 Abs. 2 lit. i das Bußgeld aufgeführt ist und lit. j ausgelassen wird. In der französischen Fassung ist es ebenso abgedruckt, wie in der englischen. (Siehe Anlage 2).
[96] Erwägungsgrund Nr. 148 S. 3 zur EU-DSGVO.

sungen der verantwortlichen Führungskraft oder auch Aktenvermerke über die rechtswidrige Datenverarbeitung herangezogen werden, sofern derartige Dokumente vorhanden sind. Auf den Grad der Verantwortlichkeit des Verantwortlichen und inwiefern Gegenmaßnahmen aufgrund des Verstoßes erfolgten, könnten sich durch ein vorhandenes Datenschutz-Management schließen lassen. Hat das Unternehmen oder die Behörde geeignete und ausreichende organisatorische und technische Maßnahmen nach den Artikeln 24, 25 und 32 EU-DSGVO getroffen, so könnte dies mildernde Umstände herbeiführen.

Wichtig ist ebenso, ob die Frist zur Meldung eines Datenschutzverstoßes nach Art. 33 EU-DSGVO eingehalten wurde. Dies lässt sich unproblematisch auf der Seite der Aufsichtsbehörde feststellen. Sollte der Verstoß durch die Medien oder durch einen Whistleblower der Öffentlichkeit bekannt werden, könnte dies negative Folgen für den Verantwortlichen haben. Da die Prüfung der Abwägungskriterien umfangreich und komplex in der Praxis sein wird, sollte der Europäische-Datenschutzausschuss Richtlinien und Leitfäden für die Durchführung des Bußgeldverfahrens den Aufsichtsbehörden bereitstellen.[97]

Für die Bestimmung der Höhe des Bußgeldes, gibt es im Erwägungsgrund Nr. 150 zu Art. 83 EU-DSGVO den Hinweis, dass für natürliche Personen auf deren Einkommensverhältnisse und deren "wirtschaftlichen Lage" geachtet werden muss.[98] Die Aufsichtsbehörden könnten für die Bußgeldfestsetzung im Falle von Behörden ebenso auf deren "wirtschaftlichen Lage" und auf das Haushaltsvolumen der Kommune bzw. das Budget der Behörde Bezug nehmen. So könnte der nationale Gesetzgeber, die Umsetzung und die Höhe des Bußgeldes für Unternehmen analog auf die Behörden anwenden. Die Regelung nach Art. 83 Abs. 4 EU-DSGVO könnte demnach für Behörden lauten: Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10

[97] Vgl. EU-Datenschutz-Grundverordnung, Gesetzestext mit eingereihten Erwägungsgründen, 2016, 165.
[98] Vgl. Erwägungsgrund Nr. 150 zur EU-DSGVO.

Mio. Euro oder von bis zu 2 Prozent des Haushaltsvolumens des vorangegangenen Haushaltsjahres verhängt, je nachdem, welcher der Beträge höher ist. Die nationalen Gesetzgeber der Mitgliedstaaten haben durch die Öffnungsklausel des Art. 83 Abs. 7 EU-DSGVO die Möglichkeit, zu bestimmen, inwieweit die Behörden von den Bußgeldvorschriften betroffen sind. Hierfür sollten nationale Vorschriften erlassen werden. Für die allgemeine Anwendbarkeit der Bußgeldvorschriften auf Behörden, wird im nächsten Kapitel eingegangen.

5. Anwendbarkeit auf den öffentlichen Bereich

Die Bußgeldvorschrift des Art. 83 gibt keine eindeutige Auskunft, ob die öffentliche Verwaltung von der Regelung betroffen ist oder nicht. Durch die Öffnungsklausel in Art. 83 Abs. 7 EU-DSGVO könnte es sogar den Anschein erwecken, dass Behörden von der Regelung grundsätzlich ausgeschlossen sind. Für diese Beurteilung muss aber genauer auf die Vorschrift eingegangen werden. Es wird darauf hingewiesen, dass bei folgender Betrachtung der Aufgabenbereich der Strafverfolgung und Gefahrenabwehr des öffentlichen Sektors ausgenommen sind.[99]

a) Grundlegende Anwendbarkeit

Der Art. 83 EU-DSGVO ist eine Sanktionsmöglichkeit nach Art. 58 Abs. i EU-DSGVO. Diese richten sich i.d.R. gegen die Verantwortlichen (und deren Auftragsverarbeiter) für die Datenverarbeitung. In Art. 4 Nr. 7 EU-DSGVO ist der Begriff des Verantwortlichen definiert. Durch diese Begriffsbestimmung sind Behörden in den Kreis der Verantwortlichen mit aufgenommen worden. Die Definition wurde aus dem Artikel 2 lit. d der ehemaligen Datenschutzrichtlinie 95/46/EG übernommen. Durch den Umstand, dass in Art. 58 Abs. 2 Satz 1 EU-DSGVO der "Verantwortliche" nicht erwähnt wird, muss jeweils auf die spezielle Maßnahme und deren Ermächtigungsgrundlage in den Buchstaben eingegangen werden.

[99] Wie bereits in Punkt B. II. 2. und 3. erwähnt, sind die Bereiche der Strafverfolgung und der Gefahrenabwehr durch den Anwendungsbereich der Datenschutzgrundverordnung und der Datenschutzrichtlinie ausgeschlossen worden.

Art. 58 Abs. 2 lit. i EU-DSGVO verweist auf die spezielleren Bestimmungen des Art. 83 EU-DSGVO. In den Absätzen 4 bis 6 des Art. 83 EU-DSGVO heißt es: "Bei Verstößen gegen die folgenden Bestimmungen werden im Einklang mit Absatz 2 Geldbußen von bis zu 10.000.000 EUR bzw. 20.000.000 EUR oder im Fall eines Unternehmens [...]". Durch diese Formulierung ergeben sich zwei Fallgruppen: Die Unternehmen und die "sonstigen Verantwortlichen", welche nicht ausdrücklich erwähnt werden. Ob die Behörden und öffentlichen Stellen unter die "sonstigen Verantwortlichen" fallen ist fraglich. In Erwägungsgrund Nr. 150 Satz 3 ff wird auf die Bußgeldfestsetzung gegenüber den beiden Fallgruppen eingegangen. In Satz 3 werden die Unternehmen erläutert. Der Satz 4 des Erwägungsgrundes 150 handelt von den Personen, die keine Unternehmen sind. Der Wortlaut des Satz 4 lässt auf natürliche Personen schließen, da bei der Bußgeldfestsetzung auf das "Einkommensniveau "des Mitgliedstaates und der "wirtschaftlichen Lage" der Person geachtet werden muss.[100] In dem Erwägungsgrund 150 Satz 6 ist wieder aufgeführt, dass die Mitgliedstaaten in nationalen Vorschriften genauere Regelungen über die Bußgeldverhängung von Behörden erlassen können.[101] Somit ergibt sich über den Wortlaut des Art. 58 und 83 EU-DSGVO keine zufriedenstellende Lösung. Er tendiert eher dazu, dass der öffentliche Sektor nicht mit inbegriffen ist. Da der genaue Wortlaut des Art. 83 EU-DSGVO keine eindeutige Auskunft darüber gibt, müssen weitere Aspekte hinzugezogen werden.

Ein Argument, dass für die Anwendbarkeit auf den öffentlichen Sektor spricht, könnte sich aus dem Europarecht ergeben. Bei der Datenschutzgrundverordnung , handelt es sich um eine Verordnung der Europäischen Union nach Art. 288 Abs. 2 AEUV. EU-Verordnungen haben den Charakter, dass sie in allen Teilen und in jedem Mitgliedstaat unmittelbar verbindlich sind.[102] Die Datenschutzgrundverordnung regelt die Verarbeitung und den Schutz personenbezogener Daten in der EU für den privaten und öffentlichen Bereich. Da der öffentliche Bereich von den Bußgeldvorschriften

[100] Vgl. Erwägungsgrund Nr. 150 zur EU-DSGVO.
[101] Ebenda.
[102] Vgl. *Hetmeier,* in: Lenz/Borchardt/u.a., 2013, Art. 288 Abs. 2 AUEV Rn. 8 und 9.

des Art. 83 EU-DSGVO nach dem Wortlaut nicht eindeutig ausgenommen wurde, könnte der Art. 83 EU-DSGVO grundsätzlich für die öffentliche Verwaltung nach dem Grundsatz des Art. 288 Abs. 2 AEUV gelten. Durch die Öffnungsklausel des Art. 83 Abs. 7 EU-DSGVO können die Mitgliedstaaten zwar nationale Bußgeldvorschriften für den öffentlichen Bereich erlassen. Sollten sie die Öffnungsklausel jedoch nicht nutzen, so kommt, durch den Charakter der Verordnung, die volle Geltung des Art. 83 EU-DSGVO auch für Behörden und öffentliche Stellen zum Tragen.[103] Es kann nicht im Sinn des EU-Gesetzgebers gewesen sein, dass der öffentliche Bereich, durch ein "Unterlassen" der Mitgliedstaaten, von den Bußgeldvorschriften nicht berührt wird.

Eine weitere Möglichkeit für die Klärung könnte sich aus einer teleologischen Auslegung des Art. 83 EU-DSGVO ergeben. Hierfür bedarf es zuerst des Zweckes des Gesetzes bzw. der Vorschrift. Der Zweck der Datenschutzgrundverordnung ist (wie bereits in B. I. 3. ausführlich erwähnt), u.a. der Schutz der personenbezogenen Daten der betroffenen Personen. In dem Erwägungsgrund Nr. 11 wurde niedergeschrieben, dass es für den Schutz personenbezogener Daten europaweit gleicher und verschärfter Sanktionen, zur konsequenteren Durchsetzung, für die Verantwortlichen erfordert. Aus diesem Erwägungsgrund erschließt sich der Charakter des Art. 83 EU-DSGVO. Es ist im Interesse des EU-Gesetzgebers, dass die Datenschutzgrundverordnung in der gesamten EU gleichmäßig in allen Bereichen, in denen personenbezogene Daten verarbeitet werden, durchgesetzt wird und die personenbezogene Daten ebenso in allen Bereichen geschützt werden. Daher hat der EU-Gesetzgeber die gleichen Regelungen für den privaten und öffentlichen Bereich geschaffen, mit der Ausnahme, dass es für den öffentlichen Bereich einige Öffnungsklauseln[104], für speziellere nationale Regelungen, gibt.[105] Vom Grundsatz gelten alle

[103] Vgl. *Benecke/Wagner*, in: DVBl 10/2016, 600 (606).
[104] Z.B. Art. 6 Abs. 2 ff; Art. 23; Art. 83 Abs. 7; Art. 86; Art. 88; usw.
[105] Vgl. Datenschutzpaket – Bericht über die unter zyprischem Vorsitz erzielten Fortschritte -Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), 2012, 8. (Siehe Anlage 6).

Regelungen der EU-DSGVO für den privaten und öffentlichen Bereich gleich. Somit kann die öffentliche Verwaltung nach diesem Gesichtspunkt nicht von den Bußgeldvorschriften des Art. 83 EU-DSGVO, vom Prinzip her, ausgeschlossen werden.

Es könnte sich aber aus einer anderen Sicht eine andere Lösung ergeben. Betrachtet man die Vorschrift des Art. 83 Abs. 7 EU-DSGVO genauer, so könnte argumentiert werden, dass der öffentliche Bereich durch die Öffnungsklausel automisch ausgeschlossen wird. Die Öffnungsklausel hat den Sinn, dass den Mitgliedstaaten die vollkommene Freiheit darüber gelassen wird, ob die Bußgeldvorschriften für den öffentlichen Bereich gelten. Durch den Umstand, dass es in der Öffnungsklausel keine Frist gibt, in der die Mitgliedstaaten ihre nationalen Vorschriften, die sie aufgrund der Öffnungsklausel erlassen haben, der Europäischen Kommission vorlegen müssen, macht es den Anschein, dass die Mitgliedstaaten keine Regelungen aufzustellen brauchen, um die Wirkung der Öffnungsklausel zu verwirklichen. In der Datenschutzrichtlinie für die Strafverfolgung haben die Mitgliedstaaten gem. Art. 57 ebenso freie Hand darüber, ob sie Sanktionen gegen ihre Behörden einführen. Hier wurde, wie damals in der Datenschutzrichtlinie 46/95/EG, eine freigestalterische Ermächtigungsgrundlage für die Sanktionierung eingefügt. Falls der europäische Gesetzgeber den Mitgliedstaaten wirklich die komplette Freiheit über die Bußgeldbewährtheit des öffentlichen Bereiches lassen wollte, so müsste die Öffnungsklausel des Art. 83 Abs. 7 EU-DSGVO eine rechtsschaffende Wirkung haben, mit dem Zweck, dass die Mitgliedstaaten erst nationale Vorschriften bzw. einen Rechtsakt erlassen müssen, damit die öffentliche Verwaltung mit Bußgeldern sanktioniert werden kann. Somit kann, aus dieser Perspektive, keiner Anwendbarkeit des Art. 83 EU-DSGVO auf den öffentlichen Bereich zugesprochen werden.

Nach den vorstehenden Gründen, kann keine eindeutige Antwort auf die Frage erbracht werden, ob eine grundlegende Anwendbarkeit vorhanden ist. Für eine endgültige Beurteilung bedarf es Rechtsprechungen des Europäischen Gerichtshofes.

b) Öffnungsklausel

> "Unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Artikel 58 Absatz 2 kann jeder Mitgliedstaat Vorschriften dafür festlegen, ob und in welchem Umfang gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen verhängt werden können." (Art. 83 Abs. 7 EU-DSGVO)

Die Öffnungsklausel des Art. 83 Abs. 7 EU-DSGVO gibt den Mitgliedstaaten die Möglichkeit, selbst zu bestimmen, inwieweit die Bußgeldvorschriften des Art. 83 für seine Behörden und öffentliche Stellen gelten. Diesen Standpunkt des EU-Gesetzgebers findet sich in dem Erwägungsgrund Nr. 150 Satz 6 und in der Gesetzesbegründung[106] wieder.

In der Öffnungsklausel wird von Behörden und öffentlichen Stellen gesprochen. Da der öffentliche Bereich in den jeweiligen Mitgliedstaaten geregelt ist, können die Begriffe und Definitionen zu den Behörden und öffentlichen Stellen aus dem Recht der Mitgliedstaaten herangezogen werden. Eine Besonderheit in der Datenschutzgrundverordnung ist, dass die Behörden selbst Adressaten des Datenschutzrechts sind, obwohl sie z.B. in Deutschland nicht rechtsfähig sind[107]. Dies hat den Grund, dass das Datenschutzrecht, als materielles Recht, in den jeweiligen Fachbereichen, also in den verantwortlichen Abteilungen eines Verwaltungsträgers, zur Anwendung kommt und von diesen ausgeführt werden.[108] Diese sind dementsprechend verpflichtet, das Datenschutzrecht einzuhalten.

In Deutschland ist der Behördenbegriff in dem Verwaltungsverfahrensgesetz (VwVfG) und in den Landesverwaltungsverfahrensgesetzen (LVwVfG) der jeweiligen Bundesländer geregelt und wird im deutschen Datenschutzrecht zu Grunde gelegt.[109] Nach § 1 Abs. 4 VwVfG ist eine Behörde, jede Stelle, die Aufgaben der öffentlichen Verwaltung wahrnimmt. Bei der Legaldefinition des § 1 Abs. 4 VwVfG, handelt es sich um den funktionalen Behördenbegriff.[110] Zu den Behörden in Deutschland

[106] Vgl. EU-Datenschutz-Grundverordnung, Gesetzestext mit eingereihten Erwägungsgründen, 2016, 165.
[107] Vgl. *Kopp/Ramsauer,* 2013, § 1 VwVfG Rn. 51a.
[108] Vgl. *Hanloser,* in: Wolff/Brink/u.a., 2013, § 2 BDSG Rn. 6.
[109] Vgl. *Hanloser,* in: Wolff/Brink/u.a., 2013, § 2 BDSG Rn. 10.
[110] Vgl. *Kopp/Ramsauer,* 2013, § 1 VwVfG Rn. 51.

zählt demnach der gesamte öffentliche Dienst, der mit hoheitlichen Verwaltungsaufgaben ausgestattet ist.

Problematisch wird der Begriff der "öffentlichen Stelle". Grundsätzlich ist jede Behörde eine öffentliche Stelle.[111] Jedoch fallen nicht alle Geschäftsbereiche der öffentlichen Verwaltung nach § 1 Abs. 4 VwVfG unter den Begriff der "öffentlichen Stelle". Kritisch wird es in den Fällen, in denen öffentliche Aufgaben in privat-rechtlicher Form ausgeführt werden. Hierzu gehört zum Beispiel die öffentliche Daseinsvorsorge.[112] Durch den § 2 BDSG, ist der Begriff der "öffentlichen Stelle" weit gefasst worden. In § 2 BDSG gelten Vereinigungen von öffentlich-rechtlicher Einrichtungen, ungeachtet ihrer Rechtsform, als öffentliche Stelle.[113] Demnach können zum Beispiel Eigenbetriebe von Kommunen, die als GmbH geführt werden, als öffentliche Stelle betrachtet werden. Als Grundvoraussetzung ist jedoch zu beachten, dass der öffentlich-rechtliche Träger die Mehrheit des wirtschaftlichen Unternehmens inne hat,[114] das Unternehmen "als öffentlich-rechtliches Wirtschaftsunternehmen tätig ist"[115] und es Aufgaben der öffentlichen Verwaltung wahrnimmt.[116] Somit gelten nach dem BDSG, alle wirtschaftlichen Unternehmen, die von öffentlichen Trägern betrieben werden, als öffentliche Stelle im deutschen Datenschutzrecht. Als Ausnahme gelten private Unternehmen, die keine öffentlichen Aufgaben wahrnehmen, aber ein öffentlich-rechtlicher Verwaltungsträger Anteile dieses Unternehmens besitzt. Solange der Verwaltungsträger nicht die Mehrheit besitzt, zählt das Unternehmen nicht als öffentliche Stelle im Sinne des BDSG. So genannte "Beliehene Personen" (z.B. der TÜV) gehören auch zur Gruppe der öffentlichen Stellen, da sie hoheitliche Aufgaben der öffentlichen Verwaltung wahrnehmen und ihre Maßnahmen nach außen gerichtet sind.[117]

[111] Vgl. *Weichert,* in: Däubler/Klebe/u.a., 2016, § 2 BDSG Rn. 4.
[112] Vgl. *Kopp/Ramsauer,* 2013, § 1 VwVfG Rn. 16d.
[113] Vgl. *Weichert,* in: Däubler/Klebe/u.a., 2016, § 2 BDSG Rn. 4.
[114] Vgl. *Weichert,* in: Däubler/Klebe/u.a., 2016, § 2 BDSG Rn. 13.
[115] Vgl. *Hanloser,* in: Wolff/Brink/u.a., 2013, § 2 BDSG Rn. 42.
[116] Vgl. *Körffer/Klug/Gola/u.a.,* 2010, § 2 BDSG Rn. 5a.
[117] Vgl. *Weichert,* in: Däubler/Klebe/u.a., 2016, § 2 BDSG Rn. 7.

Da der Datenschutz nach Art. 2 Abs. 3 EU-DSGVO, für die Behörden der Europäischen Union, durch die Verordnung (EG) Nr. 45/2001 geregelt wird, ist es nicht notwendig den europarechtlichen Behördenbegriff zu erläutern.

Durch die Öffnungsklausel können die nationalen Gesetzgeber nur die Bußgeldvorschriften des Art. 83 EU-DSGVO, für den öffentlichen Bereich, bestimmen. Die restlichen Abhilfebefugnisse des Art. 58 Abs.2 EU-DSGVO gelten laut Art. 83 Abs. 7 EU-DSGVO weiterhin in vollen Umfang für die öffentliche Verwaltung. In der Vorschrift des Art. 83 Abs. 7 EU-DSGVO wurde den Mitgliedstaaten sogar freie Hand darüber gelassen, ob überhaupt gegen den öffentlichen Bereich Bußgelder erlassen werden sollen und falls ja, in welchem Umfang. Durch diese Formulierung können die Mitgliedstaaten selbständige nationale Gesetze schaffen, die für die öffentliche Verwaltung gelten. Doch es ist fraglich, wie weit der Ermessenspielraum der Mitgliedstaaten bei der nationalen Gesetzgebung geht. Zu beachten ist, dass die nationalen Bußgeldvorschriften für den öffentlichen Bereich nicht einfach aus der Verordnung wiederholt werden dürfen. Hierzu hat der EuGH klargestellt, dass die Wiederholung von Verordnungstexten nicht mit dem Europarecht vereinbar ist.[118] Der Erwägungsgrund Nr. 8 zur EU-DSGVO eröffnet aber die Möglichkeit, dass Teile der Verordnung in das Recht der Mitgliedstaaten übernommen werden können, um präzisere Bestimmungen erlassen zu können.[119] Somit können zwar Teile der Datenschutzgrundverordnung in ein nationales Gesetz übernommen werden, es muss aber darauf geachtet werden, dass ersichtlich ist, dass die nationale Regelung aus der Datenschutzgrundverordnung hervorgeht und diese trotzdem das primär anzuwendende Recht ist.

Sollte ein Mitgliedstaat sich entscheiden, dass in seinem Hoheitsgebiet keine Bußgelder verhängt werden sollen, können die Aufsichtsbehörden gem. Art. 83 Abs. 9 EU-DSGVO eine gerichtliche Bußgeldfestsetzung einleiten. Der EU-Gesetzgeber geht nicht weiter darauf ein, ob der Absatz für

[118] Vgl. *Benecke/Wagner*, in: DVBl 10/2016, 606 (604-605).
[119] Vgl. Erwägungsgrund Nr. 8 zur EU-DSGVO.

private oder öffentliche Stellen gilt. Die nationalen Gerichte sollten sich bei der Verhängung an den Vorschlag der zuständigen Aufsichtsbehörde richten.[120] Voraussetzung hierfür ist jedoch, dass der nationale Gesetzgeber eine Rechtsvorschrift für die gerichtliche Bußgeldfestsetzung erlässt.

c) Art. 83 Abs. 7 „Lex specialis“ zu Art. 58 Abs. 2 EU-DSGVO?

Ein Problem, dass sich bei der Bearbeitung erschließen könnte, ist die Möglichkeit, dass die Öffnungsklausel für den öffentlichen Bereich eine spezialgesetzliche Vorschrift sein könnte zu Art. 58 Abs. 2 lit. i EU-DSGVO.

Die Öffnungsklausel könnte in Anbetracht der Umstände eine speziellere Bußgeldvorschrift sein, da sie die Geldbußen für die öffentliche Verwaltung regelt. Sollte dies der Fall sein, wären die Vorschriften des Art. 58 Abs. 2 lit. i und Art. 83 EU-DSGVO als allgemeinere Regelung nicht anzuwenden. Es müssten somit nationale Vorschriften für den öffentlichen Bereich erlassen werden.

Gegen diese Ansicht spricht jedoch, dass der Art. 83 Abs. 7 EU-DSGVO keine Ermächtigungsgrundlage für die Bußgeldverhängung darstellt. Der Art. 83 hat seinen Ursprung in Art. 58 Abs. 2 lit. i EU-DSGVO, der für die weitere Prüfung auf Art. 83 verweist. Die grundlegende Ermächtigungsgrundlage für die Verhängung von Bußgeldern ist demnach der Art. 58 Abs. 2 lit. i EU-DSGVO. Art. 83 EU-DSGVO beinhaltet die Bedingungen, wann und in welcher Höhe Bußgelder erlassen werden können. Der Art. 83 Abs. 7 EU-DSGVO dient den Mitgliedstaaten als Ausgestaltungsmöglichkeit, den öffentlichen Bereich anderweitig zu regeln.

IV. Weitere Sanktionsmöglichkeiten

In der EU-DSGVO gibt es neben den Abhilfebefugnissen und Bußgeldern noch weitere Möglichkeiten, um die Verantwortlichen für ihre rechtswidrigen Handlungen zu bestrafen. In Art. 84 EU-DSGVO können die Mitgliedstaaten weitere Sanktionen und Strafen einführen. Hierbei ist es den nati-

[120] Vgl. Erwägungsgrund Nr. 151 zur EU-DSGVO.

onalen Gesetzgebern freigestellt, ob es sich bei den Sanktionen um verwaltungsrechtliche Maßnahmen handelt oder um Straftatbestände.[121] Durch diese Öffnungsklausel könnten in Deutschland die Straftatbestände des BDSG, der LDSG's und der §§ 201 ff StGB (Strafgesetzbuch) beibehalten werden. Diese Straftatbestände richten sich gegen Verantwortliche sowohl des privaten als auch des öffentlichen Bereichs. Die deutsche Gesetzgebung könnte sich in diesem Zusammenhang weitere Verwaltungsstrafen in die Wege leiten,[122] um den Druck auf die öffentliche Verwaltung zu erhöhen.

Neu hinzugekommen sind auch die Vorschriften über einen Schadensersatzanspruch gem. Art. 82 EU-DSGVO. Hierdurch haben betroffene Personen das Recht, gegen Behörden und Unternehmen einen Schadensersatz gelten zu machen, sofern ein Schaden durch eine rechtswidrige Datenverarbeitung entstanden ist.[123] Diese Regelung gilt ebenso für die öffentliche Verwaltung.

[121] Vgl. Erwägungsgrund Nr. 152 zur EU-DSGVO.
[122] Vgl. *Voßhoff,* BfDI - Info 6, 2016, 33. (Siehe Anlage 10).
[123] Art. 82 Abs. 1 EU-DSGVO.

D. Umsetzung der EU-DSGVO in Deutschland

In dem letzten Teil der Arbeit sollen die Möglichkeiten erläutert werden, inwiefern der deutsche Gesetzgeber die Strukturen, Aufgaben und Befugnisse der Aufsichtsbehörden in Deutschland umsetzen könnte.

I. Gesetzgebungskompetenz

In Deutschland ist der Datenschutz in Bundes- und Landesgesetze geregelt. Die allgemeinen Datenschutzgesetze der Länder sind die Landesdatenschutzgesetze (LDSG) und auf Bundesebene das Bundesdatenschutzgesetz (BDSG). Das BDSG regelt den öffentlichen Bereich auf Bundesebene und den nicht-öffentlichen Bereich. In den LDSG's befinden sich die Vorschriften für den öffentlichen Bereich auf Länder- und kommunaler Ebene.

Da es keine ausdrückliche Gesetzgebungskompetenz über den Datenschutz in den Artikeln 70 ff GG gibt, haben grundsätzlich die Länder das Recht die Datenschutzregelungen zu erlassen. Der Datenschutz wird tatsächlich sowohl von Bund und Ländern geregelt, weil es sich hierbei um eine ungeschriebene Zuständigkeitsregel handelt, die Annexkompetenz. Da das Datenschutzrecht in Gesetzes- und Lebensbereiche von Bund und Ländern hineinwirkt, handelt es sich um eine "Querschnittsmaterie".[124] Somit können Bund und Länder eigene Datenschutzvorschriften zu den verschiedenen Rechtsbereichen erlassen.

Für die Umstellung auf das neue europäische Datenschutzrecht müssen die Landesregierungen und der Bundesgesetzgeber alle Gesetze überprüfen, in denen Datenschutzregelungen enthalten sind.[125] Politisch müssen sich alle darauf verständigen, wie die Öffnungsklauseln der Datenschutzgrundverordnung in nationales Recht umgesetzt werden[126] und auf welcher Ebene die Rechtsakte stattfinden sollen. Durch die Öffnungsklausel des Art. 6 Abs. 2 und 3 EU-DSGVO, können spezifischere Regelungen für

[124] Vgl. *Weichert,* in: Däubler/Klebe/u.a., 2016, BDSG, S. 100 Rn. 59.
[125] Vgl. *Voßhoff,* BfDI - Info 6, 2016, 33. (Siehe Anlage 10).
[126] Ebenda.

den öffentlichen Bereich erlassen werden. Sofern Datenschutzvorschriften schon den Vorschriften der EU-DSGVO genügen, können diese beibehalten werden.[127]

II. Organisation der Aufsichtsbehörden

Ein wichtiger Punkt, über den sich die Politik klar werden muss, ist die organisatorische Umsetzung der zukünftigen Aufsichtsbehörden in Deutschland. Laut Art. 54 Abs.1 lit. a EU-DSGVO ist es den Mitgliedstaaten überlassen, ihre Aufsichtsbehörden zu gestalten. Momentan gibt es in Deutschland auf Bundesebene und in jedem Bundesland eine Datenschutzbehörde, die den Datenschutz im öffentlichen und nicht-öffentlichen Bereich überwacht. In Bayern gibt es jeweils für den öffentlichen und nicht-öffentlichen Bereich eine Aufsichtsbehörde. Durch die neuen Aufgaben und Befugnisse in der EU-DSGVO, müssen die aktuellen Datenschutzbehörden erweitert und umorganisiert werden. Im Folgenden werden zwei denkbare Ansätze vorgestellt, wie die Aufsichtsbehörden in Zukunft aussehen könnten.

1. Zentrale Aufsichtsbehörde

Eine Möglichkeit für eine Neugestaltung der Datenschutzaufsicht, wäre es, eine zentrale Aufsichtsbehörde auf Bundesebene zu schaffen (wie aktuell die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit) und in dieser Behörde, die gesamten Kompetenzen und Befugnisse der EU-DSGVO zu konzentrieren. Die derzeitigen Datenschutzbehörden in den Bundesländern müssten in diesem Modell nicht zwingend abgeschafft werden. Diese können als dezentrale Zweigstellen für Bürger, Behörden und Unternehmen weiter bestehen. Die organisatorische Zugehörigkeit ist bei einer Aufgabenumverteilung zwingend erforderlich, da in den Artikeln 57 Abs. 1 und Art. 58 Abs. 1 EU-DSGVO geregelt ist, dass alle Aufsichtsbehörden über sämtliche Aufgaben und Befugnisse der EU-DSGVO ver-

[127] Vgl. Erwägungsgrund Nr. 10 zur EU-DSGVO.

fügen müssen.[128] Die Aufgaben und Befugnisse, nach der EU-DSGVO, könnten aber verwaltungsintern umverteilt werden. Den Zweigstellen, die organisatorisch der zentralen Aufsichtsbehörde angehören müssen, können Beratungen und Sensibilisierungsmaßnahmen vornehmen und als örtliche Behörde Beschwerden von betroffenen Personen entgegennehmen. Damit auch eine effektive Kontrolle gewährleistet werden kann, sollten die Zweigstellen ebenso Untersuchungsbefugnisse gem. Art. 58 Abs. 1 EU-DSGVO übertragen bekommen, um die Kolleginnen und Kollegen der zentralen Stelle bei ihrer Arbeit zu unterstützen. Die zentrale Aufsichtsbehörde kann die Zuständigkeit über die Abhilfe- und Sanktionsbefugnisse wahrnehmen. Auf diese Weise könnte dem Problemfeld der Rollenvielfalt der Aufsichtsbehörden abgeholfen werden. Durch die vielen verschiedenen Rollen, die die Aufsichtsbehörden inne haben, entstehen bei der Aufgabenerledigung Zielkonflikte.[129] In Deutschland haben die Datenschutzbehörden die Aufgabe die Verantwortlichen zu beraten und sie gleichzeitig zu kontrollieren bzw. im Falle eines Unternehmens zu sanktionieren.[130] Da der Aufgabenkatalog nach Art. 57 EU-DSGVO den Aufsichtsbehörden ebenso diese verschiedenen Rollen übertragt, kann dies negative Auswirkungen auf die Durchsetzung der EU-DSGVO haben.[131]

Für die Umgestaltung müssten viele organisatorische und personelle Maßnahmen getroffen, sowie nationale Regelungen erlassen werden. Da in den letzten Jahren das Personal in den Aufsichtsbehörden der Länder abgenommen hat,[132] könnte somit, durch die Aufgabenumlegung auf Bundesebene, diesem negativen Effekt entgegen gekommen werden. Innerhalb der zentralen Aufsichtsbehörde können verschieden Fachbereiche zu den jeweiligen Sanktionsmaßnahmen gebildet werden. Somit können sich mehrere Mitarbeiter auf eine spezielle Maßnahme konzentrieren. Außerdem ist es zu empfehlen, dass die Überwachung des öffentlichen und pri-

[128] Vgl. EU-Datenschutz-Grundverordnung, Gesetzestext mit eingereihten Erwägungsgründen, 2016, 161.
[129] Vgl. *Schulzki-Haddouti*, in: c't 10/2016, 162 (164).
[130] Ebenda, 162.
[131] Ebenda, 164.
[132] Vgl. *Schulzki-Haddouti*, in: c't 12/2015, 66.

vaten Bereichs separat vorgenommen wird. Falls ein Sachgebiet mit einigen Sachbearbeitern zu viele Verantwortliche kontrollieren muss, kann es schnell zu einer Überlastung der Mitarbeiter führen. Um diesem Zustand entgegenzuwirken und um eine sachgemäße Umsetzung der EU-DSGVO sicherzustellen, ist es dringend zu empfehlen, die umfangreiche Aufgaben auf genügend verschiedene Abteilungen und Sachgebiete aufzuteilen. Hier ist der nationale Gesetzgeber gefordert, genügend Stellen für die Aufsichtsbehörden zu schaffen und ausreichend finanzielle Ressourcen zur Verfügung zu stellen.

Das Prinzip der "zentralen Aufsichtsbehörde", kann mit der Deutschen Bundesbank und den verschiedenen Standorten in den Bundesländern verglichen werden. Die Zentrale mit Sitz in Frankfurt am Main übernimmt organisatorische und strategische Aufgaben. Die verschiedenen Hauptverwaltungen in den Bundesländern sind die örtlichen Ansprechpartner für die Banken, Bürger und die Politik. Desweiteren überwachen die Hauptverwaltungen und Filialen die Banken vor Ort und stellen die Bargeldversorgung sicher.[133] Auf dieses Weise werden die Aufgaben auf mehrere Zweigestellen verteilt um eine örtliche Betreuung sicherzustellen.

2. Mehrere Aufsichtsbehörden

Eine weitere Möglichkeit für Deutschland ist es, die aktuellen Datenschutzbehörden in den Bundesländern beizubehalten und sie mit allen Kompetenzen nach der EU-DSGVO auszustatten. Durch diesen Aufbau wäre in jedem Bundesland eine Aufsichtsbehörde mit allen Befugnissen vertreten und sie könnten somit flächendeckend die EU-DSGVO überwachen und durchsetzen. Wie bei dem organisatorischen Aufbau einer zentralen Aufsichtsbehörde in Punkt D. II. 1. ist zu empfehlen, dass den verschiedenen Aufsichtsbehörden genügend personelle und finanzielle Ressourcen von den Landesregierungen zu Verfügung gestellt bekommen

[133] Vgl. *Deutsche Bundesbank,* https://www.bundesbank.de/Redaktion/DE/Themen/2015/2015_08_27_bundesbank_vor_ort.html?view=render%5BDruckversion%5D, zuletzt geprüft am 01.09.2016. (Siehe Anlage 12).

und dass die vielfältigen Aufgaben der EU-DSGVO auf genügend Fachbereiche verteilt werden. Auf diese Weise können die aktuellen Datenschutzbehörden vollständig beibehalten werden und müssten nur im Sinne der Datenschutzgrundverordnung erweitert werden. Gem. Art. 51 Abs. 3 EU-DSGVO kann ein Mitgliedstaat über mehrere Aufsichtsbehörden verfügen. Für die Bundesrepublik wäre dieser Aufbau sogar passend, da die EU-DSGVO auf die verschiedenen nationalen Strukturen Rücksicht nimmt.[134] Der Mitgliedstaat müsste daraufhin veranlassen, dass alle nationalen Aufsichtsbehörden am Kohärenzverfahren teilnehmen können und dass eine bestimmte Aufsichtsbehörde im Europäischen Datenschutzausschuss vertreten ist.[135] Aktuell ist noch nicht klar, wer in im Europäischen Datenschutzausschuss vertreten sein wird; die CDU plädiert zur Bundesbeauftragten für den Datenschutz und Informationsfreiheit.[136]

Durch diese Struktur könnten sich jedoch Zuständigkeitsprobleme zwischen den Aufsichtsbehörden ergeben. Gem. Art. 55 Abs. 1 EU-DSGVO ist jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaates zuständig. Sollte sich eine betroffene Person über eine regelwidrige Verarbeitung seiner personenbezogenen Daten eines Verantwortlichen, mit der Hauptniederlassung in Baden-Württemberg, bei der Aufsichtsbehörde in Bayern beschweren, so ist fraglich, ob nun die Aufsichtsbehörde in Baden-Württemberg oder Bayern zuständig ist. Nach einem Gerichtsurteil des Verwaltungsgerichts Hannover richtet sich die Zuständigkeit der Aufsichtsbehörde nach dem Ort der Verarbeitung und nicht nach der Hauptniederlassung des Verantwortlichen.[137] "Da es in der EU-DSGVO keine Zuständigkeitsregelungen für die Aufsichtsbehörden innerhalb der Mitgliedstaaten gibt, kommen die nationalen Regelungen, in Deutschland vor allem das VwVfG, zur Anwendung.".[138]

[134] Vgl. Erwägungsgrund Nr. 117 zur EU-DSGVO.
[135] Art. 51 Abs. 3 EU-DSGVO.
[136] Vgl. *Schulzki-Haddouti*, in: c't 3/2016, 86 (88).
[137] Vgl. VG Hannover Urteil vom 06.11.2012 Az. 10 A 4805/11 (unveröffentlicht); *Kranig*, in: ZD 11/2013,550 (551).
[138] Vgl. *Kranig*, in: ZD 11/2013, 550 (551).

E. Fazit

Die Datenschutzgrundverordnung, mit ihren neuen Regelungen und Möglichkeiten, birgt große Herausforderungen an die Verantwortlichen für die Datenverarbeitung und die Mitgliedstaaten. Ob durch die Reform das Datenschutzniveau in der EU erhöht werden kann ist weiterhin fraglich. Die EU-DSGVO bietet aber viele Möglichkeiten für die Aufsichtsbehörden und Mitgliedstaaten, das bestmögliche daraus zu machen. Letzten Endes kommt es einerseits auf die Mitgliedstaaten an, ob sie die Ausgestaltungsmöglichkeiten nutzen und die Aufsichtsbehörden mit den erforderlichen Mitteln ausstatten und andererseits auf die Aufsichtsbehörden, ob sie die Regelungen der EU-DSGVO konsequent durchsetzen und inwieweit sie ihre neuen Befugnisse zum Einsatz bringen.

Es würde auf jeden Fall durch die Sanktionierungsmöglichkeiten des öffentlichen Dienstes ein wichtiges Zeichen für den Datenschutz gesetzt, so dass er in allen Bereichen gleichwertig anzusehen ist. Dass die neuen Abhilfebefugnisse auch gegen die öffentliche Verwaltung angewandt werden können, ist eine deutliche Verbesserung gegenüber dem alten Datenschutzrecht. Die Frage auf die Anwendbarkeit der Bußgeldvorschriften konnte in dieser Arbeit nicht eindeutig geklärt werden. Es wäre jedoch zu begrüßen, wenn die Bundesregierung die Öffnungsklausel des Art. 83 Abs. 7 EU-DSGVO nutzt und die öffentliche Verwaltung ebenso zum Adressat der Bußgeldvorschriften bestimmt, damit das Grundrecht auf informationelle Selbstbestimmung nach dem Grundgesetz und dem Grundrecht auf Datenschutz nach der europäischen Charta der Menschenrechte auch für betroffene Personen von Behörden geschützt wird.

Literaturverzeichnis

Albrecht, Jan Phillip, Die Datenschutzreform der Europäischen Union, in: Jan Phillip Albrecht (Hrsg.), 2015.

Ashkar, Daniel, Durchsetzung und Sanktionierung des Datenschutzrechts nach den Entwürfen der Datenschutz-Grundverordnung, in: DuD 12/2015, S. 796–800.

Benecke, Alexander/Wagner, Julian, Öffnungsklauseln in der Datenschutz-Grundverordnung und das deutsche BDSG - Grenzen und Gestaltungsspielräume für ein nationales Datenschutzrecht, in: DVBl 10/2016, S. 600–608.

Caspar, Johannes, Das aufsichtsbehördliche Verfahren nach der EU-Datenschutz-Grundverordnung, Defizite und Alternativregelungen, in: ZD 12/2012, S. 555–558.

Caspar, Johannes, 25. Tätigkeitsbericht Datenschutz des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit 2014 / 2015, in: Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit (Hrsg.), 2015.

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/u.a.: Bundesdatenschutzgesetz Kompaktkommentar zum BDSG, 5., vollständig neu bearbeitete Auflage, 2016.

Deutsche Bundesbank, Deutsche Bundesbank - Themen - Bundesbank: Ein wichtiger Partner vor Ort, Online verfügbar unter https://www.bundesbank.de/Redaktion/DE/Themen/2015/2015_08_27_bundesbank_vor_ort.html?view=render%5BDruckversion%5D, zuletzt geprüft am 01.09.2016.

Ehmann, Eugen, Bußgelder, behördliche Anordnungen, Verbandsklagen - wie lässt sich Datenschutz am besten durchsetzen?, in: ZD 10/2014, S. 493–494.

Forgó, Nikolaus, Und täglich grüßt die Datenschutzgrundverordnung…, in: ZD 2/2014, S. 57–58.

Hansen-Oest, Stephan/Heidrich, Joerg, Neu verordnet, Welche Änderungen die neue EU-Datenschutz-Regulierung in Deutschland bringen wird, in: c't 9/2016, S. 166–169.

Jarass, Hans D./Pieroth, Bodo, Grundgesetz für die Bundesrepublik Deutschland Kommentar, 14. Auflage, 2016.

Klingbeil, Jörg, 32. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Baden-Württemberg 2014/2015, in: Landesbeauftragten für den Datenschutz Baden-Württemberg (Hrsg.), 2016.

Kopp, Ferdinand O./Ramsauer, Ulrich, Verwaltungsverfahrensgesetz Kommentar, 14., vollst. überarb. Aufl., 2013.

Körffer, Barbara/Klug, Christoph/Gola, Peter/u.a., Bundesdatenschutzgesetz BDSG; Kommentar, 10., überarb. und erg. Aufl., 2010.

Kranig, Thomas, Zuständigkeit der Datenschutzaufsichtsbehörden, Feststellung des Status quo mit Ausblick auf die DS-GVO, in: ZD 11/2013, S. 550–557.

Lenz, Carl-Otto/Borchardt, Klaus-Dieter/Bitterlich, Joachim: EU-Verträge Kommentar EUV - AEUV - GRCh, 6. Aufl., Rechtsstand: 1. September 2012, 2013.

EU-Datenschutz-Grundverordnung, Gesetzestext mit eingereihten Erwägungsgründen, in: Linder, Andreas (Hrsg.), 1. Auflage, 2016.

Ronellenfitsch, Michael, Dreiundvierzigster Tätigkeitsbericht, in: Hessischer Datenschutzbeauftragter (Hrsg.), 2014.

Schaar, Peter, EU-Datenschutz: Schluss mit der Verzögerungstaktik!, in: ZD 3/2014, S. 113–114.

Schulzki-Haddouti, Christiane, Protected in Germany, Deutsche Datenschutz-Vorgaben sind schlechter als ihr Ruf, in: c't 12/2015, S. 66.

Schulzki-Haddouti, Christiane, Außer Kontrolle, Fragwürdiger Datenschutz in Polizeisystemen, in: c't 13/2016, S. 154–157.

Schulzki-Haddouti, Christiane, Datenschutz europaweit, Was sich mit der EU-Grundverordnung ändern wird, in: c't 3/2016, S. 86–88.

Schulzki-Haddouti, Christiane, Papiertiger, Kaum Strafen für Verstöße gegen Datenschutzvorschriften, in: c't 10/2016, S. 162–164.

Smoltczyk, Maja, Datenschutz und Informationsfreiheit Bericht 2015 Berlin, in: Berliner Beauftragte für Datenschutz und Informationsfreiheit (Hrsg.), 2016.

Spindler, Gerald, Die neue EU-Datenschutz-Grundverordnung, in: DER BETRIEB 16/2016, S. 937–947.

Voßhoff, Andrea, 25. Tätigkeitsbericht zum Datenschutz für die Jahre 2013 und 2014, in: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Hrsg.), 2015.

Voßhoff, Andrea, BfDI - Info 6 EU-Datenschutzgrundverordnung, in: Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (Hrsg.), 2016.

Wolff, Heinrich Amadeus/Brink, Stefan/Albers, Marion: Datenschutzrecht in Bund und Ländern Grundlagen Bereichsspezifischer Datenschutz BDSG Kommentar, 2013.

Wybitul, Tim, Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte? Anpassungsbedarf bei Beschäftigtendatenschutz und Betreibsvereinbarungen, in: ZD 5/2016, S. 203–208.

Eidesstattliche Erklärung

„Ich versichere, dass ich diese Bachelorarbeit selbständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe. Die aus anderen Quellen direkt oder indirekt übernommenen Daten und Konzepte sind unter Angabe der Quelle gekennzeichnet.

Es ist mir bekannt, dass die Arbeit mit einer Plagiaterkennungssoftware auf nicht gekennzeichnete Übernahme fremden geistigen Eigentums überprüft werden kann.“

Datum, Unterschrift