WWU
MÜNSTER

Grundlagen und Grenzen der Risikoanalyse zum Zwecke der allgemeinen Gefahrenabwehr innerhalb der postalischen Lieferkette

Zbigniew Adam Strzoda

Grundlagen und Grenzen der Risikoanalyse zum Zwecke der allgemeinen Gefahrenabwehr innerhalb der postalischen Lieferkette

Inaugural-Dissertation
zur Erlangung des akademischen Grades
eines Doktors der Rechte durch die Rechtswissenschaftliche
Fakultät der Westfälischen Wilhelms-Universität zu Münster

Vorgelegt von

Zbigniew Adam Strzoda

Erster Berichterstatter: Prof. Dr. Wolffgang

Zweiter Berichterstatter: Prof. Dr. Holznagel, LL.M.

Dekan/in: Prof. Dr. Boers

Tag der mündlichen Prüfung: 10.04.2018

D 6

Zugl.: Münster (Westf.), Univ., Diss. Der Rechtswissenschaftlichen Fakultät 2018

Zbigniew Adam Strzoda

Grundlagen und Grenzen der Risikoanalyse zum Zwecke der allgemeinen Gefahrenabwehr innerhalb der postalischen Lieferkette

Wissenschaftliche Schriften der WWU Münster

Reihe III

Band 34

Zbigniew Adam Strzoda

Grundlagen und Grenzen der Risikoanalyse zum Zwecke der allgemeinen Gefahrenabwehr innerhalb der postalischen Lieferkette

Wissenschaftliche Schriften der WWU Münster
herausgegeben von der Universitäts- und Landesbibliothek Münster
http://www.ulb.uni-muenster.de

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Dieses Buch steht gleichzeitig in einer elektronischen Version über den Publikations- und Archivierungsserver der WWU Münster zur Verfügung.
http://www.ulb.uni-muenster.de/wissenschaftliche-schriften

Zbigniew Adam Strzoda
„Grundlagen und Grenzen der Risikoanalyse zum Zwecke der allgemeinen Gefahrenabwehr innerhalb der postalischen Lieferkette“
Wissenschaftliche Schriften der WWU Münster, Reihe III, Band 34
Verlag readbox publishing GmbH – readbox unipress, Münster
http://unipress.readbox.net

Zugl.: Diss. Universität Münster, 2018

ISBN 978-3-8405- 0191-3 (Druckausgabe)
URN urn:nbn:de:hbz:6-06199378909 (elektronische Version) direkt zur Online-Version:

Satz: Pamela Kröhl
Umschlag: ULB Münster

VORWORT

Die vorliegende Arbeit wurde im Wintersemester 2016/17 von der Rechtswissenschafltichen Fakultät der Westfälischen Wilhelms-Universität Münster als Dissertation angenommen.

Mein besonderer Dank gilt meinem Doktorvater Herrn Professor Dr. Hans-Michael Wolffgang für die Unterstützung, die Förderung und die langjährige Zusammenarbeit, nicht nur im Rahmen dieser Promotion, sondern auch während meiner Tätigkeit in der Abteilung für Zölle und Verbrauchsteuern an der Universität Münster. Ebenfalls danken möchte ich Herrn Professor Dr. Bernd Holznagel, LL.M. für die Erstellung des Zweitgutachtens.

Meinen Eltern danke ich für ihre uneingeschränkte Unterstützung während des Studiums und der Promotion. Ohne ihren Rückhalt wäre das Erstellen dieser Arbeit nicht möglich gewesen.

Münster, im Mai 2018

Zbigniew Adam Strzoda

INHALT

ABKÜRZUNGSVERZEICHNIS

ABl.	Amtsblatt
Abs.	Absatz
AEO	Authorized Economic Operator (WCO)/Authorised Economic Operator (EU)
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AfP	Archiv für Presserecht
AG	Aktiengesellschaft
AöR	Archiv für öffentliches Recht (Zeitschrift)
Art.	Artikel
ATLAS	Automatisiertes Tarif- und Lokales Zollabwicklungssystem
Aufl.	Auflage
AW-Prax	Außenwirtschaftliche Praxis (Zeitschrift)
Az.	Aktenzeichen
BB	Betriebs-Berater (Zeitschrift)
Bd.	Band
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
BVerfG	Bundesverfassungsgericht
BVerfGE	Sammlung der Entscheidungen des Bundesverfassungsgerichts
BVerwG	Bundesverwaltungsgericht
BVerwGE	Sammlung der Entscheidungen des Bundesverwaltungsgerichts
bzw.	beziehungsweise
CT	Computer und Recht (Zeitschrift)
DatenschutzVO	Datenschutz-Grundverordnung
d. h.	das heißt
Diss.	Dissertation

DIN	Deutsches Institut für Normierung
DÖV	Die öffentliche Verwaltung (Zeitschrift)
DPAG	Deutsche Post Aktiengesellschaft
DuD	Datenschutz und Datensicherung (Zeitschrift)
DVBL	Deutsches Verwaltungsblatt (Zeitschrift)
DVO	Durchführungsverordnung
DVR	Datenverarbeitung im Recht (Zeitschrift)
E-Government	Electronic Government
EDI	Electronic Data Interchange
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft(en)
EGMR	Europäischer Gerichtshof für Menschenrechte
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
EMRK	Europäische Menschenrechtskonvention
endg.	endgültig
EORI	Economic Operators Registration and Identification
EU	Europäische Union
EuG	Europäisches Gericht
EuGH	Europäischer Gerichtshof
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht
EWG	Europäische Wirtschaftsgemeinschaft
f./ff.	folgende(r)
Fn.	Fußnote
Gem.	gemäß
GG	Grundgesetz
GrCh	Charta der Grundrechte der Europäischen Uniony
Hrsg.	Herausgeber
Hs.	Halbsatz
ISO	International Organization for Standardization

i. V. m.	in Verbindung mit
JA	Juristische Arbeitsblätter (Zeitschrift)
JR	Juristische Rundschau (Zeitschrift)
JURA	Juristische Ausbildung (Zeitschrift)
JuS	Juristische Schulung (Zeitschrift)
JZ	Juristenzeitung (Zeitschrift)
KOM	Dokumente der Kommission der Europäischen Gemeinschaften
MZK	Modernisierter Zollkodex
MZK-DVO	Verordnung mit Durchführungsvorschriften zum Modernisierten Zollkodex
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OECD	Organisation for Economic Co-operation and Development
OVG	Oberverwaltungsgericht
PDLV	Postdienstleistungsverordnung
PDSV	Postdienste-Datenschutzverordnung
PostG	PostGesetz
PTNeuOG	Postneuordnungsgesetz
PUDLV	Postuniversaldienstleistungsverordnung
RDV	Recht der Datenverarbeitung (Zeitschrift)
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
S.	Seite(n), Satz
Slg.	Sammlung
TAXUD	Generaldirektion Steuern und Zollunion (Europäische Kommission)
UN	United Nationsswiatowe dni mlodziezy
UZK	Zollkodex der Europäischen Union, kurz: Unionszollkodex
VerwArch	Verwaltungsarchiv (Zeitschrift)

VGH	Verwaltungsgerichtshof
vgl.	vergleiche
VO	Verordnung
Vol.	Volume
VR	Verwaltungsrunschau
VwGO	Verwaltungsgerichtsordnung
z. B.	zum Beispiel
ZfZ	Zeitschrift für Zölle und Verbrauchssteuern
ZHR	Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht
ZK	Zollkodex der Europäischen Gemeinschaften
ZK-EU	Zollkodex der EU
ZK-DVO	Verordnung mit Durchführungsvorschriften zum Zollkodex der Europäischen Gemeinschaften
ZollVG	Zollverwaltungsgesetz
ZORA	Zentralstelle Risikoanalyse
ZRP	Zeitschrift für Rechtspolitik

1. Teil |
Einleitung und Problemaufriss

A. Einleitung

Angesichts terroristischer Bedrohungen ist der offene Lebensstil freiheitlich demokratischer Gesellschaften zunehmenden Sicherheitsrisiken ausgesetzt. Jeder Terrorangriff und damit verbundene Opfer – seien es finanzielle Schäden oder gar Verletzte und Getötete – lassen den Ruf nach mehr Sicherheit lauter werden. Jede neue Sicherheitsmaßnahme bringt jedoch auch in der Regel mehr Kontrolle und Einschränkungen von Freiheitsrechten mit sich. Um das Merkmal einer offenen Gesellschaft zu wahren, bedarf es einer Austarierung von Freiheit und Sicherheit.

Lebensader unserer modernen Industrie- und Informationsgesellschaft ist der Fluss von Waren und Informationen rund um den Globus. An dieser Stelle ist die Gesellschaft besonders verwundbar und gleichzeitig auf Offenheit besonders angewiesen.

Die Verkehrs-, Transport- und Informationsinfrastruktur ist dabei ein neuralgischer Punkt und potenzielles Angriffsziel. Solchen Angriffen war – wenn auch bisher nur im Expressdienst – die postalische Lieferkette bereits ausgesetzt.

Fraglich erscheint daher, inwieweit unsere Kommunikations- und Transportsysteme auf diese neuen Gefahren vorbereitet sind. Ob das gegenwärtige Sicherheitsniveau ausreichend ist und inwieweit dieses unter Beibehaltung des gegenwärtigen Grundrechtsschutzes und Grundrechtsniveaus überhaupt weiter ausbaubar ist, ist zu untersuchen.

Die neu zu findenden technischen Lösungen müssen sich in einem juristischen Rahmen bewegen, den Anforderungen des geltenden Rechts standhalten und insbesondere die Grundrechte ausreichend beachten. Die rasante Entwicklung

der Informations- und Datenverarbeitungstechnologie führt zu ihrem vermehrten Einsatz im Sicherheitsbereich. Insbesondere die massenhafte Auswertung von Daten zur „lückenlosen“ Überwachung suggeriert zumindest Sicherheit. Die Auswertung von Informationen zwecks Risikoanalyse soll helfen, der Flut an Informationen Herr zu werden, und durch gezielte weitergehende Untersuchungen Sicherheit gewährleisten

Ob und inwieweit die betroffenen Rechtsgebiete darauf vorbereitet sind und wie Lösungen grundrechtskonform ausgestaltet werden können und müssen, soll Teil dieser Arbeit sein.

Wie viel ist das Recht auf informationelle Selbstbestimmung angesichts terroristischer Bedrohungen noch wert? Wie können datenschutzrechtliche Lösungen gefunden werden, die das Recht auf informationelle Selbstbestimmung schützen und gleichzeitig Sicherheit gewährleisten? Wie sehen technische und juristische Lösungen aus, die das Sicherheitsniveau steigern und gleichzeitig das Brief- und Postgeheimnis und den Schutz personenbezogener Daten achten?

Der Grundrechtsschutz steht hier vor neuen Herausforderungen auf die Rechtsprechung und Lehre versuchen müssen adäquate Antworten zu finden.

B. Problemaufriss und Eingrenzung des Themas

Die Sicherheit der postalischen Lieferkette ließe sich in so vielen unterschiedlichen Konstellationen prüfen und darstellen, dass sie den Rahmen dieser Arbeit übersteigen würde. Daher gilt es das Forschungsfeld einzugrenzen.

I. Beförderer

Seit der Liberalisierung des Postmarktes und dem Wegfall des Postmonopols ist eine Vielzahl von Postdiensteanbietern auf dem deutschen Markt für Postdienstleistungen aktiv. Diese unterscheiden sich jedoch in ihrer Größe und ihrem Dienstleistungsangebot erheblich. Daher soll die Deutsche Post AG (DPAG), als ehemaliger Monopolist größter Postdiensteanbieter und einziger Universaldienstleister in Deutschland, als Forschungsobjekt dienen.[1]

II. Beförderungsarten

Auf dem Markt für Postdienste ist zwischen verschiedenen Beförderungsarten bzw. Vertriebswegen zu unterscheiden. Die Kurier-, Express- und Paketdienste zeichnen sich in Abgrenzung zum Universaldienst durch einen Mehrwert in den erbrachten Dienstleistungen aus.[2] Der Universaldienst hingegen soll durch ein standardisiertes System möglichst kostengünstig und flächendeckend Postdienstleitungen sicherstellen. Damit nimmt der Universaldienst eine – auch unter legislatorischen Gesichtspunkten – besondere Stellung im Wirtschaftszweig der Postdienstleistungen ein. Diese Arbeit soll sich daher mit der Beförderung innerhalb des Universaldienstes beschäftigen.

---

1 Zu Universaldienstleistern siehe 2. Teil, B.,III, 1.), Der Begriff des Universaldienstes.

2 Erwägungsgrund 18, RL 97/67/EG.

III. Beförderungsgegenstand

Um das Forschungsfeld weiter einzugrenzen, soll der für die Sicherheitsarchitektur relevante Vorgang des Imports von Paketen aus dem „Nicht-EU-Ausland" exemplarisch betrachtet werden. Briefe und Päckchen auf diesem Vertriebsweg werden in die Betrachtung nicht mit einbezogen.

IV. Sicherheitsinstrument

Weiterhin gilt es ein zu untersuchendes Sicherheitsinstrument auszuwählen. Mit der Automatisierung und „EDVisierung" der postalischen Lieferkette rückt die Risikoanalyse als Instrument der Risikosteuerung in den Mittelpunkt der Sicherheitsarchitektur. Die Eingrenzung auf gefährdete bzw. risikoreiche Pakete erlaubt eine entsprechende Untersuchung dieser Pakete bei gleichzeitiger Beschleunigung und Straffung risikoarmer Warenflüsse. Damit wird dem Bedürfnis nach Sicherheit, wie auch nach Effizienz und Schnelligkeit der Lieferkette gleichermaßen gedient.

Die Möglichkeiten der Ausgestaltung dieser Risikoanalyse sollen daher im Mittelpunkt dieser Ausarbeitung stehen. Dabei ist neben der im Zollrecht vorgesehenen Risikoanalyse durch die Zollbehörden eine Beleihung der DPAG zu diesem Zweck genauso denkbar wie die Durchführung einer „weiteren" Risikoanalyse durch die DPAG.

C. Untersuchungsverlauf

Für diese Untersuchung gilt es zunächst die einschlägigen Rechtsgebiete des Zollrechts, des Postrechts und des Datenschutzrechts auf nationaler wie auch europäischer Ebene bezogen auf diese Problematik aufzuarbeiten. Die entsprechenden Rechtsgrundlagen sind auf relevante Rechtsvorschriften hin zu untersuchen und diese zu analysieren. Die in diesem Themengebiet notwendigen Rechtsbegriffe sind zu bestimmen und auf Übereinstimmung in den verschieden Rechtsebenen und Rechtsgebieten hin zu untersuchen. Ferner gilt es, den im Datenschutzrecht grundsätzlich gängigen Sicherheitsstandard für eine Datenverarbeitung zu erarbeiten.

Anhand der in Frage kommenden Szenarien, die sich aus den beteiligten Akteuren und den Datenverarbeitungsmöglichkeiten ergeben, gilt es die Möglichkeiten der Verwendung von Daten zu einer Risikoanalyse zwecks allgemeiner Gefahrenabwehr herauszuarbeiten.

Im Kern wird dabei die Frage nach den dafür benötigten Ermächtigungsgrundlagen zu beantworten sein und die dafür in Frage kommenden Tatbestände werden zu untersuchen sein. In die Untersuchung einzuschließen sind neben dem nationalen Recht eventuelle Vorgaben des internationalen und des unionalen Rechts.

Schließlich sind die potenziellen Ermächtigungsgrundlagen auf ihre Vereinbarkeit mit den grundrechtlichen Vorgaben hin zu analysieren. Dafür sind neben den Grundrechten nach dem Grundgesetz die Europäische Menschenrechtskonvention sowie die Europäische Grundrechtecharta heranzuziehen. Die Untersuchung des Grundrechtsschutzes setzt dabei eine Analyse der Rechtsebenen sowie ihrer Verhältnisse zueinander voraus. Darauf aufbauend sind die Grundrechtsgewährleistungen herauszuarbeiten und miteinander ins Verhältnis zu setzen, um den Schutz der Grundrechte und mögliche Eingriffe und Rechtfertigungen umfassend darzustellen.

D. Ziel der Untersuchung

Im Ergebnis soll diese Arbeit die Möglichkeiten und Grenzen der Datenverarbeitung der betroffenen Parteien zu Zwecken der Risikoanalyse zur Abwehr allgemeiner Gefahren darstellen. Dabei sollen nicht nur die Möglichkeiten des Status quo beschrieben werden, sondern auch weitere potenzielle Lösungen herausgearbeitet werden, die sich innerhalb des verfassungsrechtlichen Rahmens bewegen und durch legislatorische Veränderungen zu erreichen wären.

2. Teil |
Die betroffenen Rechtsgebiete

Zunächst gilt es die Rechtsgrundlagen in den betroffenen Rechtsgebieten des Datenschutzrechts, des Postrechts und des Zollrechts auf internationaler, europäischer und deutscher Rechtsebene freizulegen.

A. Datenschutz

„Die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, bedarf unter den Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe." (Bundesverfassungsgericht im Volkszählungsurteil)[3]

In einer informatisierten und digitalisierten Welt, die nicht mehr von Großrechnern, sondern von dezentraler Informationsverbreitung und -verarbeitung geprägt ist, nimmt der Datenschutz eine immer wichtigere Rolle ein. Von dessen Ausgestaltung hängt in zunehmendem Maße ein effektiver Grundrechtsschutz, insbesondere des allgemeinen Persönlichkeitsrechts und des Schutzes personenbezogener Daten ab. Die Interaktion in sozialen Netzwerken verlagert einen Teil des öffentlichen, wie auch des privaten Lebens ins Internet und lässt Rückschlüsse auf Persönlichkeitsprofile und Persönlichkeitsentwicklungen zu.

Die Wichtigkeit von Daten in einer Informationsgesellschaft führt nicht nur zu gesellschaftlicher, sondern auch zu wirtschaftlicher Relevanz. Von einem effektiven, aber auch umsetzbaren und wirtschaftlich darstellbaren Datenschutz hängt

[3] BVerfGE 65, S. 1, (41 ff.).

ein Teil der wirtschaftlichen Entwicklung ab. Das Vertrauen in den Schutz von Geschäftsgeheimnissen, Kundendaten, Patenten, Geschäftsmodellen etc. ist ein wichtiger Standortfaktor.

Die rasante technische Entwicklung führt dazu, dass der Gesetzgeber kaum mit ihr Schritt halten kann und die betreffenden Gesetze entsprechend offen formulieren muss, um zukünftige Entwicklungen mit einzubeziehen.

I. Historische Einführung

Der Datenschutz ist aus juristischer Perspektive ein relativ junger Rechtsbereich. Der erste Schutz von Daten ist wohl in der ärztlichen Verschwiegenheit von ca. 500 v. Chr. im Eid des Hippokrates und später im Seelsorge- und Beichtgeheimnis zu sehen, welches 1215 n. Chr. Einzug ins Kirchenrecht gefunden hat.[4]

An der Entwicklung des Datenschutzes lässt sich deutlich die Entwicklung von der Industrie- zur Informationsgesellschaft – mit der Verlagerung des regulatorischen Schwerpunktes von Betriebs- und Geschäftsgeheimnissen auf das Wirtschaftsgut „Information" selbst – ablesen.[5] Neben einem klassischen Schutz- und Abwehrcharakter gegenüber dem Staat tritt immer mehr die Regelung und Rahmensetzung für das Verhältnis von Grundrechtsträgern zueinander in den Vordergrund.[6]

Der Datenschutz im heutigen Sinne ist vor dem Hintergrund der automatisierten Verarbeitung personenbezogener Daten zu sehen.[7] Das weltweit erste Datenschutzgesetz wurde am 30.09.1970 in Deutschland in Hessen mit dem 1. Hessischen Datenschutzgesetz (HDSG) verabschiedet. 1974 folgte ein Datenschutzgesetz in

---

4 Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, Einleitung in BDSG, Rn. 3; Weigand in Listl, Handbuch des Kirchenrechts, S. 841 f.; Polenz/Heussen CHB, Besonderer Datenschutz Rn. 16.

5 Helfrich in Hoeren/Sieber/Holznagel, Teil 16.1 Einführung in die Grundbegriffe des Datenschutzes Rn. 1.

6 Helfrich in Hoeren/Sieber/Holznagel, Teil 16.1 Einführung in die Grundbegriffe des Datenschutzes Rn. 1.

7 Simitis in Simitis, BDSG, Einleitung Rn. 1 ff.

Rheinland-Pfalz. Auf Bundesebene wurde schließlich am 01.02.1977 das erste Bundesdatenschutzgesetz (BDSG) verabschiedet. Im Mittelpunkt stand dabei der Schutz personenbezogener Daten bei automatisierter Verarbeitung.

Einen weiteren Meilenstein im Datenschutzrecht stellte das sogenannte Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983 dar.[8] Das Urteil stellte fest, dass der Schutz vor Verarbeitung personenbezogener Daten vom allgemeinen Persönlichkeitsrecht in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG umfasst ist, und steckte weiter den Rahmen ab, in dem sich die Datenverarbeitung bewegen darf. Das Urteil stellte dabei den *„vernachlässigten verfassungsrechtlichen Konnex wieder her: Datenschutz ist Grundrechtsschutz"*.[9] Die Möglichkeit, durch Kombination von Datensätzen und Abgleichen von Datenbanken mittels Datenverarbeitung teilweise oder ganze Persönlichkeitsprofile zu erstellen, die der Betroffene weder erfassen noch auf Richtigkeit kontrollieren kann, führt dazu dass die informationelle Selbstbestimmung untrennbar mit der freien Entfaltung der Persönlichkeit verbunden ist.[10] Deren Schutz soll durch eine strenge Zweckbindung, informationelle Gewaltenteilung, ein Höchstmaß an Transparenz sowie die Einrichtung eines Datenschutzbeauftragten – der Präventiv einen Datenverarbeitungsprozess kontrollieren kann –, sichergestellt werden.[11]

Infolgedessen kam es zur Novellierung der Landesgesetzgebung zum Datenschutz und schließlich am 20.12.1990 zur Novellierung des BDSG.[12] Dem Schutz des Persönlichkeitsrechts standen die Funktionsfähigkeit der Verwaltung sowie Sicherheitsinteressen gegenüber, die nicht im Übermaß beschnitten werden sollten.

Mit der EG-Datenschutzrichtlinie vom 24.10.1995 wurde der Datenschutz auf Gemeinschaftsebene abgesteckt und der Versuch unternommen, das europäische Datenschutzrecht zu harmonisieren, um den Anforderungen der Voll-

---

8 BVerfGE 65, S. 1; Scheja/Haag in Leupold/Glossner MAH IT-Recht, Teil 5. Datenschutzrecht Rn. 7.

9 Simitis in Simitis, BDSG, Einleitung Rn. 30.

10 BVerfGE 65, S. 1 (42 f.).

11 Simitis in Simitis, BDSG, Einleitung Rn. 36 ff.; BVerfGE 65, S. 1 (45 ff.).

12 Simitis in Simitis, BDSG, Einleitung Rn. 52; Fundstelle BDSG, BGBl. I, 2954; zum Erlass von Landesgesetzen siehe Simitis in Simitis, BDSG, Einleitung Rn. 50 ff.

endung des gemeinsamen Marktes gerecht zu werden. Es sollte ein einheitliches Schutzniveau hinsichtlich der Rechte und Pflichten von datenverarbeitenden Personen sichergestellt werden und ein grenzüberschreitendender Verkehr personenbezogener Daten ermöglicht werden.[13] Aufgrund unterschiedlicher Schutzniveaus und teilweise sogar fehlender Regelungen wurden jedoch Ausnahmen vereinbart, die Unterschiede zwischen den Mitgliedstaaten zuließen.[14] Das Ziel, den Schutz personenbezogener Daten auszubauen, wurde beibehalten und sichergestellt, sodass Staaten mit einem höheren Schutzniveau dieses auch halten konnten. Als Reaktion darauf wurde mit der Novellierung des BDSG am 22.05.2001 die EG-Richtlinie in nationales Recht umgesetzt. Eine komplette Überarbeitung des Regelwerks, um eine innere Stimmigkeit herzustellen, war jedoch ausgeblieben, sodass eine Vielzahl widersprüchlicher Regelungen und Generalklauseln die Lesbarkeit des Textes erschwerte und der Normenklarheit widersprach.[15]

Die zunehmende Digitalisierung vieler Lebensbereiche führt zu bereichsspezifischen Regelungen im Datenschutz und damit gleichermaßen zu einem Zerfall dieses Rechtsgebietes[16]. Zukünftige Revisionen werden deswegen eine Konzentration des BDSG auf die Festlegung eines allgemeingültigen Rahmens erfordern, das Grundsätze für den Datenschutz festlegt.[17]

II. Datenschutz in der postalischen Lieferkette

Der Postverkehr offenbart Kommunikations- und Handelsbeziehungen zwischen natürlichen wie auch juristischen Personen. Innerhalb der postalischen Lieferkette können zahlreiche Informationen erhoben werden. Dazu zählen Sachdaten zum Inhalt einer Sendung wie das Gewicht oder der Warenwert, personenbezogene Informationen wie Absender oder Empfänger oder die Um-

13 RL 95/46/EG, S. 3 ff.

14 Simitis in Simitis, BDSG, Einleitung Rn. 205 ff. RL 95/46/EG, S. 5 ff.

15 Simitis in Simitis, BDSG, Einleitung Rn. 101 ff.

16 Simitis in Simitis, BDSG, Einleitung Rn. 123 ff.

17 Simitis in Simitis, BDSG, Einleitung Rn. 124.

stände einer Versendung wie Zeit und Ort. Mittels automatisierter Datenverarbeitung ist es heute möglich, diese Datensätze beliebig zu verarbeiten. Die Verarbeitungsmöglichkeiten dieser Datensätze und Ihre letztendlich grenzenlose Abruf- und Verwendbarkeit lassen Rückschlüsse auf Personen und Geschäfte bzw. Geschäftsgeheimnisse sowie auf persönliche Beziehungen, und auch Geschäftsbeziehungen zu. Daraus kann sich ein bestimmtes Profil ergeben, das je nach Qualität und Intensität der Informationen ein unterschiedliches Schutzniveau genießt.

Diese Informationen und die sich aus ihnen ergebenden Profile lassen jedoch auch Rückschlüsse auf die potenzielle Gefährlichkeit von Personen und Sendungen und das durch sie entstehende mögliche Bedrohungspotential zu. Deswegen steht der Datenschutz in diesem Bereich, in einem Spannungsverhältnis zwischen den Individualinteressen der Betroffenen und deren Schutz sowie der Sicherheit des Postverkehrs und damit der postalischen Kommunikation und des Handelsverkehrs. Von der Ausgestaltung der postalischen Prozesse und der Implementierung datenschutzrechtlicher Standards hängt in hohem Maße der Schutz des Allgemeinen Persönlichkeitsrechts und der Individualinteressen bei gleichzeitig größtmöglicher und umsetzbarer Sicherheit der Lieferkette ab.

III. Rechtsgrundlagen

Das Datenschutzrecht stellt einen durch das Unionsrecht harmonisierten Rechtsbereich dar. Infolgedessen müssen die Wechselwirkungen und Verpflichtungen des Unionsrechts sowie internationaler Vereinbarungen und die konkrete Ausgestaltung durch das nationale Recht beachtet werden.

1. Internationale Rechtsgrundlagen

Zahlreiche internationale Organisationen – wie die Vereinten Nationen, der Europarat oder die OECD – haben Dokumente verbschiedet, die Datenschutzstandards festlegen.

a) „Übereinkommen zum Schutz des Menschen bei automatisierter Verarbeitung personenbezogener Daten" des Europarates vom 28.01.1981

Die wichtigste internationale Vereinbarung ist das „Übereinkommen zum Schutz des *Menschen bei automatisierter Verarbeitung personenbezogener Daten*" des Europarates vom 28.01.1981. Auch wenn es sich um ein *„non self executing treaty"* handelt, wurde ein Mindeststandard festgelegt.[18] Die Konvention beschränkt sich auf den Schutz natürlicher Personen und legt fünf Verarbeitungsgrundsätze fest: So sind persönliche Daten rechtlich einwandfrei nach Treu und Glauben zu erheben und zu verarbeiten; ihre Nutzung ist zweckgebunden; sie müssen für den Verarbeitungszweck angemessen und relevant sein; sie haben sachlich richtig und aktuell zu sein und die Betroffenen dürfen aufgrund der Daten nur für den erforderlichen Zeitraum identifizierbar sein.[19]

Mit der Verabschiedung der EG-Datenschutzrichtlinie die höhere Datenschutzstandards für die EU-Mitgliedstaaten festlegte, sank die Bedeutung der Konvention, so dass ihr insoweit eine Hilfsfunktion für EU-Beitrittskandidaten zukommt, die vor ihrem Beitritt die Konvention ratifizieren müssen.[20]

b) „Richtlinien zur Verarbeitung personenbezogener Daten in automatisierten Dateien" der Vereinten Nationen vom 04.12.1990

Die *„Richtlinien zur Verarbeitung personenbezogener Daten in automatisierten Dateien*" der Vereinten Nationen vom 04.12.1990 legen ebenso wie die Konvention des Europarates einen Mindeststandard fest, nach dem sich neben den Staaten auch internationale Organisationen richten.[21] Die Verarbeitungsgrundsätze überschneiden sich und sehen den Grundsatz von Treu und Glauben; die Verarbei-

[18] Zum „non self-executing treaty" siehe Simitis in Simitis, BDSG, Einleitung Rn. 153.

[19] Simitis in Simitis, BDSG, Einleitung Rn. 158.

[20] Simitis in Simitis, BDSG, Einleitung Rn. 182.

[21] Simitis in Simitis, BDSG, Einleitung Rn. 196.

tung aktualisierter und vollständiger Daten, die Zweckbindung von Daten, die Einräumung garantierter Recht; sowie Sonderregeln für „sensitive Angaben vor.[22]

c) *„Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten" der OECD vom 23.09.1980*

Die *„Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten"* der OECD vom 23.09.1980 sind kein völkerrechtlich ratifiziertes und bindendes Dokument, sondern enthalten lediglich Vorschläge für Datenverarbeitungsgrundsätze.[23] Sie enthalten ebenfalls den Grundsatz von Treu und Glauben, die Zweckbindung, ein Recht auf Richtigkeit und Vollständigkeit der Daten, außerdem den Grundsatz einer transparenten Verarbeitung, Auskunfts-, Berichtigungs- und Löschungsrechte sowie die Verantwortlichkeit der adressierten Stellen.[24]

2. Das Recht der Europäischen Union

Inzwischen enthält das unionale Recht eine Vielzahl datenschutzrechtlicher Regelungen. Neben den Grundrechten der Grundrechtecharta und der EMRK befassen sich die Art. 39 EUV sowie 16 AEUV mit dem Schutz personenbezogener Daten.

Grundlage des unionalen Datenschutzes ist inzwischen die Datenschutz-Grundverordnung, die die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24.10.1995 ablöst. Die DatenschutzVO wurde am 04.05.2016 veröffentlicht und ist am 24.05.2016 in Kraft getreten. Im Telekommunikationsbereich gilt daneben die Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

---

22 Simitis in Simitis, BDSG, Einleitung Rn. 197.

23 Simitis in Simitis, BDSG, Einleitung Rn. 186 ff.

24 Simitis in Simitis, BDSG, Einleitung Rn. 186.

a) Art. 39 EUV

Art. 39 EUV enthält eine Forderung *„zur Festlegung von Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten* [...] *und über den freien Datenverkehr"*. Der Vertrag zur Gründung der Europäischen Gemeinschaft (EGV) enthielt keine Vorgängerregelung. Art. 39 EUV steht in einem Wechselwirkungsverhältnis zu Art. 16 AEUV. Weiterhin ist Art. 39 EUV lex specialis zu Art. 16 Abs. 2 AEUV.[25] So wird dem intergouvernementalen Charakter der GASP Rechnung getragen.[26]

b) Art. 16 AEUV (ex Art. 286 EGV)

Gemäß Art. 16 Abs. 1 AEUV hat jede Person *„das Recht auf Schutz der sie betreffenden personenbezogenen Daten"*. Weiterhin erlassen laut Art. 16 Abs. 2 AEUV das Europäische Parlament und der Rat, *„gemäß dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr. Die Einhaltung dieser Vorschriften wird von unabhängigen Behörden überwacht"*.

Durch den Schutz personenbezogener Daten in Art. 8 GrCh kommt es durch Art. 16 AEUV zu einer Dopplung des Datenschutzes.[27] Weiterhin begründet Art. 16 Abs. 2 AEUV eine Gesetzgebungskompetenz für den Datenschutz. Damit wird gleichzeitig die bisherige Akzessorietät zum Binnenmarkt abgelöst.[28]

---

25 Kugelmann in Streinz, EUV, Art. 39 EUV Rn. 3.

26 Kugelmann in Streinz, EUV, Art. 39 EUV Rn. 2.

27 Wegener/Kingreen in Callies/Ruffert, EUV, Art. 16 AEUV Rn. 3.

28 Wegener/Kingreen in Callies/Ruffert, EUV, Art. 16 AEUV Rn. 4.

c) Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr vom 24.10.1995

Die Richtlinie 95/46/EG ist zwar von der DatenschutzVO abgelöst worden, jedoch wurde Ihr Regelungsinhalt in nationales Recht umgesetzt und beeinflusst damit weiterhin das deutsche Datenschutzrecht. Dewegen soll ihr wesentlicher Inhalt im folgenden dargestellt werden.

Die Richtlinie 95/46/EG stützte sich auf Art. 95 EUV (ex Art. 100a EGV) und diente der Verwirklichung des Binnenmarktes.[29] Sie sollte den freien Datenverkehr zwischen den Mitgliedstaaten durch eine Harmonisierung der nationalen Vorschriften sicherstellen.[30] Bestehendes nationales Recht war damit entsprechend anzupassen und Richtlinienkonform auszulegen.[31] Sie galt gemäß Art. 3 Abs. 1 *„für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen“*. Eine Trennung zwischen der Datenverarbeitung öffentlicher und nicht-öffentlicher Stellen wie im BDSG fand nicht statt.[32]

Über die Intention und den Umfang der RL 95/46/EG geben die Erwägungsgründe Auskunft. Erwägungsgrund Nr. 2 betont den Dienstcharakter von Datenverarbeitungssystemen und den Schutz der Privatsphäre, der in Art. 1 Abs. 1 der RL 95/46/EG verbrieft wird.

---

29 EuGH, Urt. v. 20.05.2003 – C 465/00 u.a. SLG 2003, I – 4989, Österreichischer Rundfunk u.a., S. I–5033; Brühann/Wezembeek-Oppem, Mindeststandards oder Vollharmonisierung des Datenschutzes in der EG – Zugleich ein Beitrag zur Systematik von Richtlinien zur Rechtsangleichung im Binnenmarkt in der Rechtsprechung des Europäischen Gerichtshofs in EuZW 2009, S. 639 (640).

30 EuGH, Urt. v. 20.5.2003 – C 465/00 u.a. Slg. 2003, I – 4989, Österreichischer Rundfunk u.a., S. I–5033; Brühann/Wezembeek-Oppem, Mindeststandards oder Vollharmonisierung des Datenschutzes in der EG – Zugleich ein Beitrag zur Systematik von Richtlinien zur Rechtsangleichung im Binnenmarkt in der Rechtsprechung des Europäischen Gerichtshofs in EuZW 2009, S. 639 (640).

31 Scheja/Haag in Leupold/Glossner MAH IT-Recht Teil 5. Datenschutzrecht Rn. 17.

32 Scheja/Haag in Leupold/Glossner MAH IT-Recht Teil 5. Datenschutzrecht Rn. 21 ff.

aa) Art. 6 RL 95/46/EG

Art. 6 RL 95/46/EG legte Grundsätze, Rechte und Pflichten für die Verarbeitung personenbezogener Daten fest. Art. 6 Abs. 1a) RL 95/46/EG legte die Verarbeitung nach Treu und Glauben sowie in rechtmäßiger Weise als Grundsätze fest. Art. 6 Abs. 1b–e) RL 95/46/EG regelte die Zweckbindung der Daten. Wann eine Datenverarbeitung rechtmäßig ist, wird in Erwägungsgrund Nr. 30 RL 95/46/EG weiter präzisiert: *„Die Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn sie auf der Einwilligung der betroffenen Person beruht oder notwendig ist im Hinblick auf den Abschluss oder die Erfüllung eines für die betroffene Person bindenden Vertrags, zur Erfüllung einer gesetzlichen Verpflichtung, zur Wahrnehmung einer Aufgabe im öffentlichen Interesse, in Ausübung hoheitlicher Gewalt oder wenn sie im Interesse einer anderen Person erforderlich ist, vorausgesetzt, dass die Interessen oder die Rechte und Freiheiten der betroffenen Person nicht überwiegen. Um den Ausgleich der in Frage stehenden Interessen unter Gewährleistung eines effektiven Wettbewerbs sicherzustellen, können die Mitgliedstaaten insbesondere die Bedingungen näher bestimmen, unter denen personenbezogene Daten bei rechtmäßigen Tätigkeiten im Rahmen laufender Geschäfte von Unternehmen und anderen Einrichtungen an Dritte weitergegeben werden können.* [...]*“*. Dabei handelt es sich um Gründe, die in Art. 13 RL 95/46/EG als Ausnahmetatbestand wieder aufgegriffen werden.

bb) Art. 7 RL 95/46/EG

Art. 7 RL 95/46/EG regelt, unter welchen Voraussetzungen eine Verarbeitung personenbezogener Daten zulässig ist. Im „Machtbereich“ des Betroffenen liegen die Einwilligung (Art. 7a) RL 96/47/EG) sowie die Datenverarbeitung, die infolge einer Vertragserfüllung erforderlich ist (Art. 7b) RL 95/46/EG). Des Weiteren kann eine Datenverarbeitung durch eine Interessenabwägung bei „Wahrung lebenswichtiger Interessen der betroffenen Person“ (Art. 7d) RL 96/46/EG) oder zur Verwirklichung eines berechtigten Interesses (Art. 7f) RL 95/46/EG) zulässig sein. Schließlich lassen Interessen der Allgemeinheit eine Datenverarbeitung zu: bei Wahrnehmung von Aufgaben, die im öffentlichen Interesse liegen oder die in Ausübung öffentlicher Gewalt erfolgen (Art. 7e) RL 95/46/EG), sowie zur Erfüllung rechtlicher Verpflichtungen (Art. 7c) RL 95/46/EG).

cc) Art. 13 RL 95/46/EG

Art. 13 RL 95/46/EG regelt Ausnahmen und Einschränkungen auch von den Grundsätzen in Art. 6 RL 95/46/EG. Gemäß Art. 13 Abs. 1 RL 95/46/EG können Beschränkungen erlassen werden, wenn sich aus Gründen der Sicherheit des Staates (a); der Landesverteidigung (b); der öffentlichen Sicherheit (c); der Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder bei Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen (d); für ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union einschließlich Währungs-, Haushalts- und Steuerangelegenheiten (e); für Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben c), d) und e) genannten Zwecke verbunden sind (f) oder für den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen (g) notwendig sind.

Folglich sind dies auch Gründe für eine Abweichung von der Zweckbindung, wie sie in § 14 Abs. 2 BDSG oder § 28 Abs. 2 BDSG umgesetzt ist.[33] Die Zweckänderung darf mit dem Ursprungszweck jedoch nicht unvereinbar sein.[34]

dd) Art. 17 RL 95/46/EG

Art. 17 RL95/45/EG regelt die Sicherheit der Verarbeitung. Gemäß Art. 17 Abs. 1 RL 95/46/EG sehen die Mitgliedstaaten vor, *„daß der für die Verarbeitung Verantwortliche die geeigneten technischen und organisatorischen Maßnahmen durchführen muß, die für den Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang – insbesondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden – und gegen jede andere Form der unrechtmäßigen Verarbeitung personenbezogener Daten erforderlich sind. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei ihrer Durchführung*

33 Vgl. 4. Teil. C, II. 2.) b) hh) sowie 4. Teil. C. II. 2.) b) dd).

34 Erwägungsgrund Nr. 28 RL 95/46/EG.

entstehenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist".

Diese Aufforderung wird in § 9 BDSG sowie der Anlage zu § 9 BDSG aufgegriffen, umgesetzt und weiter präzisiert.[35]

ee) Zwischenergebnis

Die Richtlinie 95/46/EG legte den Rahmen für die Verarbeitung personenbezogener Daten fest, der im BDSG umgesetzt wurde. Neben den Begriffsbestimmungen wurden auch die Grundlagen für die Datenverarbeitung gesetzt und weiterhin festgelegt in welchen Fällen davon abgewichen werden durfte.

d) DatenschutzVO

Am 25.01.2012 hat die Kommission einen Vorschlag für eine Verordnung „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)" gemacht (im Folgenden: DatenschutzVO). Die DatenschutzVO orientiert sich dabei grundsätzlich an der Struktur der RL 95/46/EG, die sie abgelöst hat.

Die DatenschutzVO wurde am 04.05.2016 veröffentlicht und ist am 24.05.2016 in Kraft getreten. Als Verordnung ist das Regelwerk unmittelbar anwendbar und muss nicht mehr wie eine Richtlinie zuerst in nationales Recht umgesetzt werden. Dies ist auch mit weitreichenden Folgen für das deutsche Datenschutzrecht verbunden, insbesondere für das BDSG, das auf Kollisionen hin untersucht werden muss und in weiten Teilen an eigenständiger Regelungswirkung verliert.

aa) Einschlägige Neuregelungen/Änderungen

Die DatenschutzVO enthält eine Vielzahl von Neuregelungen und Änderungen. Insbesondere die Art. 4–7, 21, 23, 30, 33 und 34 DatenschutzVO erscheinen für eine Risikoanalyse besonders relevant und sollten genauer untersucht werden.

---

[35] Vgl. 2. Teil. VI. Technische und Organisatorische Maßnahmen.

(1) Art. 4 DatenschutzVO, Begriffsbestimmungen

Wie schon die RL 95/46/EG, bestimmt die DatenschutzVO einige Begriffe, die im Zusammenhang mit der Datenverarbeitung stehen.

Die Definition des für die Verarbeitung Verantwortlichen wurde fast wortwörtlich aus der RL 95/46/EG übernommen. Der materielle Gehalt hat sich nicht verändert.[36] Die Definition der betroffenen Person wurde im Vergleich zur RL 95/46/EG neu in den Definitionenkatalog aufgenommen (Art. 4 Nr. 1 DatenschutzVO). „[...] *personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann"*.

Das BDSG enthält einen Hinweis auf den Betroffenen in § 3 Abs. 1 BDSG.[37] Kern beider Definitionen ist, dass die bestimmte bzw. bestimmbare Person betroffen ist. Art. 4 DatenschutzVO präzisiert weiter, wie das Bestimmen aussehen kann.

Die Definition des Empfängers wurde in Art. 4 Nr. 9 DatenschutzVO gekürzt. Ein Empfänger ist demnach *„eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht"*. Die Definition wurde damit sogar sprachlich weiter an die Definition in § 3 Abs. 8 BDSG angenähert.[38]

---

[36] Daher kann auf die Ausführungen zur RL 95/46/EG verwiesen werden.

[37] Vgl. 2 Teil. IV. 2.) a).

[38] Vgl. 2 Teil. IV. 2.) c).

Die Definition der Verarbeitung von Daten (Art. 4 Abs. 3 DatenschutzVO) ist mit der Definition in Art. 2 b) RL 95/46/EG nahezu wortgleich. Lediglich der Begriff der „Kombination" wurde durch „Abgleich" ersetzt.

Im Vergleich der Begriffsbestimmungen aus Art. 4 DatenschutzVO zu Art. 2 RL 95/46/EG ergeben sich keine materiellen Veränderungen bei den oben besprochenen Begriffen. Einige Definitionen wurden redaktionell überarbeitet und weisen teilweise größere sprachliche Übereinstimmungen zu den Definitionen in § 3 BDSG auf.

(2) Art. 5 DatenschutzVO, Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten

Art. 5 Abs. 1 DatenschutzVO legt die Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten fest. *„Personenbezogene Daten müssen a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz"); b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Art. 89 Abs. 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung"); c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung"); d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit"); e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder*

für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 Abs. 1 verarbeitet werden („Speicherbegrenzung"); f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit")."

Art. 5 DatenschutzVO orientiert sich an Art. 6 RL 95/46/EG. Der Grundsatz von Treu und Glauben sowie die Rechtmäßigkeit finden sich bereits in Art. 6 Abs. 1 a) RL 95/46/EG. Art. 5 b) DatenschutzVO ist Art. 6 Abs. 1 b) nachgebildet, die Verarbeitung zu historischen, statistischen sowie wissenschaftlichen Zwecken wird hingegen gesondert geregelt. Art. 5 c) DatenschutzVO erweitert die bisherige Zweckbindung der Datenverarbeitung um eine Angemessenheitsprüfung und die Erforderlichkeit der Datenverarbeitung und schränkt diese dadurch ein. Neu hinzugekommen sind das Transparenzprinzip und die Haftung des Verantwortlichen.[39] Die weiteren Ziffern unterscheiden sich materiell nicht von Art. 6 RL 95/46/EG.

(3) Art. 6 DatenschutzVO, Rechtmäßigkeit der Verarbeitung

Art. 6 DatenschutzVO regelt die Rechtmäßigkeit der Verarbeitung. *„(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist: a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben; b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen; c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt; d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen; e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder*

[39] Erläuterungen zur DatenschutzVO Nr. 3.4.1.

in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde; f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Abs. 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Abs. 1 Buchstaben c und e wird festgelegt durch a) Unionsrecht oder b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt. Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Abs. 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Inte-

resse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Abs. 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche – um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist – unter anderem a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung, b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen, c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Art. 9 verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 verarbeitet werden, d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen, e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann."

Art. 6 Abs. 1a–e) DatenschutzVO ist wortgleich Art. 7 RL 95/46/EG nachgebildet.[40] Art. 6 Abs. 1f) DatenschutzVO erweitert die Interessensabwägung um die Betonung des besonderen Schutzes von Kindern.

Art. 6 Nr. 2 DatenschutzVO ist neu hinzugekommen und trägt dem Verordnungscharakter der Regelung Rechnung, indem ein Rechtsrahmen für Ermächtigungsgrundlagen der Datenverarbeitung festgelegt wird. Ermächtigungsgrundlagen können sich aus unionalem wie auch nationalem Recht ergeben. Demnach sind Regelungen nur aus öffentlichen Interesse oder zum Schutz der Rechte und Freiheiten Dritter zulässig. Darüber hinaus müssen sie allgemeinen Rechtsgrundsätzen wie dem Verhältnismäßigkeitsprinzip entsprechen und den Wesensgehalt des Schutzes personenbezogener Daten wahren.

[40] Siehe 2. Teil. A. III. 2.) c) aa).

(4) Art. 7 DatenschutzVO, Einwilligung

Art. 7 DatenschutzVO legt einen Rahmen für eine Einwilligung zur Datenverarbeitung fest. Dazu zählen die Beweislast, eine Eindeutigkeit im Bezug auf den zu bewilligenden Sachverhalt sowie der Widerruf und das „Machtverhältnis" zwischen den Beteiligten. Die Norm geht in ihrer Regelungsdichte damit über die Regelungen des § 4a BDSG hinaus, die sich mehr mit der Wirksamkeit als mit den Umständen einer Einwilligung beschäftigt.

(5) Art. 14 DatenschutzVO, Informationspflichten

Mit Art. 14 DatenschutzVO ist im Vergleich mit der RL 95/46/EG eine ausgedehnte Regelung der Informationspflicht gegenüber dem Betroffenen hinzugekommen. Diese wird bei jeder Datenverarbeitung auf ihre Anwendbarkeit hin untersucht werden müssen. Ausnahmetatbestände für eine Beschränkung der Regelung finden sich in Art. 21 DatenschutzVO.

(6) Art. 23 DatenschutzVO, Beschränkungen

Art. 23 DatenschutzVO regelt Beschränkungen der vorangegangenen Vorschriften.

Die Vorschrift ist Art. 13 RL 95/46/EG nachgebildet, wurde jedoch neu strukturiert. Allen Ausnahmetatbeständen vorangestellt sind das Verhältnismäßigkeitsprinzip und die „Notwendigkeit in einer demokratischen Gesellschaft".

(7) Art. 25 DatenschutzVO, Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Art. 25 DatenschutzVO findet keine Entsprechung in der RL 95/46/EG. Er steht in einem sachlichen Zusammenhang mit Art. 30 Nr. 1 DatenschutzVO und greift den Datenschutz durch technische und organisatorische Maßnahmen auf.

(8) Art. 32 Nr. 1 DatenschutzVO, Sicherheit der Verarbeitung

Art. 32 Abs. 1 DatenschutzVO findet keine Entsprechung in der RL 95/46/EG. *„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und*

der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein [...]". Im BDSG findet sich jedoch eine entsprechende Regelung in § 9.[41] § 9 BDSG wäre entsprechend Art. 32 Abs. 1 DatenschutzVO auszulegen. Ein dem entgegen stehender materieller Widerspruch der Regelungen ist nicht ersichtlich.

(9) Art. 35 DatenschutzVO, Datenschutz-Folgenabschätzung

Die Datenschutz-Folgeabschätzung in Art. 35 DatenschutzVO ist ein neues Element des unionalen Datenschutzes, das weder in RL 95/46/EG noch im BDSG eine Entsprechung hat. Demnach wird es im Vorfeld von Datenverarbeitung notwendig, eine Prognose über die Folgen und die Rechtswirkung von Datenverarbeitung für die betroffene Person zu stellen.

(10) Art. 36 DatenschutzVO, Vorherige Konsultation

Art. 36 DatenschutzVO stattet die Aufsichtsbehörden mit neuen Rechten und Pflichten aus. Sie sind vor einer den Betroffenen belastenden Datenverarbeitung vorab zu Rate zu ziehen und haben Datenverarbeitungsvorgänge gegebenenfalls zu genehmigen. Diese Regelung baut auf Art. 21 RL 95/46/EG auf.[42] Das BDSG sieht solche ausgedehnten Rechte bisher nicht vor.

Diese wären entsprechend beim Entwickeln neuer Datenverarbeitungsvorgänge zu berücksichtigen.

bb) Zwischenergebnis

Die DatenschutzVO nimmt die bisherigen Regelungen der RL 95/46/EG weitgehend auf. So sind Definitionen lediglich redaktionell überarbeitet worden. An den

41 Vgl. 2. Teil. VI. Technische und organisatorische Maßnahmen.

42 Erläuterungen zur DatenschutzVO Nr. 3.4.4.3.

Grundsätzen für die Datenverarbeitung hat sich im Wesentlichen wenig geändert. Die Neuerungen betreffen hauptsächlich den Schutz personenbezogener Daten und der betroffenen Personen. Ihr Schutz soll von Anfang an bei der Entwicklung und dem Entwurf von Datenverarbeitungssystemen berücksichtigt werden.[43] Dazu werden Vorgaben zum Verfahren gemacht. Es wird festgelegt, wie Datenverarbeitung in Zukunft entworfen werden soll. Weiterhin werden die Rechte und Pflichten von Aufsichtsbehörden und Datenschutzbeauftragten ausgebaut, um die Verfahren und Grundsätze zu implementieren und zu überwachen.

e) Zwischenergebnis

Bisher stellt das europäische Datenschutzrecht die gemeinsame Grundlage – als kleinsten gemeinsamen Nenner – für die nationalen Datenschutz-Rechtsordnungen der Mitgliedstaaten. Diese haben die Vorgaben der Richtlinien in nationales Recht umzusetzen, welches im Lichte der Richtlinien zu lesen ist. Bisher ist die Regelungsdichte des nationalen Datenschutzrechts in Deutschland höher als in Europa. Die DatenschutzVO etabliert jedoch auch neue Instrumente zum Schutz personenbezogener Daten. Mit einer DatenschutzVO wird der Schwerpunkt des Datenschutzrechts deutlich auf die europäische Ebene verlagert. Gleichzeitig werden weite Teile nationalen Datenschutzrechts verdrängt.

3. Nationale Gesetzgebung

Neben bereichsspezifischen Regelungen bildet das Bundesdatenschutzgesetz (BDSG) vom 14.01.2003 die Grundlage datenschutzrechtlicher Regelungen in Deutschland.

a) BDSG

Das erste Bundesdatenschutzgesetz wurde am 27.01.1977 als „Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung“ verab-

[43] Vgl. auch Privacy by Design Vgl. 2. Teil. VI. 3.)

schiedet und in Folge des Volkszählungsurteils des Bundesverfassungsgerichts 1990 schließlich einer großen Novellierung unterzogen.[44] Weitere Anpassungen folgten aufgrund europäischer Gesetzesakte.[45] Weiterhin dürfte die Datenschutz-VO weitere Anpassungen notwendig machen.

b) Zwischenergebnis

Die regelmäßigen Gesetzesanpassungen des BDSG lassen einen Rückschluss auf die hohe Dynamik auf diesem Rechtsgebiet zu. Durch die unionalen Vorgaben und Harmonisierungen sind weitere Novellierungen des BDSG zu erwarten.

4. Verhältnis der Rechtsebenen zueinander

Die Anwendung einzelner Rechtsebenen setzt ihre Anwendbarkeit voraus. Dafür ist das Verhältnis der Rechtsebenen zueinander zu bestimmen. Im Grundsatz gilt „lex superior derogat lege inferiori".[46] Dafür muss jedoch der gleiche Sachverhalt geregelt werden.[47] Darüber hinaus regeln viele Gesetzestexte ihr Verhältnis zu anderen Rechtsgebieten selbst.

a) Verhältnis internationaler Verträge zum nationalen Recht

Internationale Bestimmungen sind im nationalen Recht nur so weit bindend wie sie in nationales Recht umgesetzt wurden. Das „Übereinkommen zum Schutz des Menschen bei automatisierter Verarbeitung personenbezogener Daten" des Europarates vom 28.01.1981 kann darüber hinaus eine besondere Wirkung entfalten, insoweit es vom EGMR zur Urteilsfindung herangezogen wird.

---

44 Zur Geschichte des Datenschutzes siehe auch ausführlich Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, Einleitung BDSG, Rn. 1 ff.

45 Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, Einleitung BDSG, Rn. 6.

46 Kirchhof in Maunz/Dürig, GG, Art. 84 Rn. 114.

47 Vgl. 4. Teil. C. II. 2.) d).

b) Verhältnis der RL 95/46/EG zum nationalen Recht

Das Verhältnis der Richtlinie 95/46/EG zum nationalen Recht regelte diese in Art. 4. Demnach wendet jeder Mitgliedstaat die Vorschriften an, *„die er zur Umsetzung dieser Richtlinie erläßt, auf alle Verarbeitungen personenbezogener Daten an* [...]*"*. Für Deutschland ist dies das BDSG, das mit dem Änderungsgesetz am 22.05.2001 die Vorgaben der Richtlinie umgesetzt hat.

c) Verhältnis der DatenschutzVO zum nationalen Recht

Als Verordnung ist die DatenschutzVO anders als eine Richtlinie direkt anwendbar. Regelungsbereiche, die bisher durch das BDSG in nationales Recht umgesetzt werden bzw. direkt vom BDSG geregelt werden, treten hinter dem Anwendungsvorrang der Grundverordnung zurück.[48] Damit könnten weite Teile des bisherigen Regelungsgehaltes des BDSG verdrängt werden.

5. Zwischenergebnis

In den letzten 35 Jahren hat das Datenschutzrecht auf internationaler Ebene eine neue Regelungsdichte erfahren, die insbesondere durch Regelungen auf europäischer Ebene auch die nationalen Regelwerke stark beeinflusst hat. Diese Entwicklung wird sich mit der DatenschutzVO weiter beschleunigen und verstärken. Das nationale Datenschutzrecht, bisher für die Adressaten und Verpflichteten letztendlich gleichermaßen maßgeblich, wird allmählich durch das europäische Datenschutzrecht in seiner Bedeutung abgelöst.

[48] Schmidt-Aßmann in Schoch/Schneider/Bier, VwGO, I, Rn. 110 ff.

IV. Begriffsbestimmungen im Datenschutz

Grundlage für die Analyse der elektronischen Datenverarbeitung ist die Bestimmung der dafür wichtigen Grundbegriffe.

Das BDSG regelt bereits im ersten Abschnitt allgemeine und gemeinsame Bestimmungen. Hervorzuheben sind dabei die für die Risikoanalyse relevanten Legaldefinitionen in § 3 BDSG. Daneben sind die europarechtlichen Vorgaben, insbesondere die Begriffsbestimmungen in Art. 2 der DatenschutzVO, zu beachten und mit den Vorgaben des BDSG zu vergleichen.

Den Ausgangspunkt bildet der Begriff der „personenbezogenen Daten", der die Reichweite und die damit verbundene Art der Informationen festlegt. Weiterhin sind die möglichen Adressaten datenschutzrechtlicher Regelungen, die „verantwortlichen Stellen", die „Empfänger" und die „Dritten" zu typisieren und voneinander abzugrenzen.

Schließlich werden die möglichen Phasen und Vorgänge der Datenverarbeitung: das Erheben und das Verarbeiten, mit den Vorgängen des Speicherns, des Veränderns, des Übermittelns, des Sperren und des Löschens sowie dem Nutzen kategorisiert, voneinander abgegrenzt und definiert. Die Definitionen sind grundsätzlich medienneutral formuliert und können deswegen von den Definitionen in der reinen IT-Fachsprache abweichen.[49]

1. Personenbezogene Daten

Ausgangspunkt für Erwägungen im datenschutzrechtlichen Bereich ist die Analyse eines Personenbezugs von Daten. Nationale Begriffsbestimmungen sind dabei europarechtskonform auszulegen und die unionalen Begriffsbestimmungen sind zu beachten.

[49] Die Definitonen der IT-Fachsprache sind aufgrund ihrer mangelnden rechtlichen Relevanz, soweit juristische Legaldefinitionen überhaupt vorhanden sind, nicht Gegenstand der Untersuchung. Vgl. auch Dammann in Simitis, BDSG, § 3 Rn. 1.

a) Begriffsbestimmung nach dem BDSG

Der Begriff der personenbezogenen Daten ist in § 3 Abs. 1 BDSG legaldefiniert und meint *„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“.* Eine solche Definition findet sich ebenfalls in anderen Gesetzen.[50] Die besonderen Arten personenbezogener Daten sind in Art. 3 Abs. 9 BDSG aufgezählt. Das *„sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben“.*

Unter Einzelangaben versteht man jede Information, die sich auf einzelne bestimmte oder bestimmbare Personen bezieht. Darunter fallen auch die Adresse oder Anschrift sowie Namen – oder diesen ersetzende Angaben oder Nummern – falls sich ein Personenbezug herstellen lässt.[51] Aggregierte, d. h. zusammengefasste, Daten sind keine personenbezogenen Daten.[52] Die Einbeziehung der persönlichen und sachlichen Verhältnisse verdeutlicht die umfassende Anwendung des Begriffs der personenbezogenen Daten.[53] Geschützt sind vom BDSG zudem nur natürliche Personen. Juristische Personen sowie Personengruppen sind nicht umfasst und werden nur vom allgemeinen Persönlichkeitsrecht geschützt.[54]

Der Begriff der personenbezogenen Daten ist relativ zu sehen. Sind Daten durch Zusatzwissen, Verknüpfungen, technische Systeme etc. unter Berücksichtigung eines verhältnismäßigen Aufwandes bestimmbar, so können sie in diesen Fällen einen Personenbezug aufweisen, für Unsicherheiten diesbezüglich haftet die verantwortliche Stelle.[55]

---

50 So in § 203 Abs. 2, S. 2 StGB, sowie in § 16 Abs. 1 des Gesetzes über die Statistik für Bundeszwecke.

51 Dammann in Simitis, BDSG, § 3 Rn. 10.

52 Schild/Ronellenfitsch/Arlt/Dembowski/Müller/Piendl/Rydzy/Schriever-Steinberg/Topp/Wehrmann/Wellbrock, Praxis der Kommunalverwaltung, Bd. B16, 23 Rn. 13 f.

53 Dammann in Simitis, BDSG, § 3 Rn. 7.

54 Dammann in Simitis, BDSG, § 3 Rn. 17.

55 Dammann in Simitis, BDSG, § 3 Rn. 32 ff.

b) Begriffsbestimmung nach Unionsrecht

Die DatenschutzVO definiert unter Art. 4 Nr. 1) personenbezogene Daten als *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann".*[56]

Die unionsrechtliche Begriffsbestimmung versucht ebenfalls eine möglichst breite Definition und die Erfassung aller Daten mit Personenbezug.[57] Besondere Beachtung verdient der explizite Bezug auf die Zuordnung zu einer Kennnummer, womit wohl auch die IP-Adresse ein personenbezogenes Datum darstellt.[58]

c) Schlussfolgerung

Die Definitionen „personenbezogener Daten" auf nationaler und unionaler Ebene sind weitgehend deckungsgleich. Ausgehend von einer bestimmten bzw. bestimmbaren natürlichen Person wird auf die ihr zuordnungsfähigen Informationen abgestellt. Die DatenschutzVO spricht klarer von „allen Informationen" und führt dann Beispiele an, während das BDSG diese mit „Einzelangaben über persönliche und sachliche Verhältnisse umschreibt. Unterschiede im materiellen Gehalt beider Definitionen sind nicht auszumachen.

---

[56] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ABl. Nr. L 281 vom 23.11.1995, S. 0031–0050.

[57] ABl. EG Nr. C94 v. 11.03.1992, S. 173.

[58] Helfrich in Hoeren/Sieber/Holznagel, Teil 16.1 Einführung in die Grundbegriffe des Datenschutzes Rn. 34.

2. An der Datenverarbeitung beteiligte Parteien

Zu untersuchen und voneinander abzugrenzen sind die verschiedenen Gruppen der „verantwortlichen Stelle", der „Betroffenen", der „Empfänger" und der „Dritten", die mit der Datenverarbeitung in Berührung kommen.

a) Verantwortliche Stelle

Als verantwortliche Stelle bezeichnet § 3 Abs. 7 BDSG *„jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt".*

Die Definition macht den Willen des Gesetzgebers deutlich, den „Herrn der Daten" – das bedeutet jeden der Daten verarbeitet oder dies zu verantworten hat – zu erfassen.[59] Das BDSG stellt auf eine juristische, nicht auf eine wirtschaftliche Einheit ab.[60] Bei Tochterunternehmen oder Outsourcing kann es sich um Dritte handeln, es sei denn es liegt eine Weisungsgebundenheit vor; die freie Gestaltungsmöglichkeit dient hierbei als Abgrenzungskriterium.[61]

Art. 4 Nr. 7) DatenschutzVO sieht als für die Verarbeitung verantwortliche *„die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche bzw. können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden".*

Das BDSG wie auch die DatenschutzVO gehen von einem weiten Begriff der verantwortlichen Stelle aus. Während das BDSG von jeder Person oder Stelle spricht, differenziert die Richtlinie den Begriff der Stelle in Behörden, Einrichtungen und anderen Stellen aus, die vom Stellenbegriff des BDSG ebenfalls umfasst sind. Das Abstellen auf die eigene Verarbeitung oder im Auftrag ist von der

[59] Schaffland/Wiltfang, BDSG, § 3 Rn. 79.

[60] Schaffland/Wiltfang, BDSG, § 3 Rn. 86 f.

[61] Schaffland/Wiltfang, BDSG, § 3 Rn. 54 f.

Formulierung nahezu identisch. Hier kann von einem einheitlichen Begriff der verantwortlichen Stelle ausgegangen werden.

b) Betroffener

Neben der Definition der personenbezogenen Daten enthält § 3 Abs. 1 BDSG den Hinweis auf die Betroffenen als bestimmte oder bestimmbare natürliche Person. Der Betroffene ist die Person, die durch die Regelungen des BDSG geschützt werden, und der deswegen eine Reihe von Kontroll- und Schutzmechanismen eingeräumt werden soll.

In der DatenschutzVO findet sich keine Legaldefinition für den Begriff des Betroffenen.

c) Empfänger von Daten

Ein Empfänger ist gemäß § 3 Abs. 8 S. 1 BDSG *„jede Person oder Stelle, die Daten erhält“.*

Dabei kann es sich um eine verantwortliche Stelle oder auch um einen Dritten handeln.[62]

Art. 4 Nr. 9) der DatenschutzVO sieht in einem Empfänger *„eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung“*.

Die Bezeichnung der „Stelle“ unterscheidet sich nach unionalem und nationalem Recht in der Formulierung, wie bei der verantwortlichen Stelle, meint jedoch

[62] Dammann in Simitis, BDSG, § 3 Rn. 228a ff.

den gleichen materiellen Umfang. Auch die Einbeziehung eines Dritten gilt für beide Definitionen.

d) Dritte im Bezug auf die Datenverarbeitung

Ein Dritter ist nach der Definition des § 3 Abs. 8 S. 2 BDSG *„jede Person oder Stelle außerhalb* der verantwortlichen Stelle". § 3 Abs. 8 S. 3 BDSG schließt die Eigenschaft eines Dritten aus für *„Betroffene, sowie Personen und Stelle, die im Inland, in einem anderen Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogenen Daten im Auftrag erheben, verarbeiten oder nutzen".*

Unter einem Dritten versteht Art. 4 Nr. 10) DatenschutzVO *„ine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten".*

Die Legaldefinition der DatenschutzVO geht genauer auf die Personen ein, die nicht Empfänger sind. Diese Personen zählen nach nationalem Recht zur verarbeitenden Stelle, die nicht Empfänger sein kann. Demnach decken sich auch diese Begriffsbestimmungen.

3. Phasen der Datenverarbeitung

Die Terminologie bezüglich der Phasen der Datenverarbeitung ist nicht einheitlich. Die Begriffe auf unionaler, Bundes- und Landesebene unterscheiden sich.

Das BDSG geht von einem engeren Verarbeitungsbegriff aus und fasst das Erheben und das Nutzen nicht unter den Begriff der Datenverarbeitung, sondern lässt beide Begriffe daneben stehen, so dass es hier zu einer „Trias" kommt.[63]

Das Europarecht und die meisten Landesgesetze gehen hingegen von einem umfassenden Verarbeitungsbegriff aus und schließen die Begriffe des Erhebens

[63] Polenz in Kilian/Heussen CHB, Phasen der Datenverarbeitung Rn. 29.

und des Nutzens in den Begriff der Datenverarbeitung mit ein.[64] So versteht Art. 4 Nr. 2) der DatenschutzVO unter Verarbeitung personenbezogener Daten *„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung"* und fächert so die Verarbeitungsmöglichkeiten weiter auf.

a) Datenerhebung

Die Erhebung von Daten ist in § 3 Abs. 3 BDSG als *„das Beschaffen von Daten über den Betroffenen"* definiert.

Für den Begriff der Datenerhebung ist es irrelevant, ob diese manuell oder automatisiert, mündlich oder schriftlich, vom Betroffenen selbst oder von Dritten beschafft werden.[65] Die Erhebung von Daten ist nicht Teil der Datenverarbeitung, sondern als Vorphase eine Voraussetzung für die Datenverarbeitung.

b) Datenverarbeitung

Das Verarbeiten von Daten regelt § 3 Abs. 4 S. 1 BDSG als *„das Speichern, Verändern, Übermitteln, Sperren, und Löschen personenbezogener Daten"* und stellt damit einen Oberbegriff für den Umgang mit personenbezogenen Daten dar.[66] Die Verarbeitung geschieht *„ungeachtet der dabei angewendeten Verfahren"*. Es ist somit unerheblich, ob die Verarbeitung manuell oder automatisiert erfolgt.

---

64 Polenz in Kilian/Heussen CHB, Phasen der Datenverarbeitung Rn. 28.

65 Buchner in Taeger/Gabel, BDSG, § 3 Rn. 25 f.

66 Schaffland/Wiltfang, BDSG, § 3 Rn. 21.

aa) Das Speichern von Daten

Unter Speichern versteht § 3 Abs. 4 S. 2 Nr. 1 BDSG *„das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung“.*

Der Begriff der Datenspeicherung wird anhand der drei Vorgänge Erfassen, Aufnehmen und Aufbewahren beschrieben, die eine Vergegenwärtigung von Daten zur Folge haben.[67] Weiterhin ist eine Zweckbindung an eine weitere Verarbeitung oder Nutzung notwendig, ausreichend ist hierfür die Absicht oder die potenzielle Möglichkeit.[68]

bb) Das Verändern von Daten

Das Verändern von Daten definiert § 3 Abs. 4 S. 2 Nr. 2 BDSG als *„das inhaltliche Umgestalten gespeicherter personenbezogener Daten“.*

Eine Umgestaltung liegt dann vor, wenn die Daten ihren Informationswert oder Aussagewert ändern.[69] Dies kann ebenfalls durch eine Verknüpfung von Daten verschiedener Dateien, die so in einen neuen Kontext gestellt werden, der Fall sein.[70] Das Hinzufügen von Informationen ist vom Speichern abzugrenzen: Falls die bestehenden Informationen nicht verändert werden, handelt es sich um ein „Hinzu-speichern“.[71]

cc) Das Übermitteln von Daten

Das Übermitteln von Daten ist grundsätzlich in § 3 Abs. 4 S. 2 Nr. 3 BDSG als *„das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten“* definiert. Weiterhin macht das Gesetz zwei

67 Dammann in Simitis, BDSG, § 3 Rn. 115 ff.; Schaffland/Wiltfang, BDSG, § 3 Rn. 36.

68 Schaffland/Wiltfang, BDSG, § 3 Rn. 36 ff.

69 Schaffland/Wiltfang, BDSG, § 3 Rn. 65.

70 Dammann in Simitis, BDSG, § 3 Rn. 131.

71 Schaffland/Wiltfang, BDSG, § 3 Rn. 67.

Varianten der Übermittlung aus, die Weitergabe an Dritte sowie das Einsehen oder Abrufen bereitgehaltener Daten durch Dritte.

Keine Weitergabe an Dritte liegt bei Übermittlung an einen Auftragnehmer innerhalb der speichernden Stelle vor.[72]

dd) Das Sperren von Daten

Unter Sperren versteht § 3 Abs. 4 S. 2 Nr. 4 BDSG *„das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken".*

Eine bestimmte Form ist für die Kennzeichnung nicht vorgeschrieben, muss jedoch für jedermann erkennbar sein.[73] Die so gekennzeichneten Daten dürfen außer in gesetzlich erlaubten Fällen nicht mehr genutzt werden.[74]

ee) Das Löschen von Daten

Das Löschen ist in § 3 Abs. 4 S. 2 Nr. 5 BDSG als *„das Unkenntlichmachen gespeicherter personenbezogener Daten"* definiert.

Im Ergebnis des Löschungsvorganges darf der Inhalt – die Information – einer Datei nicht mehr erkennbar bzw. lesbar sein.[75] Ein Rückgriff auf diese Informationen muss ausgeschlossen sein.[76]

c) Nutzen von Daten

Gemäß § 3 Abs. 5 BDSG ist Nutzen *„jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt".*

---

72 Buchner in Taeger/Gabel, BDSG, § 3 Rn. 34.

73 Schaffland/Wiltfang, BDSG, § 3 Rn. 73a.

74 Schaffland/Wiltfang, BDSG, § 3 Rn. 73a.

75 So auch im Ergebnis Dammann in Simitis, BDSG, § 3 Rn. 173 ff.

76 Schaffland/Wiltfang, BDSG, § 3 Rn. 75.

Das Nutzen stellt somit einen Auffangtatbestand dar, um jede Verwendung personenbezogener Daten zu erfassen.

d) Zwischenergebnis

Auch wenn das BDSG nicht einem weiten Verarbeitungsbegriff folgt, dient die Trias von Erheben, Verarbeiten und Nutzen insbesondere mit der weiteren Auffächerung des Begriffs der Datenverarbeitung einer lückenlosen und flächendeckenden Erfassung aller potenziellen gegenwärtigen und zukünftigen Möglichkeiten der Verwendung von Daten.

4. Anonymisieren und pseudonymisieren

Weiterhin kommt der Begriffen des Anonymisierens (§ 3 Abs. 6 BDSG) und Pseudonymisierens (§ 3 Abs. 6a BDSG) im Bereich des Schutzes personenbezogener Daten eine besondere Bedeutung zu.

a) Anonymisieren

Gemäß § 3 Abs. 6 BDSG versteht man unter Anonymisieren *„das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können"*. Die DatenschutzVO definiert den Begriff nicht.

Die Folge des Anonymisierens ist der Verlust des Personenbezugs der Daten, sodass diese nicht mehr unter das Regime des BDSG fallen.[77] Dafür darf eine Reanonymisierung unter normalen Bedingungen nicht mehr möglich sein.[78] Die Beweislast trägt die verarbeitende Stelle[79].

---

[77] So auch Gola/Schomerus, BDSG, § 3 Rn. 43.

[78] Gola/Schomerus, BDSG, § 3 Rn. 44; Plath/Schreiber in Plath, BDSG, § 3 Rn. 58; Buchner in Taeger/Gabel, BDSG, § 3 Rn. 44; wohl strengere Anforderungen an die Reanonymisierung bei Dammann in Simitis, BDSG, § 3 Rn. 196 ff.

[79] Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 51.

b) Pseudonymisieren

Gemäß § 3 Abs. 6a BDSG versteht man unter Pseudonymisieren *„das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren"*. Das Pseudonymisieren ist eine Technik zur Datenvermeidung, die angewendet wird, wenn die Identität der betroffenen Person nicht zwingend erforderlich ist.[80] Über eine Referenzdatei kann die verarbeitende Stelle die Pseudonymisiererung auflösen.[81] Ohne diese findet letztendlich eine Anonymisierung statt.[82]

Die DatenschutzVO definiert in Art. 4 Nr. 5 die Pseudonymisierung als *„die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden"*.

Der materielle Gehalt der Bestimmungen deckt sich.

c) Zwischenergebnis

Den beiden Begriffspaaren der Anonymisierung und Pseudonymisierung kommt mit einer steigend EDV-gestützten Datenverarbeitung eine immer größere Rolle zu. Dies wird besonders an der prominenten Nennung in § 3a BDSG deutlich. Eine Diskrepanz zwischen den nationalen Definitionen und der europarechtlichen Verwendung der Begriffe besteht nicht.

---

80 Gola/Schomerus, BDSG, § 3 Rn. 46.

81 Gola/Schomerus, BDSG, § 3 Rn. 46; Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 52.

82 Plath/Schreiber in Plath, BDSG, § 3 Rn. 62.

5. Zwischenergebnis

Die Legaldefinitionen des § 3 BDSG sowie von Art. 2 DatenschutzVO beabsichtigen eine weitgehende Erfassung und Beschreibung der im Zusammenhang mit Datenverarbeitung stehenden Faktoren. Keine materiellen Unterschiede ergeben sich bei den Definitionen der personenbezogenen Daten, der verantwortlichen Stelle, dem Empfänger und dem Dritten. Bei der Beschreibung der Phasen der Datenverarbeitung bestehen hingegen Unterschiede. Während die Datenschutz-VO von einem einheitlichen Begriff der Datenverarbeitung ausgeht, unterscheidet das BDSG zwischen der Erhebung, Verarbeitung und Nutzung von Daten, die nach der Richtlinie alle unter den Begriff der Verarbeitung fallen.

V. Ermächtigungsgrundlagen der Datenverwendung

Das BDSG regelt, unter welchen Umständen personenbezogene Daten überhaupt verwendet werden dürfen.

1. Grundsatz des Verbots mit Erlaubnisvorbehalt

Ausgangspunkt für die Regelung der Ermächtigungsgrundlagen der Datenverwendung ist der Grundsatz des Verbots mit Erlaubnisvorbehalt gemäß § 4 Abs. 1 BDSG.[83] Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist somit grundsätzlich verboten.[84] Eine Erlaubnis liegt lediglich bei Einwilligung des Betroffenen oder aufgrund eines Erlaubnistatbestandes in einer Rechtsvorschrift vor.[85] Die Vorschrift setzt damit das Volkszählungsurteil des Bundesverfassungsgerichts um.[86] Erwägungsgründe der Datenschutz-VO folgen dem gleichen Prinzip.

[83] So auch Plath in Plath, BDSG, § 4 Rn. 1; Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, § 4 Rn. 1.

[84] Taeger in Taeger/Gabel, BDSG, § 4 Rn. 1; Scholz/Sokol in Simitis, BDSG, § 4 Rn. 3.

[85] Helfrich in Hoeren/Sieber/Holznagel, Teil 16.1 Einführung in die Grundbegriffe des Datenschutzes Rn. 35.

[86] BVerfG, NJW 1984, 419 (422); Gola/Schomerus in Gola/Schomerus, BDSG, § 4 Rn. 1.

a) Einwilligung

Ohne Erlaubnistatbestand in einer Rechtsnorm bedarf es gemäß § 4 Abs. 1 BDSG für die Verwendung personenbezogener Daten der Einwilligung durch den Betroffenen.[87] Diese wird in § 4a BDSG genauer geregelt. Demnach bedarf es für eine wirksame Einwilligung einer freien Entscheidung des Betroffenen. Weiterhin bestehen Informationspflichten und grundsätzlich die Schriftform.

Die DatenschutzVO sieht in Art. 2 Nr. 11) in einer Einwilligung *„der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist"*. Damit folgt der Tatbestand von § 4a BDSG den unionalen Vorgaben.

Bei einer Einwilligung handelt es sich – der Terminologie und Systematik des bürgerlichen Rechts folgend – um eine auslegbare Willenserklärung und nicht um einen bloßen Rechtsakt.[88]

b) Erlaubnistatbestände

Fraglich erscheint, wann ein Erlaubnistatbestand vorliegt bzw. als Ermächtigung ausreicht. Teilweise werden Erlaubnistatbestände außerhalb des BDSG verlangt, die eine Abwägung des Gesetzgebers zwischen dem informationellen Selbstbestimmungsrecht des Einzelnen und des Wohls der Allgemeinheit erkennen lassen.[89] Andere lassen einen Rückgriff auf die Erlaubnistatbestände des BDSG zu.[90]

---

87 Spindler/Nink in Spindler/Schuster, Recht der elektronischen Medien, § 4 BDSG, Rn. 6; Taeger in Taeger/Gabel, BDSG, § 4 Rn. 48.

88 Gola/Schomerus in Gola/Schomerus, BDSG, § 4a Rn. 2; Plath in Plath, BDSG, § 4a Rn. 7 ff.; Simitis in Simitis, BDSG, § 4a Rn. 20.

89 Wohl Taeger in Taeger/Gabel, BDSG. § 4 Rn. 24 ff.

90 Wohl Gola/Schomerus in Gola/Schomerus, BDSG, § 4 Rn. 8; sowie Scholz/Sokol in Simitis, BDSG, Rn. 8 ff.

Der Wortlaut des § 4 Abs. 1 BDSG nennt die beiden Varianten eines Erlaubnistatbestands („[...] *soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet* [...]“) gleichberechtigt nebeneinander, ohne ein Rangverhältnis oder eine Subsidiarität festzulegen. Weder die Systematik noch die Historie der Norm lassen den Ausschluss von Erlaubnistatbeständen des BDSG zu. Vielmehr ist davon auszugehen, dass gerade bei älteren Gesetzen der Datenschutz noch nicht in ausreichender Form berücksichtigt wurde und so ein Rückgriff auf die Regelungen des BDSG notwendig wird. Schließlich würden die speziellen Erlaubnistatbestände des BDSG ins Leere laufen, was nicht dem Willen des Gesetzgebers entsprechen dürfte, der spezielle Rechtsvorschriften (beispielsweise in § 14 BDSG) als eine Tatbestandsvariante von mehreren aufführt. Darüber hinaus wird ein Erlaubnistatbestand den generellen Anforderungen an die Bestimmtheit und Klarheit genügen müssen.

2. Zwischenergebnis

Grundsätzlich bauen das europäische und das nationale Datenschutzrecht auf einem Konsens der Beteiligten in der Datenverarbeitung auf. Insbesondere soll der Betroffene Herr über seine Daten bleiben. Da dies nicht immer möglich ist und das Rechtsgut der informationellen Selbstbestimmung mit den Rechtsgütern der Allgemeinheit abgewogen werden muss, hat sich im Datenschutzrecht ein Dualismus aus der Einwilligung des Betroffenen und der Abwägung des Gesetzgebers in Form eines Erlaubnistatbestandes entwickelt, sodass durch das Verbot mit Erlaubnisvorbehalt keine „ungeregelte“ Verwendung personenbezogener Daten mehr stattfinden kann.

VI. Technische und organisatorische Maßnahmen

Ein effektiver Datenschutz setzt entsprechende technische und organisatorische Maßnahmen voraus, die die Grundsätze des Datenschutzes in der Praxis umsetzen und verankern.

1. § 9 BDSG

Die Verpflichtung zu einem effektiven Datenschutz wird in § 9 BDSG statuiert „Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht".

Diese Regelung kann als Kernregelung der Sicherheit personenbezogener Daten in Deutschland verstanden werden.[91] Sie dient dem Schutz, der von der Verarbeitung ihrer personenbezogenen Daten Betroffenen und verlangt von den Verpflichteten die Auswahl angemessener und wirksamer Maßnahmen.[92]

a) Anwendungsbereich

§ 9 BDSG gilt für den Fall der Verarbeitung personenbezogener Daten (siehe I. 3.) a)) und verpflichtet jede öffentliche und nicht-öffentliche Stelle.[93] Im Fall der Auftragsdatenverarbeitung liegt die Verpflichtung, für die Umsetzung des § 9 BDSG zu sorgen, bei der verantwortlichen Stelle im Sinne von § 3 Abs. 7 BDSG.[94]

Der Wortlaut sagt nichts über die Art der Datenverarbeitung, ob sie manuell oder automatisiert zu erfolgen hat. Unter nichtautomatisierter (manueller) Datenverarbeitung versteht man Vorgänge, die ohne den Einsatz von programmgesteuerten Datenverarbeitungsanlagen ablaufen.[95] Das BDSG regelt in § 1 Abs. 2 sowie § 27 Abs. 1 auch Fälle nichtautomatisierter Datenverarbeitung und es deu-

---

91 Kramer/Meints in Hoeren/Sieber/Holznagel, Teil 16.5 Datensicherheit Rn. 24.

92 Schaffland/Wiltfang, BDSG, § 9 Rn. 1.

93 Ernestus in Simitis, BDSG, § 9 Rn. 4 f.

94 Plath in Plath, BDSG, § 9 BDSG, Rn. 5; Gola/Schomerus, BDSG, § 9 Rn. 3.

95 Schaffland/Wiltfang, BDSG, § 9 Rn. 14.

tet nichts darauf hin, diese Fälle aus dem Anwendungsbereich des § 9 ausschließen zu wollen.[96] Folglich ist es unerheblich, ob die Datenverarbeitung manuell oder automatisiert stattfindet.[97]

Die Regelung umfasst den gesamten Vorgang der Datenverarbeitung vom Erheben über das Verarbeiten bis zum Nutzen von Daten. Gemäß § 1 Abs. 2 BDSG ist lediglich die Erhebung, Verarbeitung und Nutzung von Daten zu persönlichen und familiären Zwecken ausgeschlossen.

b) Gewährleistungsumfang

Der Gewährleistungsumfang der Norm ist es, den Schutzzweck des BDSG zu erfüllen. Dies beinhaltet den Schutz des Persönlichkeitsrechts des Einzelnen, nicht jedoch die sonstigen Interessen der verantwortlichen Stellen.[98] Der Schutz soll durch die Umsetzung technischer und organisatorischer Maßnahmen erfolgen. So soll präventiv durch die Gestaltung der Technik, der Schutz des Persönlichkeitsrechts bereits in der Planungs- und Gestaltungsphase datenverarbeitender Prozesse berücksichtigt und implementiert werden.[99] Die Anforderungen des Gesetzgebers werden insbesondere durch den Katalog in der Anlage zu § 9 S. 1 BDSG deutlich.

Die Begriffe der technischen und organisatorischen Maßnahmen sind dabei weit und umfassend zu verstehen und meinen alle Handlungen, Vorkehrungen und Regelungen, die notwendig sind, um eine datenschutzkonforme Erhebung, Verarbeitung und Nutzung personenbezogener Daten sicherzustellen, einschließlich Maßnahmen zur Gewährleistung eines ordnungsgemäßen Betriebsablaufs.[100] Aufgrund der stetigen technischen Entwicklung war auf einen konkreten Maßnahmenkatalog zu verzichten, selbst die Abgrenzung beider Begriffe ist nicht

96 Ernestus in Simitis, BDSG, § 9 Rn. 12; Schaffland/Wiltfang, BDSG, § 9 Rn. 13.

97 Ernestus in Simitis, BDSG, § 9 Rn. 12 ff.

98 Ernestus in Simitis, BDSG, § 9 Rn. 12 ff.

99 Ernestus in Simitis, BDSG, § 9 Rn. 16.

100 So auch Ernestus in Simitis, BDSG, § 9 Rn. 20 f.

möglich, eine Hilfestellung bezüglich möglicher Maßnahmen gibt hingegen die Anlage zu § 9 BDSG.[101]

c) Erforderlichkeit, § 9 Satz 2 BDSG

Welche Maßnahmen im konkreten Fall zu treffen sind, ist eine Frage der Erforderlichkeit (§ 9 S. 2 BDSG). Dieser Prüfung unterliegen jedoch nur Maßnahmen, die einzig § 9 BDSG unterliegen. Solche Maßnahmen, die bereits nach anderen Vorschriften zwingend vorgeschrieben sind, sind davon ausgeschlossen.[102]

aa) Verhältnismäßigkeit

Die Maßnahmen müssen in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen.[103] Dem Verhältnismäßigkeitsprinzip folgend, sind die milderen gleichgeeigneten Mittel einzusetzen.[104] Der erreichte Schutz ist mit dem dafür benötigten Aufwand abzuwägen. Die Wahrscheinlichkeit des Risikoeintritts, der mögliche Schadenumfang und die Schadenshöhe sind dabei zu berücksichtigen. Bei einem geringeren Schutzniveau, das mit geringerem Aufwand zu erreichen wäre, ist zu prüfen, ob dieses Schutzniveau noch für den angestrebten Schutzzweck ausreichend ist.[105] Je wichtiger der Schutzzweck und je höher das Risiko einer Verletzung des Persönlichkeitsrechts sind, umso mehr kann ein erhöhter Aufwand gerechtfertigt sein.[106] Das Schutzbedürfnis steigt mit den Nachteilen, die aus einer fehlerhaften Erhebung, Verarbeitung oder Nutzung personenbezogener Daten entstehen können und die dafür auch einen stark erhöhten Aufwand rechtfertigen.[107] Es muss auf jeden Fall sichergestellt werden, dass die Anforderungen der Rechtsvorschrift umgesetzt werden.[108]

---

101 Plath in Plath, BDSG, § 9 BDSG, Rn. 11.

102 Plath in Plath, BDSG, § 9 BDSG, Rn. 18; Gola/Schomerus, BDSG, § 9 Rn. 3.

103 Auernhammer, § 9 Rn. 5.

104 Ernestus in Simitis, BDSG, § 9 Rn. 44.

105 Ernestus in Simitis, BDSG, § 9 Rn. 23.

106 Ernestus in Simitis, BDSG, § 9 Rn. 38.

107 Ernestus in Simitis, BDSG, § 9 Rn. 41.

108 Gola/Schomerus, BDSG, § 9 Rn. 8.

bb) Schutzzweck

Die Prüfung hängt demzufolge auch vom Umfang und Stellenwert des Schutzzwecks ab. Der Schutzzeck des BDSG im Ganzen ist in § 1 Abs. 1 BDSG als Schutz des Einzelnen vor Beeinträchtigung seines Persönlichkeitsrechts durch Umgang mit seinen personenbezogenen Daten beschrieben. Darüber hinaus muss jedoch auch auf den jeweiligen Schutzweck der konkreten Norm abgestellt werden und dieser mit den Schutzmaßnahmen abgewogen werden.[109] Entscheidend ist das von der konkreten Erhebung, Verarbeitung oder Nutzung personenbezogener Daten verursachte Risiko für das Persönlichkeitsrecht. Dies hängt von der Sensitivität der personenbezogenen Daten ab.[110] Ebenso zu berücksichtigen sind die Art und Weise der Verarbeitung und des Umgangs mit den Daten sowie die Intensität der Verarbeitung, die Komplexität der Vorgänge, der Standard der Ausrüstung und der technischen Geräte, aber auch die beteiligten Personen, ihre Anzahl und damit auch die Seriosität des Verarbeiters.[111]

Es ist eine Prognose zu treffen, wie wahrscheinlich eine Verletzung des Persönlichkeitsrechts in welchem Schadensumfang ist. Bei unterschiedlichen Daten ist die Prüfung an den sensibelsten Daten auszurichten.[112]

cc) Aufwand

Auf Seiten des Verarbeiters sind der Nutzen und die Wichtigkeit der Daten zu berücksichtigen sowie ein evtl. öffentliches bzw. Allgemeininteresse an der Verarbeitung.[113]

---

109 Ernestus in Simitis, BDSG, § 9 Rn. 27.

110 Ernestus in Simitis, BDSG, § 9 Rn. 27; Schaffland/Wiltfang, BDSG, § 9 Rn. 35.

111 Grundsätzlich ebenso Ernestus in Simitis, BDSG, § 9 Rn. 27, 31; Schaffland/Wiltfang, BDSG, § 9 Rn. 5, 17.

112 Ernestus in Simitis, BDSG, § 9 Rn. 28.
So hat das VG Berlin in seinem Urteil vom 24.05.2011 – 1 K 133/10 entschieden, es sei unverhältnismäßig, von einem Arbeitsvermittler zu verlangen, die Übersendung personenbezogener Daten Arbeitssuchender an potenzielle Arbeitgeber zu verschlüsseln oder zu pseudonymisieren.

113 Ernestus in Simitis, BDSG, § 9 Rn. 30, 32.

§ 9 S. 2 BDSG stellt den Schutzzweck ins Verhältnis zum Aufwand, den die technischen und organisatorischen Maßnahmen erzeugen. Unter den Begriff des Aufwandes fallen sämtliche Kosten, die die technischen und organisatorischen Maßnahmen verursachen, angefangen bei der Planungsphase, über die Einführung der Maßnahmen bis hin zu den Betriebskosten – inklusive durch die Maßnahmen entstehenden Leistungseinbußen in der Verarbeitungskapazität.[114] Demzufolge sind Entwicklungs- und Investitionskosten in Technik, Soft- und Hardware sowie die Kosten für Verfahren und Abläufe und deren möglicher Mehraufwand miteinzurechnen.[115]

Unter den Aufwand fallen keine Kosten, die auch bei der Verarbeitung nichtpersonenbezogener Daten bei einer ordnungsgemäßen Datenverarbeitung entstehen wie notwendige Sicherungskosten.[116] Kosten, die aus wirtschaftlichen Motiven anfallen oder mit denen der Verarbeiter eigene Interessen verfolgt, sind dem Aufwand ebenfalls nicht zuzurechnen.[117] Positive wirtschaftliche Effekte, die sich aus den technischen und organisatorischen Maßnahmen ergeben, sind mit den Kosten zu verrechnen.[118]

dd) Rechtsfolgen

Die Aufsichtsbehörde kann bei fehlender oder unzureichender Umsetzung des § 9 BDSG gemäß § 38 Abs. 5 BDSG Maßnahmen zur Beseitigung technischer und organisatorischer Mängel treffen.[119] Davon ausgeschlossen sind lediglich Fälle nichtautomatisierter Datenverarbeitung.[120]

---

114 Ernestus in Simitis, BDSG, § 9 Rn. 34.

115 Ernestus in Simitis, BDSG, § 9 Rn. 34.

116 Ernestus in Simitis, BDSG, § 9 Rn. 36.

117 Ernestus in Simitis, BDSG, § 9 Rn. 36.

118 So auch Ernestus in Simitis, BDSG, § 9 Rn. 36.

119 Plath in Plath, BDSG, § 9 BDSG, Rn. 19.

120 OVG Hamburg, Urteil vom 07.07.2005 – 1 Bf 172/03.

d) Zwischenergebnis

§ 9 BDSG setzt den Prüfungsmaßstab für die praktische Umsetzung der Sicherung der Schutzgüter des BDSG. Die das Persönlichkeitsrecht natürlicher Personen tangierende Datenverarbeitung ist so anhand von § 9 BDSG zu kontrollieren. Davon betroffen ist nicht nur die Sicherung des Schutzes des Persönlichkeitsrechts im Allgemeinen, sondern ebenfalls der einzelnen datenschützenden Normen des BDSG im Speziellen. Die Vorgaben sind bereits in der Phase der Technikgestaltung zu berücksichtigen und bestehende Prozesse entsprechend zu überprüfen und anzupassen.

2. Anlage zu § 9 S. 1 BDSG

§ 9 S. 1 BDSG ist eine Anlage beigefügt, die die technischen und organisatorischen Maßnahmen von § 9 S. 1 BDSG um einen konkreten Maßnahmenkatalog erweitert. Sie bildet ein Mindestmaß an Anforderungen ab, das der Gesetzgeber zur Gewährleistung der Schutzgüter des BDSG für notwendig hält.[121] Der Verpflichtete muss dabei in eigener Verantwortung die Maßnahmen auswählen, die geeignet sind, einen entsprechenden Schutz personenbezogener Daten zu bieten.[122]

Grundsätzlich geht es um die Sicherung der Verfügbarkeit, Authentizität und Integrität der Datenverarbeitung.[123] Verfügbarkeit meint den Zugang und die Einsatzbereitschaft der technischen Systeme. Authentizität umfasst die nachvollziehbare Echtheit von Daten. Integrität bezieht sich auf die Zuverlässigkeit und Sicherung eines korrekten Umgangs, insbesondere in Bezug auf die Veränderung von Daten.[124]

---

121 Plath in Plath, BDSG, § 9 BDSG, Rn. 21.

122 Schaffland/Wiltfang, BDSG, § 9 Anh. 1 S. 3.

123 Gola/Schomerus, BDSG, § 9 Rn. 2.

124 Im Ergebnis auch Gola/Schomerus, BDSG, § 9 Rn. 2

a) Anwendungsbereich

Die Anlage setzt zunächst eine automatisierte Verarbeitung oder Nutzung personenbezogener Daten voraus. Dadurch dass § 9 BDSG inzwischen auch auf die Erhebung personenbezogener Daten anzuwenden ist, gilt dies ebenfalls für die Anlage, auch wenn die Erhebung nicht explizit genannt wird.[125] Für die nichtautomatisierte Datenverarbeitung ist die Anlage folglich nicht bindend, sie ist jedoch als Auslegungshilfe nicht unerheblich, verdeutlicht sie doch, welche Maßnahmen der Gesetzgeber grundsätzlich für umsetzbar und zumutbar hält.[126]

b) Organisationskontrolle

Abgestellt wird in Satz 1 der Anlage zu § 9 BDSG auf die Gestaltung der innerbetrieblichen oder innerbehördlichen Organisation, die den besonderen Anforderungen des Datenschutzes gerecht werden soll. Die Organisationskontrolle bildet das Leitmotiv der Regelung und soll mittels eines innerorganisatorischen Konzeptes den Datenschutz strukturell verbessern.[127] Angestrebt wird eine Harmonisierung und Verzahnung der einzelnen Maßnahmen, die aufeinander abgestimmt erst ein effektives Gesamtkonzept bilden. So soll verhindert werden, dass sich die Maßnahmen untereinander eliminieren oder durch mangelnde Abstimmung der Schutz verringert wird.[128]

Der Begriff der Organisation umfasst sowohl die Aufbau- als auch die Ablauforganisation.[129]

c) Maßnahmenkatalog

Der Maßnahmenkatalog bietet eine Hilfestellung in der Umsetzung wirksamer Datenschutzkonzepte. Aufgrund der technischen Entwicklung muss eine Be-

125 Ernestus in Simitis, BDSG, § 9 Rn. 59.

126 Wohl auch Ernestus in Simitis, BDSG, § 9 Rn. 59.

127 Plath in Plath, BDSG, § 9 BDSG, Rn. 25.

128 Schaffland/Wiltfang, BDSG, § 9 Rn. 43.

129 Ernestus in Simitis, BDSG, § 9 Rn. 50,; Schaffland/Wiltfang BDSG, § 9 Rn. 44.

rücksichtigung einzelner Punkte nicht zwingend sein, der Fokus ist vielmehr auf ein stimmiges Gesamtkonzept zu legen.[130]

aa) Zutrittskontrolle, Anlage zu § 9 BDSG Nr. 1

Nr. 1 der Anlage zu § 9 BDSG regelt die Zutrittskontrolle, wonach Unbefugten der Zutritt *„zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren"* ist.

Zweck der Regelung ist es zu verhindern, dass unbefugte von personenbezogenen Daten Kenntnis erhalten können oder auf diese in irgendeiner Weise einwirken können.[131] Jeder Adressat der Norm trägt dabei für seinen Herrschaftsbereich die Verantwortung.[132] Bei einer Auftragsdatenverarbeitung trägt damit der Auftragnehmer für seinen Herrschaftsbereich die Verantwortung.[133]

DIN 44300 definiert Datenverarbeitungsanlagen als die Gesamtheit der Baueinheiten, aus denen eine Funktionseinheit zur Verarbeitung von Daten aufgebaut ist.[134] Dazu zählen Digital-Kameras, Kopiergeräte mit Festplatten, moderne Faxgeräte mit eingebauten Speichern, Kombigeräte wie Handys oder PDAs, insbesondere jedoch Geräte, mit denen Daten automatisiert verarbeitet werden können, wie Computer – einschließlich von Monitoren, Druckern, Scannern, Tastaturen, „Mäusen" – oder (Chipkarten-)Lesegeräte.[135] Zu Datenverarbeitungsanlagen gehören auch die Leitungen, soweit der Verarbeiter auf diese zugreifen kann.[136] Es kann verhältnismäßig sein, dass der Verarbeiter eine Zugriffsmöglichkeit schaffen muss.[137] Parallel dazu sind Funknetze (WLAN) ebenfalls Teil von

130 Plath in Plath, BDSG, § 9 BDSG, Rn. 28.

131 Ernestus in Simitis, BDSG, § 9 Rn. 68.

132 Schaffland/Wiltfang, § 9 BDSG, Anh. 1 S. 3.

133 Schaffland/Wiltfang, § 9 BDSG, Anh. 1 S. 3.

134 DIN Norm 44300 zitiert in Ernestus in Simitis, BDSG, § 9 Rn. 72.

135 Ernestus in Simitis, BDSG, § 9 Rn. 72, 75.

136 Ähnlich Ernestus in Simitis, BDSG, § 9 Rn. 73.

137 Ähnlich Ernestus in Simitis, BDSG, § 9 Rn. 73.

Datenverarbeitungsanlagen, für deren ausreichenden Schutz die verantwortliche Stelle durch geeignete Verschlüsselungsmaßnahmen sorgen muss.[138] Nicht angeschlossene Datenträger sind kein Teil der Datenverarbeitungsanlage.[139]

„Unter Zutritt ist die räumliche Annäherung einer natürlichen Person zu verstehen."[140] Die Sicherheitsvorkehrungen sind dabei so zu gestalten, dass die Möglichkeit einer Kenntnisnahme oder Einwirkung unbefugter Personen auf die Datenverarbeitungsanlagen verhindert wird. In Betracht kommen unter anderem Formen des inneren und äußeren Gebäudeschutzes, wie automatisierte Kontrolleinrichtungen, Zugangssicherungssysteme, der „Closed-Shop-Betrieb" oder Formen der Überwachung.[141] Der zunehmende Einsatz mobiler Geräte und die Möglichkeiten der räumlichen Entkopplung einzelner Arbeitsschritte, fortschreitende Dezentralisierung und Vernetzung stellen die Effizienz und Funktionsfähigkeit der Zutrittskontrolle vor neue Herausforderungen. Diese Entwicklung darf jedoch nicht zu einer Schwächung des Sicherheitsniveaus führen, weswegen hier das gleiche Schutzniveau aufrechtzuerhalten ist. Die Maßnahmen können sich in der Art und Weise unterscheiden, haben jedoch die entsprechende Kontroll- und Sicherheitsdichte sicherzustellen.[142] In Frage kommen komplexe, regelmäßig wechselnde Passwörter, Zugänge über Chipkarten, automatische „log-offs" oder Sicherheitsschlösser.[143]

Die Zutrittsberechtigungen sind genau festzulegen und – soweit notwendig – gestuft, von der Funktion abhängig und auf diese zugeschnitten, zu erteilen.

---

138 Ernestus in Simitis, BDSG, § 9 Rn. 73.

139 Ernestus in Simitis, BDSG, § 9 Rn. 73.

140 Ernestus in Simitis, BDSG, § 9 Rn. 77.

141 Ernestus in Simitis, BDSG, § 9 Rn. 81, Bergmann/Möhrle/Herb, Datenschutzrecht, Anlage zu § 9 BDSG 01; Weitere genauere Beispiele für mögliche Maßnahmen in Ernestus in Simitis, BDSG, § 9 Rn. 83. Eine ausführliche Liste ist zu finden bei Bergmann/Möhrle/Herb, Datenschutzrecht, Anlage zu § 9 BDSG 01.

142 Im Ergebnis auch Ernestus in Simitis, BDSG, § 9 Rn. 85 f.

143 Ernestus in Simitis, BDSG, § 9 Rn. 84 ff.

bb) Zugangskontrolle, Anlage zu § 9 BDSG Nr. 2

Nach der Zugangskontrolle, Anlage zu § 9 BDSG Nr. 2 gilt es *„zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können"*.

Eine unbefugte Nutzung von Datenverarbeitungssystemen – in Abgrenzung zu Datenverarbeitungsanlage – steht hier im Mittelpunkt der Regelung.

Gemäß DIN 44300 Nr. 99 ist ein *„Datenverarbeitungssystem eine Funktionseinheit zur Verarbeitung von Daten"*.[144] Damit geht es um einen Gesamtzusammenhang von Daten, Hardware und insbesondere Software.[145] Mit der Zugangskontrolle wird weniger eine räumliche als vielmehr jegliche „Annäherung" in den Fokus gerückt, insbesondere der technisch-organisatorische Zugang.[146] Davon umfasst ist ebenfalls die Datenübertragung via Internet.[147] Die Möglichkeit der Steuerung und des Einwirkens auf das Datenverarbeitungssystem ist bereits ausreichend und soll nur durch einen kontrollierten und genehmigten Zugang erfolgen.[148] Dafür muss exakt festgelegt werden, wer inwieweit auf welche Teile des Systems unter welchen Bedingungen zugreifen darf.[149]

Unbefugt ist demzufolge eine Person, die keine oder keine ausreichende Zugangsberechtigung für die Nutzung des Datenverarbeitungssystems als Ganzes oder einzelner Komponenten, Verarbeitungsschritte, Software oder Daten hat.

Potenzielle Gefahren für das Datenverarbeitungssystem sind, soweit möglich, auf dem neuesten Stand der Technik vorab zu prognostizieren, um das System entsprechend zu gestalten. Mögliche Maßnahmen sind Verfahren zur Identifizierung und Authentifikation, wie die Vergabe von Passwörtern, IDs und Zugangsberechtigungen, weiterhin die Protokollierung der Vorgänge und deren

144 Ernestus in Simitis, BDSG, § 9 Rn. 90.

145 Ernestus in Simitis, BDSG, § 9 Rn. 90.

146 Schaffland/Wiltfang, § 9 BDSG, Anh. 1 S. 4; Ernestus in Simitis, BDSG, § 9 Rn. 89.

147 Ernestus in Simitis, BDSG, § 9 Rn. 89.

148 Ernestus in Simitis, BDSG, § 9 Rn. 91.

149 Ernestus in Simitis, BDSG, § 9 Rn. 94.

Auswertung, Sanktionen, Verschlüsselungen, abgeschottete Netzwerke.[150] Insbesondere bei Personalcomputern kommen spezielle Sicherheitssoftware, Antivirusprogramme und Firewalls in Betracht.[151]

cc) Zugriffskontrolle, Anlage zu § 9 BDSG Nr. 3

Gemäß Nr. 3 der Anlage zu § 9 BDSG ist *„zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können“*.

Im Fokus der Regelung steht eine datenschutzgerechte Benutzung und Sicherung der Datenverarbeitungssysteme durch Berechtigte, indem man ihre Zugriffsrechte exakt festlegt und entsprechend überwacht und durchsetzt. Damit soll sichergestellt werden, dass Berechtigte auch nur auf die Datensätze zugreifen können, für die sie eine Berechtigung besitzen.[152]

Fraglich erscheint, ob diese Regelung nicht zu eng gefasst ist und ebenfalls die Präzisierung der Zugriffsrechte auf bestimmte Funktionen – wie Eingeben, Lesen, Kopieren, Verändern, Weiterleiten – eines Datenverarbeitungssystems umfassen sollte, da auch ohne den Zugriff auf eine bestimmte Datei Ihre Aussage- und Informationskraft durch das Hinzufügen, Verändern oder Löschen anderer Dateien mitverändert werden kann.[153]

Die zunehmenden Möglichkeiten, Datensätze miteinander zu verknüpfen und daraus neue Aussagen, Profile und Informationen zu gewinnen, lassen die isolierte Betrachtung einzelner Daten nicht mehr zu. Der Datenschutz ist hier systematisch zu betrachten, um alle Gefahren einer umfassenden automatisierten Datenverarbeitung für das Persönlichkeitsrecht des Einzelnen zu erfassen und

150 Ernestus in Simitis, BDSG, § 9 Rn. 97 f.; Bergmann/Möhrle/Herb, Datenschutzrecht, Anlage zu § 9 BDSG 01, dort findet sich auch eine ausführliche Liste mit Maßnahmen.

151 Ernestus in Simitis, BDSG, § 9 Rn. 97 f.

152 Schaffland/Wiltfang, BDSG, § 9 Rn. 78.

153 Ernestus in Simitis, BDSG, § 9 Rn. 101.

deren Risiko zu minimieren. Damit sollte umfassend der Zugriff auf das gesamte Datenverarbeitungssystem inklusive aller Funktionen betrachtet werden.

Der Begriff des Datenverarbeitungssystems ist wie in Nr. 2 zu verstehen.[154]

„Zugriff ist der Zugang zu den personenbezogenen Daten zum Zwecke ihrer Verwendung."[155] Dies umfasst jegliche Wahrnehmung, Erfassung, Verarbeitung oder Nutzung von Daten, auch ihre Verknüpfung innerhalb eines Datenverarbeitungssystems.[156]

Schutzmaßnahmen um den Zugriff Unbefugter zu verhindern, können auch hier Protokollierungen und deren Auswertung, IDs und Formen von Sperren und Chiffrerungen sein, eine entsprechend sichere Organisation des Archivs und der Datenträgerverwaltung, bei Personalcomputern insbesondere eine lückenlose Menüsteuerung oder eine benutzerspezifisch abgestufte Rechteverwaltung.[157]

dd) Weitergabekontrolle, Anlage zu § 9 BDSG Nr. 4

Die Weitergabekontrolle gemäß der Anlage zu § 9 BDSG Nr. 4 soll *„gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist"*.

Die Regelung stellt den Vorgang der Übertragung in den Mittelpunkt, um den Schutz personenbezogener Daten während sämtlicher Weitergabeprozesse zu gewährleisten. Davon umfasst ist ebenfalls eine Weitergabe im Rahmen der

154 Ernestus in Simitis, BDSG, § 9 Rn. 102.

155 Ernestus in Simitis, BDSG, § 9 Rn. 103.

156 Ernestus in Simitis, BDSG, § 9 Rn. 103.

157 Bergmann/Möhrle/Herb, Datenschutzrecht, Anlage zu § 9 BDSG 01. Hier findet sich auch ein ausführlicher Maßnahmenkatalog. Ein umfassender Maßnahmenkatalog ist ebenfalls zu finden bei Ernestus in Simitis, BDSG, § 9 Rn. 108.

Auftragsdatenverarbeitung zwischen den Beteiligten.[158] Es sind Maßnahmen zu treffen, die den Übertragungsweg sichern. Dies umfasst den elektronischen Übertragungsweg, wie auch eine „physische Weitergabe".[159] Zu möglichen Maßnahmen zählen Verschlüsselungen oder Signaturen.[160] Bei Personalcomputern können weitere Schutzmaßnahmen zum Schutz der lokalen Festplatten sowie der Verzicht von „Network File Systemen" hinzukommen.[161]

Weiterhin soll die Sicherheit durch die Möglichkeit gesteigert werden, die Übermittlungsvorgänge nachvollziehen und überprüfen zu können. Der Begriff der Übermittlung ist in § 3 Abs. 4 Nr. 3 BDSG bereits legaldefiniert (siehe I. Nr. 3.), d), cc)).

Die Datenverarbeitungssysteme sind so auszugestalten, dass ein möglicher Empfängerkreis festgelegt werden kann und auch nachvollziehbar festgelegt wird. Weiterhin können begrenzte Kommunikations- bzw. Übermittlungskanäle eingerichtet werden, über die einzig eine Übertragung möglich sein kann. Bei der Übermittlung sensitiver Daten kann, über den Wortlaut der Norm hinaus, eine Protokollierung der Vorgänge verhältnismäßig sein, wenn nur dadurch ein ausreichender Schutz gewährleistet werden kann.[162] Weitere Maßnahmen können fortwährend aktualisierte Übersichten und Dokumentationen mit Zeitspannen und Zugriffsrechten, beteiligten Personen sowie der angewendeten Software und der benutzten Hardware sein.[163]

Die Vorgänge müssen für Dritte, ggf. externe Kontrollen und Aufsichtsbehörden nachvollziehbar sein.[164] Die Dauer der Archivierungspflicht richtet sich nach

---

158 Bergmann/Möhrle/Herb, Datenschutzrecht, Anlage zu § 9 BDSG 01, S. 26; Schaffland/Wiltfang, BDSG, § 9 Rn. 112.

159 Bergmann/Möhrle/Herb, Datenschutzrecht, Anlage zu § 9 BDSG 01, S. 26.

160 Ernestus in Simitis, BDSG, § 9 Rn. 11. Ein ausführlicher Maßnahmenkatalog findet sich bei Bergmann/Möhrle/Herb, Datenschutzrecht, Anlage zu § 9 BDSG 01, S. 26 ff.

161 Ernestus in Simitis, BDSG, § 9 Rn. 127.

162 Ernestus in Simitis, BDSG, § 9 Rn. 118.

163 Ernestus in Simitis, BDSG, § 9 Rn. 126.

164 Ernestus in Simitis, BDSG, § 9 Rn. 123 f.

der Wichtigkeit der Daten sowie ggf. nach vorliegenden gesetzlichen Aufbewahrungspflichten.[165]

ee) Eingabekontrolle, Anlage zu § 9 BDSG Nr. 5

Die Eingabekontrolle gemäß der Anlage zu § 9 BDSG Nr. 5 soll *„gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind"*.

Durch die Nachvollziehbarkeit der „Einspeisung" personenbezogener Daten in das Datenverarbeitungssystem soll ihre Richtigkeit sichergestellt werden. Dies geschieht durch die Verbindung des Vorgangs der Eingabe mit der individualisierten Person, die den Vorgang durchführt, wodurch es zu einer persönlichen Verantwortung kommt.[166] Die in Verantwortung stehende Person muss eindeutig, zum Beispiel durch eine Nutzerkennung, identifizierbar sein.[167] Es muss dabei ausgeschlossen sein, dass eine andere Person, wie ein Systemadministrator oder ein Vorgesetzter, den bestimmten Vorgang unter der Kennung durchgeführt hat.[168]

Dies kann durch eine Protokollierung des Zeitpunkts, des vollständigen Datums, des Vorgangs sowie der verarbeitenden Person erfolgen.[169] Weitere Maßnahmen können die Protokollierung der Admin-Aktivitäten, Dokumentationen der Programme und Programmversionen sein.[170] Bei Personalcomputern kommt darüber hinaus die Protokollierung sämtlicher Nutzer und Systemverwalter in

165 Ernestus in Simitis, BDSG, § 9 Rn. 123 f.

166 Ernestus in Simitis, BDSG, § 9 Rn. 135.

167 Ernestus in Simitis, BDSG, § 9 Rn. 135 ff.

168 Ernestus in Simitis, BDSG, § 9 Rn. 135 ff.

169 Ernestus in Simitis, BDSG, § 9 Rn. 131, 134. Ein ausführlicher Maßnahemnkatalog findet sich bei Bergmann/Möhrle/Herb, Datenschutzrecht, Anlage zu § 9 BDSG 01, S. 29.

170 Ernestus in Simitis, BDSG, § 9 Rn. 144 f.

Frage.[171] Die Protokolldatei muss – insbesondere im Hinblick auf Ihre Größe und Aussagekraft – auswertbar sein.[172]

Ein Problem stellt die Überprüfbarkeit der Entfernung bestimmter personenbezogener Daten dar. Protokolliert man den Dateninhalt, so läuft man dem Sinn und Zweck des Entfernens entgegen, hier sollten identifizierende Merkmale des Datensatzes ausreichen[173].

ff) Auftragskontrolle, Anlage zu § 9 BDSG Nr. 6

Die Auftragskontrolle gemäß Nr. 6 der Anlage zu § 9 BDSG soll *„gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können“*.

Die Regelung stellt eine „Auftragsbindung“ des Verarbeiters an die Weisungen des Auftraggebers in Bezug auf die Art und Weise der Verarbeitung her. Die Norm wirkt damit parallel zu einer Zweckbindung bei personenbezogenen Daten. Sie ergänzt dabei die Regelungen zur Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag aus § 11 BDSG, indem sie den Schwerpunkt auf den Auftragnehmer legt, der erteilte Weisungen exakt umzusetzen hat.[174] Dies setzt voraus, dass der Auftraggeber präzise Weisungen erteilt. Um die Nachvollziehbarkeit sicherzustellen, sollten die Weisungen schriftlich erfolgen, standardisierte Formulare können zu einer Systematisierung der Befehle und ihrer Eindeutigkeit beitragen.[175]

Es sollen auch „nur“ die erteilten Weisungen umgesetzt werden. Dies bedeutet, dass personenbezogene Daten durch niemandem – weder Mitarbeiter noch Dritte – außer der berechtigten Person und nur in der vorgeschriebenen Art und Weise bearbeitet werden dürfen.[176]

---

171 Ernestus in Simitis, BDSG, § 9 Rn. 144 f.

172 Ernestus in Simitis, BDSG, § 9 Rn. 132.

173 Ernestus in Simitis, BDSG, § 9 Rn. 132.

174 Ernestus in Simitis, BDSG, § 9 Rn. 146 f.

175 Im Ergebnis auch Ernestus in Simitis, BDSG, § 9 Rn. 148 ff.

176 So auch Ernestus in Simitis, BDSG, § 9 Rn. 153.

Der Auftraggeber hat den Auftragnehmer sorgfältig auszuwählen, er hat mit ihm den datenschutzrechtlichen Rahmen festzulegen und entsprechend bei einer Verletzung von Sicherungsmaßnahmen Vertragsstrafen festzulegen.[177]

gg) Verfügbarkeitskontrolle, Anlage zu § 9 BDSG Nr. 7

Die Verfügbarkeitskontrolle gemäß Nr. 7 der Anlage zu § 9 BDSG, soll *„gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind"*.

Geschützt werden soll damit vor der physischen Zerstörung der Geräte, wenngleich dies einen Schutz sowohl der Hardware als auch der Software beinhaltet. Der Schutz vor zufälligen Zerstörungen beinhaltet nicht vorhersehbare Ereignisse wie Stromausfälle, Wassereinbrüche oder Blitzeinschläge.[178] Maßnahmen können im Einzelnen gesicherte Stromanschlüsse, die galvanische Trennung von Netzwerkanschlüssen oder Batteriepufferungen sein.[179]

Gesichert werden sollen die Funktionsfähigkeit der Verarbeitung sowie die Datenbestände an sich, deren Rekonstruktion möglich sein muss.[180] Es darf dabei nicht zu einem Verlust der personenbezogenen Daten kommen. Dafür sind Sicherheitskopien zu erstellen, deren Taktung von der Sensitivität der Daten abhängt.

hh) Gewährleistung der Zweckbindung, Anlage zu § 9 BDSG Nr. 8

Die Gewährleistung der Zweckbindung gemäß Nr. 8 der Anlage zu § 9 BDSG soll sicherstellen, *„dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können"*.

---

177 Bergmann/Möhrle/Herb, Datenschutzrecht, Anlage zu § 9 BDSG 01, S. 31 ff.; weiterhin findet sich hier ein ausführlicher Maßnahmenkatalog.

178 Ernestus in Simitis, BDSG, § 9 Rn. 156.

179 Ernestus in Simitis, BDSG, § 9 Rn. 156.

180 Bergmann/Möhrle/Herb, Datenschutzrecht, Anlage zu § 9 BDSG 01, S. 34 f. Hier findet sich auch eine ausführliche Übersicht möglicher Maßnahmen.

Das Trennungsverbot der Verarbeitung unterschiedlich bestimmter Daten stellt einen Beitrag zum Systemdatenschutz dar.[181] Die Regelung verfolgt dabei den Privacy-by-Design-Ansatz, den Schutz personenbezogener Daten bereits bei der Gestaltung der Datenverarbeitungssysteme zu verankern, indem man sie von vornherein so gestaltet, dass eine getrennte Verarbeitung unterschiedlicher bzw. anders bestimmter Datensätze ermöglicht wird.

Mögliche Maßnahmen um dies zu erreichen, können die Speicherung der Daten in physikalisch getrennten Datenbanken, unterschiedliche Verschlüsselungen und Signaturen sein.[182]

ii) Verschlüsselungsverfahren, Anlage zu § 9 BDSG Satz 3

„Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren." Satz 3 der Anlage zu § 9 BDSG erwähnt die Verschlüsselungstechnik als besondere Maßnahme und hebt diese als einzige gesondert hervor. Verschlüsselungsverfahren kommen als Maßnahme bei der Zugangs-, der Zugriffs- und der Weitergabekontrolle in Betracht.[183] Der Gesetzgeber trägt mit der Regelung der wachsenden Bedeutung des Internets für die Verarbeitung personenbezogener Daten, insbesondere deren Übertragung und den damit verbundenen Gefahren Rechnung.[184]

Der Begriff der Verschlüsselung ist nicht im BDSG legaldefiniert. Eine Definition findet sich im Landesdatenschutzgesetz von Mecklenburg-Vorpommern, dort heißt es in § 3 Abs. 4 Nr. 10, Verschlüsseln sei *„das Verändern personenbezogener Daten derart, dass ohne Entschlüsselung die Kenntnisnahme des Inhaltes der Daten nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist"*. Unter Verschlüsselung im technischen Sinn versteht man *„den Vorgang, bei dem ein klar lesbarer Text (Klartext) oder auch Informationen anderer Art wie Ton- oder Bildaufzeichnungen mit Hilfe*

---

181 Ernestus in Simitis, BDSG, § 9 Rn. 160.

182 Ein ausführlicher Maßnahmenkatalog ist zu finden bei Ernestus in Simitis, BDSG, § 9 Rn. 163.

183 Ernestus in Simitis, BDSG, § 9 Rn. 164 f.

184 Ernestus in Simitis, BDSG, § 9 Rn. 165.

eines Verschlüsselungsverfahrens (Kryptosystem) in eine „unleserliche", das heißt nicht einfach interpretierbare Zeichenfolge (Geheimtext) umgewandelt wird."[185]

Über die Art der Verschlüsselung gibt das Gesetz keine Auskunft, wobei diese dem Stand der Technik entsprechen soll. Unter Stand der Technik versteht die europäische Norm EN 45020 ein *„entwickeltes Stadium der technischen Möglichkeiten zu einem bestimmten Zeitpunkt, soweit Produkte, Prozesse und Dienstleistungen betroffen sind, basierend auf entsprechenden gesicherten Erkenntnissen von Wissenschaft, Technik und Erfahrung"*.[186] Die Sicherheitstechnik steht in einem ständigen Wettbewerb, immer neue weiterentwickelte Angriffe auf sie mit neuen technischen Lösungen abzuwehren. Deswegen spielt besonders bei der Verschlüsselungssoftware ihr aktueller Stand – gemessen am Bedrohungspotenzial – eine besondere Rolle. Bei dem Anforderungsprofil an das Schutzniveau sind das Risiko, die Sensibilität der Daten sowie die bei dem Verfahren entstehenden Kosten unter Verhältnismäßigkeitsgesichtspunkten in Einklang zu bringen.[187]

d) Zwischenergebnis

Der Maßnahmenkatalog der Anlage zu § 9 BDSG ist nicht abschließend. Für einen effektiven Datenschutz kann er das bei der rasanten Entwicklung der Technik auch gar nicht sein. Trotzdem bietet er jedoch eine konkrete Handreichung, anhand derer Maßnahmen im Bereich der Datenverarbeitung überprüft und gegebenenfalls angepasst werden müssen.

Die Vorgaben des § 9 BDSG sind entsprechend bei der gesamten Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Bereich der postalischen Lieferkette zu beachten und umzusetzen. Dafür ist jeder einzelne Verarbeitungsschritt auf ausreichenden Schutz personenbezogener Daten hin zu überprüfen.

---

185 Ernestus in Simitis, BDSG, § 9 Rn. 166.

186 CEN: Zitat aus DIN EN 45020:2006 – Normung und damit zusammenhängende Tätigkeiten – Allgemeine Begriffe (ISO/IEC Guide 2:2004); dreisprachige Fassung EN 45020:2006 zitiert aus Ernestus in Simitis, BDSG, § 9 Rn. 172.

187 Im Ergebnis aus Ernestus in Simitis, BDSG, § 9 Rn. 171.

3. Privacy by Design

Um dem Datenschutz möglichst effektiv zur Geltung zu verhelfen, soll dieser nicht nur reaktiv bzw. nachträglich in bereits bestehende Systeme implementiert werden, sondern bereits in der Modellierungsphase technischer Prozesse und Abläufe berücksichtigt werden.[188]

Einen Ansatz, den Datenschutz in Prozessen automatisierter Datenverarbeitung zu verankern, stellt „Privacy by Design" dar, das sieben Grundsätze für die Implementierung des Datenschutzes aufstellt.

Privacy by Design meint dabei die Einbeziehung datenschutzrechtlicher Probleme in die Entwicklung neuer Technologien und technischer Systeme und soll so von vornherein eine datenschutzkonforme Erarbeitung solcher Gesamtkonzepte sicherstellen.[189]

a) Grundsätze

Folgende sieben Grundsätze sollen den Privacy-by-Design-Ansatz umsetzen.

(1) Proactive not Reactive; Preventative not Remedial

Im Vordergrund steht eine proaktive beratende Tätigkeit sowie die Einbeziehung von Datenschutzbeauftragten, soweit möglich/nötig. Der Grundsatz ist als Aufforderung zu verstehen, datenschutzrechtliche Überlegungen bereits in der Planungsphase miteinzubeziehen.[190]

(2) Privacy as Default

Der maximale Schutz der Privatsphäre ist gegeben, wenn in der Grundeinstellung keine personenbezogenen Daten verarbeitet werden dürfen und eine Person

---

188 So auch Schaar, Peter, Privacy by Design in Identity in the Information Society, Quelle: http://www.bfdi.bund.de/SharedDocs/Publikationen/EN/0610EUPrivacyByDesign.pdf?__blob=publicationFile, S. 5.

189 Schaar, Peter, Privacy by Design in Identity in the Information Society, http://www.bfdi.bund.de/SharedDocs/Publikationen/EN/0610EUPrivacyByDesign.pdf?__blob=publicationFile, S. 1.

190 Rost, Martin/Bock, Kirsten, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31); Cavoukian, Ann, Privacy by Design, The 7 Foundational Principles, Nr. 1.

davon ausgehen kann, dass ihre Privatsphäre sicher und intakt bleibt, solange sie von sich aus nichts unternimmt.[191] Dieser Grundsatz steht in einem engen Zusammenhang mit den Global Privacy Standards, „Collection Limitation" und „Use, Retention, and Disclosure Limitation".[192]

(3) Privacy Embedded into Design

Die Ganzheitlichkeit der technischen Lösungen wird betont.[193] Der Schutz der Privatsphäre soll in die Systeme eingebaut werden, ohne deren Funktionalität zu beeinträchtigen.[194]

(4) Full Functionality – Positive Sum, not Zero-Sum

Ziel ist, eine Win-Win-Situation zwischen den verschiedenen Interessen, etwa der Funktionalität oder Datensicherheit auf der einen und der Privatsphäre auf der anderen Seite, herzustellen.[195]

(5) End-to-End-Security – Lifecycle Protection

Der gesamte Lebenszyklus eines IT-Prozesses ist von seinem Anfang bis zu seinem Ende zu betrachten, um die Privatsphäre effektiv über den gesamten Prozess hinweg zu schützen.[196] Hier spielt besonders der Global Privacy Standard der Security eine entscheidende Rolle.[197]

---

191 Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31).

192 Cavoukian, Privacy by Design, The 7 Foundational Principles, Nr. 2.

193 Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31).

194 Cavoukian, Privacy by Design, The 7 Foundational Principles, Nr. 3; Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31).

195 Ähnlich auch Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31); Cavoukian, Privacy by Design, The 7 Foundational Principles, Nr. 4.

196 Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31); Cavoukian, Privacy by Design, The 7 Foundational Principles, Nr. 5.

197 Cavoukian, Privacy by Design, The 7 Foundational Principles, Nr. 5.

(6) Visibility and Transparency

Transparenz stellt eine Voraussetzung für die Prüfbarkeit bzw. Prüffähigkeit der Prozesse und technischen Systeme im Hinblick auf die Verarbeitung personenbezogener Daten dar.[198] Sie steht in einem Wechselwirkungsverhältnis mit den Grundsätzen „Accountability", „Openness" und „Compliance".[199]

(7) Respect for User Privacy

Der Respekt vor der Privatsphäre der Nutzer beinhaltet neben seiner Appellfunktion den Anspruch, Techniken nutzerzentriert auszugestalten.[200] Er steht so ebenfalls in einem engen Verhältnis zu den Global Privacy Standards.[201]

b) Zwischenergebnis

Die Privacy-by-Design-Grundsätze stellen ein Sediment an Erfahrungen für einen effektiven, sicheren und datenschutzgerechten Umgang mit personenbezogenen Daten dar.[202]

4. Global Privacy Standards

Die Global Privacy Standards sollen einen Rahmen für den Umgang mit personenbezogenen Daten bei der automatisierten Datenverarbeitung schaffen.

198 Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31); Cavoukian, Privacy by Design, The 7 Foundational Principles, Nr. 6.

199 Cavoukian, Privacy by Design, The 7 Foundational Principles, Nr. 6.

200 Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31).

201 Im Ergebnis auch Cavoukian, Privacy by Design, The 7 Foundational Principles, Nr. 7.

202 Ähnlich auch Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30.

a) Grundsätze

Consent

Eine übereinstimmende Einigung aller Beteiligten soll Voraussetzung für die Sammlung und Nutzung von Daten sein.[203] In Deutschland korrespondiert die Einwilligung gemäß § 4a BDSG mit diesem Grundsatz.

Accountability

Bei der Verarbeitung personenbezogener Daten sollen Prozesse zurechenbar und verantwortlich sowie haftbar ausgestaltet sein.[204]

Purposes

Eine Zweckbindung der Anforderungen soll im Verfahren berücksichtigt werden.[205] Dieser Grundsatz wurde im unionalen und im nationalen Datenschutzrecht umgesetzt.

Collection Limitation

Die Sammlung von Daten hat nach den Grundsätzen der Datensparsamkeit und Erforderlichkeit fair, begrenzt und rechtskonform zu geschehen.[206] Die Grundsätze der Datenvermeidung und Datensparsamkeit in § 3a BDSG greifen diesen Gedanken auf.

Use, Retention and Disclosure Limitation

Mit „Use, Retention and Disclosure Limitation" werden Anforderungen bzgl. der Nutzung, Speicherung und Weitergabe von Daten aufgestellt.[207] Das BDSG

---

203 Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31).

204 Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31).

205 Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31).

206 Schaar, Privacy by Design in Identity in the Information Society, http://www.bfdi.bund.de/SharedDocs/Publikationen/EN/0610EUPrivacyByDesign.pdf?__blob=publicationFile, S. 13; Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31).

207 Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31).

hat diesen Grundsatz insoweit umgesetzt, als dass es für jeden einzelnen Verarbeitungsschritt eine eigene Ermächtigung gibt, die einzeln untersucht wird.

Accuracy

Daten sollen korrekt hinsichtlich des Verarbeitungszwecks sein.[208]

Security

Die Datensicherheit muss entsprechend internationalen Standards gewährleistet sein.[209]

Openness

Der Zugang zu Leitlinien und Arbeitspraktiken hinsichtlich des IT-Betriebs stellt eine Voraussetzung für Transparenz, Verantwortbarkeit und Zurechenbarkeit dar.[210]

Access

Betroffene Personen sollen Zugriff auf ihre Daten bekommen und über ihre Verwendung informiert werden.[211]

Compliance

Compliance meint in diesem Zusammenhang, dass die notwendigen Schritte unternommen werden, um Prozesse, Leitlinien und Grundsatze bezüglich des Schutzes der Privatsphäre zu überwachen und zu bewerten.[212]

---

208 Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31).

209 Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31).

210 Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31); so auch Schaar, Privacy by Design in Identity in the Information Society, Quelle: http://www.bfdi.bund.de/SharedDocs/Publikationen/EN/0610EUPrivacyByDesign.pdf?__blob=publicationFile, S. 13.

211 Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31).

212 Schaar, Privacy by Design in Identity in the Information Society, Quelle: http://www.bfdi.bund.de/SharedDocs/Publikationen/EN/0610EUPrivacyByDesign.pdf?__blob=publicationFile, S. 5; Rost/Bock, Privacy by Design und die Neuen Schutzziele in DuD 2011, S. 30 (31).

b) Zwischenergebnis

In Zeiten sich schnell verändernder Technik kann das Datenschutzrecht allein kaum optimale Sicherheit und einen umfassenden Datenschutz gewährleisten. Dazu ist es notwendig, in die Entwicklung der technischen Abläufe und Verfahren Datenschutzüberlegungen von Anfang an mit einzubeziehen und Systeme entsprechend auszugestalten.[213] Die Grundsätze des Privacy by Design und die Global Privacy Standards bilden den Rahmen, um Datenverarbeitung datenschutzgerecht auszugestalten.

VII. Zwischenergebnis

Das Datenschutzrecht bildet einen Rahmen für die Verarbeitung personenbezogener Daten. Inzwischen hat sich durch eine enge Verzahnung von nationalem und unionalem Recht sowie durch die Rechtsprechung der Gerichte, die Forschung und insbesondere die Arbeit der Datenschutzbeauftragten ein detailliertes Netz aus Grundsätzen, Rechtsgrundlagen und Definitionen gebildet, das bei der Gestaltung von Datenverarbeitungsprozessen beachtet werden muss.

[213] Ähnlich Bizer, Datenschutz als Gestaltungsaufgabe in DuD 2007, S. 725 (727).

B. Postrecht

„Es bleibet also das förmliche Post-Wesen allerdings eine Taxische Erfindung, welche gantz erstaunliche Folgen nach sich gezogen und die Welt in manchen Sachen fast in einen andern Model gegossen hat [...] " (Moser, Teutsches Staatsrecht, Theil 5).[214]

I. Einführung

Als Teil des öffentlichen Rechts lassen sich am Postrecht konzentriert die Veränderungen des öffentlichen Rechts im Allgemeinen ablesen. Die Einflüsse und Vorgaben des europäischen Rechts, sich verändernde Wirtschaftsstrukturen, wie die Privatisierung ganzer Wirtschaftszweige, die bisher von staatlicher Seite bewirtschaftet wurden, sowie zunehmender Wettbewerb und neue Kommunikationsformen haben in ein althergebrachtes erprobtes Rechtsgebiet viel Bewegung gebracht.

1. Historische Einordnung

Die Geschichte der Post in Deutschland beginnt im Heiligen Römischen Reich Deutscher Nationen mit der Zusammenarbeit des Hauses Habsburg mit dem Haus Taxis, das zwischen den habsburgischen Landen regelmäßige Postverbindungen aufbaute.[215] Kaiser Rudolph II. beanspruchte 1595 das Postwesen als kaiserliches Regal und übertrugt die Verantwortung Leonhard von Taxis, der zum Generalpostmeister ernannt wurde und das Postnetz größtenteils in eigener wirtschaftlicher Verantwortung betrieb.[216] Mit der Gründung des Norddeutschen Bundes 1867 wurden die sich auf diesem Gebiet befindenden selbstständigen

---

214 Vgl. Poststammbuch, S. 160, Berlin 1877, Verlag der Königlichen Geheimen Ober-Hofbuchdruckerei (R.v.Decker); zitiert nach: Hempel, Postleidfaden. Leidfaden für die berufliche Bildung, Teil 1: Postverfassungsrecht, Heidelberg 1983, S. VII.

215 Eidenmüller, Grundlagen des Post- und Postbankrechts, Frankfurt am Main 1983, S. 1 ff.

216 Hempel, Postleidfaden. Leidfaden für die berufliche Bildung, Teil 1: Postverfassungsrecht, Heidelberg 1983, S. 3.

Post- und Telegraphenverwaltungen zu einer einheitlichen Postverwaltung zusammengefasst.[217]

Schließlich wurde im Deutschen Kaiserreich mit dem Reichspostgesetz vom 28.10.1871 das Postrecht als Rechtsgebiet etabliert und zu einem Referenzgebiet des Allgemeinen Verwaltungsrechts.[218] In der Weimarer Republik wurden die Postverwaltungen Bayerns und Württembergs in die allgemeine Postverwaltung eingegliedert, sodass es zum ersten Mal eine einheitliche Postverwaltung auf dem gesamten Staatsgebiet des Deutschen Reichs gab.[219] Am 01.04.1924 trat das Reichspostfinanzgesetz in Kraft, das als erstes deutsches Postverfassungsgesetz die Struktur der Post als Sondervermögen mit eigener Haushaltsführung regelte.[220] Nach dem Zusammenbruch des Dritten Reichs endete die Reichspost als Sondervermögen.[221] Nach separaten Postverwaltungen in den Besatzungsgebieten wurde mit dem Grundgesetz wieder eine einheitliche Postverwaltung geschaffen.[222] Weitere rechtliche Regelungen traf die Verordnung zur Überführung der Verwaltungen des Post- und Fernmeldewesens vom 31.03.1950.[223]

2. Die Postreformen

Erste große Veränderungen innerhalb des Postwesens ergaben sich durch die veränderten Kommunikationsstrukturen und neue Anforderungen an ein wettbe-

217 Hempel, Postleidfaden. Leidfaden für die berufliche Bildung, Teil 1: Postverfassungsrecht, Heidelberg 1983, S. 4.

218 RGBl. S., 347; Tettinger, Das aktuelle Deutsche Postrecht in NVwZ 2000, S. 633

219 Hempel, Postleidfaden. Leidfaden für die berufliche Bildung, Teil 1: Postverfassungsrecht, Heidelberg 1983, S. 4 f.

220 Hempel, Postleidfaden. Leidfaden für die berufliche Bildung, Teil 1: Postverfassungsrecht, Heidelberg 1983, S. 5.

221 Hempel, Postleidfaden. Leidfaden für die berufliche Bildung, Teil 1: Postverfassungsrecht, Heidelberg 1983, S. 5.

222 Hempel, Postleidfaden. Leidfaden für die berufliche Bildung, Teil 1: Postverfassungsrecht, Heidelberg 1983, S. 6.

223 Hempel, Postleidfaden. Leidfaden für die berufliche Bildung, Teil 1: Postverfassungsrecht, Heidelberg 1983, S. 6.

werbsfähiges und kundenorientiertes Wirtschaften. Mit dem PostStruktG vom 01.07.1989 wurden die rechtlichen Grundlagen für eine Veränderung der Rahmenbedingungen in der Bundesverwaltung gelegt.[224] Die Deutsche Bundespost wurde in drei öffentliche Unternehmen aufgeteilt, die Deutsche Bundespost TELEKOM, die Deutsche Bundespost POSTBANK und die Deutsche Bundespost POSTDIENST, in deren Aufgabenbereich der Postverkehr fiel.[225]

Der Finanzbedarf zum Aufbau der Infrastruktur im Zuge der Wiedervereinigung, zunehmender Wettbewerbsdruck und der damit verbundene notwendige Handlungs- und Entwicklungsspielraum, den die bisherigen Rechtsformen nicht geboten hatten, machten eine weitere Postreform notwendig.[226] Mit dem Gesetz zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz – PTNeuOG) vom 14.09.1994 wurde die Grundlage, für eine Privatisierung der drei Unternehmen der Deutschen Bundespost geschaffen.[227] Eine Verankerung der Infrastrukturgewährleistung entsprechend Art. 87f Abs. 1 GG und eine privatwirtschaftliche Erbringung von Dienstleistungen nach Art. 87f Abs. 2 GG bildeten sich wechselseitig ergänzende Pfeiler der Neuordnung im Postbereich.[228]

Um auslaufende Übergangsregelungen des PTNeuOG zu ersetzen sowie durch den Wunsch chancengleichen und funktionsfähigen Wettbewerb bei gleichzeitiger Infrastruktursicherung herzustellen, trat am 22.12.1997 ein neues Postgesetz (PostG) in Kraft.[229]

---

224 Pfeffermann/Kühn, § 1 Einführung in Stern in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar, S. 29 ff.

225 Pfeffermann/Kühn, § 1 Einführung in Stern in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar, S. 27 Rn. 14.

226 Zu den Ursachen ausführlicher Pfeffermann/Kühn, § 1 Einführung in Stern in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar, S. 30 Rn. 33 ff.

227 BGBl. I, S. 2325; 1996 I, S. 103.

228 Klaus Stern, Postreform zwischen Privatisierung und Infrastrukturgewährleistung, DVBL 1997, S. 309, (315).

229 BGBl. I, S. 3294; Vorblatt des PostG Abschnitt A Zielsetzung; Pfeffermann/Kühn, § 1 Einführung in Stern in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar, S. 39 Rn. 89 f.

Es folgten drei Gesetze zur Änderung des Postgesetzes. Das erste Gesetz zur Änderung des PostG vom 02.09.2001 diente der Verlängerung der Exklusivlizenzen für die Deutsche Post AG bis zum 31.12.2007.[230] Das zweite Gesetz zur Änderung des Postgesetzes vom 30.01.2002 diente der Anpassung der gesetzlichen Regelungen an die Verlängerung der Exklusivlizenzen des Ersten Änderungsgesetzes.[231]

Das dritte Gesetz zur Änderung des Postgesetzes vom 16.08.2002 diente der Umsetzung der Änderungen der Postdienst-Richtlinie 97/67/EG durch die RL 2002/39/EG, die eine Liberalisierung des Postmarktes durch eine Absenkung des durch die Exklusivlizenz reservierten Bereichs auf 100 Gramm vorsah.[232]

3. Die Postpolitik der Europäischen Union

Die Europäische Union hat den Markt für Postdienste als wichtigen Zukunfts- und Wachstumsmarkt erkannt, der im Groben die Bereiche Kommunikation, Werbung und Transport umfasst und zusammen mit anderen Logistik-, Kommunikations- und Transportdienstleistungen eine Schlüsselindustrie darstellt.[233] Er stellt eine Schnittstelle zwischen dem Kommunikationssektor und dem elektronischen Handel dar, erwirtschaftet etwa 1 % des Bruttoinlandsprodukts der Europäischen Union und bildet damit einen Pfeiler des Binnenmarktes.[234] Neue Technologien und ein sich veränderndes Kommunikationsverhalten stellen Herausforderungen und Chancen gleichermaßen dar. Die Umsätze im Briefverkehr sinken zugunsten steigender Kommunikation über E-Mail und andere Neue

230 Pfeffermann/Kühn, § 1 Einführung in Stern in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar, S. 44 Rn. 118.

231 Pfeffermann/Kühn, § 1 Einführung in Stern in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar, S. 45 Rn. 121.

232 Pfeffermann/Kühn, § 1 Einführung in Stern in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar, S. 45 Rn. 123 ff.

233 IP/08/928, Brüssel den 13.06.2008, Binnenmarkt, Kommissar McCreevy veranstaltet hochrangige Konferenz zur Postmarktreform.

234 IP/08/323, Brüssel, den 27.02.2008, Veröffentlichung der Postrichtlinie markiert den Beginn der vollständigen Marktöffnung.

Medien, neue Formen wie der Hybridbrief, bieten jedoch auch hier neue Chancen.[235] Dieser Entwicklung stehen, unter anderem bedingt durch einen wachsenden Onlinehandel, steigende Umsätze im Versandhandel gegenüber.[236]

Um die Weiterentwicklung des Postdienstemarktes sicherzustellen, hat die Union Leitlinien formuliert.[237] Eine Liberalisierung des Marktes für Postdienste sowie die Schaffung eines Binnenmarktes für Postdienstleistungen sollte Wachstumspotenziale freisetzen und langfristig Arbeitsplätze sichern. Dafür sollten Postmonopole und reservierte Bereiche schrittweise abgetragen werden und in einem weiteren Schritt sonstige Markteintrittsbarrieren in den Blick genommen und abgeschafft werden.[238] Diese Öffnung überwachen und fairen Wettbewerb und Kundenschutz sicherstellen sollen dabei unabhängige nationale Regulierungsbehörden. Bestimmt werden die Leitlinien hierbei grundsätzlich von der Sicherung des Universaldienstes.[239] Deswegen ist ein leistungsstarker und qualitativ hochwertiger, bezahlbarer und effizienter Universaldienst einzurichten und zu erhalten.

II. Rechtsgrundlagen

Die Grundlage für die Anwendung des Postrechts bildet das nationale Recht, das jedoch durch weitgehende Harmonisierung des Rechtsrahmens auf Ebene der Europäischen Union in Teilen eine Umsetzung der unionalen Vorgaben darstellt. Eine weitere internationale Grundlage bildet der Weltpostvertrag.

---

235 KOM(2008) 884 endg., Bericht der Kommission an den Rat und das Europäische Parlament über die Anwendung der Postrichtlinie, S. 4.

236 Quelle: http://www.welt.de/wirtschaft/article106271062/Boomender-Internethandel-steigert-Gewinn-der-Post.html.

237 So auch im Ergebnis die Studie WIK – Consult, Study on the External Dimension of the EU Postal Acquis, S. i.

238 IP/08/323, Brüssel, den 27.02.2008, Veröffentlichung der Postrichtlinie markiert den Beginn der Vollständigen Marktöffnung.

239 Ähnlich Stern, Postreform zwischen Privatisierung und Infrastrukturgewährleistung, DVBL 1997, S. 309, (311).

1. Das nationale Recht

Ausgangspunkt für die Betrachtung des Rechtsrahmens für das deutsche Postrecht kann nur das Grundgesetz sein. Art. 87f GG und Art. 143b GG bilden hier die Grundlage der Regelungen im Postwesen. Das Briefgeheimnis aus Art. 10 GG stellt die grundrechtliche Basis dar. Davon ausgehend bildet das PostG die spezialgesetzliche Basis. Präzisiert und ausgefüllt wird dieses durch die Postuniversaldienstleistungsverordnung (PUDLV), die Post-Entgeltregulierungsverordnung (PEntgV), die Postdienstleistungsverordnung (PDLV), die Postlizenzgebührenverordnung (PLGebV) sowie die Postdienste-Datenschutzverordnung (PDSV).

a) Verfassungsrechtliche Grundlagen

Mit der Privatisierung der Deutschen Bundespost veränderte sich auch ihre Stellung im institutionellen Gefüge.[240] Die unmittelbare Grundrechtsbindung der Deutschen Post fiel weg. Die datenschutzrechtlichen Regelungen wurden so zum Ausfluss der Schutzpflicht des Staates.[241] Die Grundlagen dieser Privatisierung liegen verfassungsrechtlich in Art. 87f GG sowie in Art. 143b GG, die die Postreformen ermöglicht haben.

aa) Die Infrastrukturgewährleistung, Art. 87f GG

Mit der Feststellung, dass *„der Bund im Bereich des Postwesens und der Telekommunikation flächendeckend angemessene und ausreichende Dienstleistungen"* gewährleistet, statuiert Art. 87f Abs. 1 GG als Ausprägung des Sozialstaatsprinzips ein Staatsziel.[242] Mit einer angemessenen Versorgung ist die Qualität der Dienstleistung, mit einer ausreichenden Versorgung die Quantität der Dienstleistungen gemeint.[243] Der Umfang der Versorgung als Universaldienst ist mehr im Sinne

---

240 Art. 10 GG wird unter 4. Teil. E. III. 3.) besprochen.

241 Bzgl. des Persönlichkeitsrechts vgl. auch BverfG 35, S. 202, (221).

242 Herdgen, Verfasssungsrechtliche Grundlagen in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar Rn. 25 ff.; Windthorst in Sachs, GG, Art. 87f GG Rn. 14.

243 Herdgen, Verfasssungsrechtliche Grundlagen in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar Rn. 30; BT-Drs. 12/7269, S. 8.

einer Grundversorgung zu verstehen und hat sich grundsätzlich nach dem Bedarf zu richten.[244] Der Begriff „flächendeckend" umfasst das gesamte Staatsgebiet der Bundesrepublik, in dem eine Grundversorgung bereitgestellt werden muss, eine Tarifeinheit im Raum ergibt sich daraus allerdings noch nicht.[245] Darüber hinaus umfasst der Infrastrukturauftrag eine grenzüberschreitende Versorgung mit Postdienstleistungen im Sinne des Weltpostvertrages.

Adressat ist der Bundesgesetzgeber, nicht die Nachfolgeunternehmen der Deutschen Bundespost.[246] Art. 87f Abs. 1 GG gewährt keine subjektiven Rechte, sodass Postkunden hieraus keine Ansprüche ableiten können.[247]

bb) Art. 143b GG

Art. 143b GG stellt die verfassungsrechtliche Grundlage für die Postreformen und damit eine Privatisierung der Deutschen Bundespost dar.[248] Art. 143b Abs. 1 GG regelt die Umwandlung des Sondervermögens Deutsche Bundespost, während die Absätze 2–3 Übergangsregelungen enthalten.[249] Mit der Umwandlung des Sondervermögens Deutsche Bundespost wurde zunächst eine formelle Privatisierung (Organisationsprivatisierung) ermöglicht.[250] Eine materielle Privatisie-

---

244 Herdgen, Verfasssungsrechtliche Grundlagen in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar Rn. 31 ff.

245 Herdgen, Verfasssungsrechtliche Grundlagen in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar Rn. 36 f.; zur Tarifeinheit im Raum: Herdegen, Die Regulierung des Postuniversaldienstes: Abschied vom Markt? in ZRP 1999, S. 63 (67).

246 Herdgen, Verfasssungsrechtliche Grundlagen in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar Rn. 26.

247 Herdgen, Verfasssungsrechtliche Grundlagen in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar Rn. 27.

248 Wieland in Dreier, GG, 143b GG Rn. 4; Kienemund in Schmidt-Bleibtreu/Klein, GG, Art. 143b GG Rn. 1; Battis in Sachs, GG, Art. 143b Rn. 3; Gersdorf in v. Mangoldt/Klein/Starck, GG, 143b GG, Bd. 3 Rn. 1.

249 Kienemund in Schmidt-Bleibtreu/Klein, GG, Art. 143b GG Rn. 1; Battis in Sachs, GG, Art. 143b, Bd. 3 Rn. 3; Gersdorf in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 143b, Bd. 3 Rn. 1.

250 Uerpmann/Wittzack in v. Münch/Kunig, Grundgesetz, Art. 143b GG Rn. 1;Battis in Sachs, GG, Art. 143b Rn. 6; Gersdorf in v. Mangoldt/Klein/Starck, GG, Art. 143b GG, Bd. 3 Rn. 1 ff.

rung durch den Verkauf von Anteilen wurde dem Bund erst mit Ablauf von fünf Jahren und mit Zustimmung des Bundesrates erlaubt.[251]

b) Das Postgesetz

Das PostG vom 22.12.1997 stellt die Grundlage des Postwesens in Deutschland dar.[252] Es trägt den Erfordernissen der Umgestaltung des Postsektors sowie der Infrastruktursicherung Rechnung.[253] So soll es dem verfassungsrechtlichen Auftrag gerecht werden *„über Wettbewerb den Zugang von Wirtschaft und Verbrauchern zu modernen, preiswerten und leistungsfähigen Postdienstleistungen zu gewährleisten"*.[254]

c) Postdienste-Datenschutzverordnung (PDSV)

Mit der Postdienste-Datenschutzverordnung PDSV vom 02.07.2002 setzte die Bundesregierung ihre Verordnungsermächtigung aus § 41 Abs. 1 PostG um und ersetzte damit die Postdienstunternehmen-Datenschutzverordnung vom 04.11.1996.[255] Damit hat die Bundesregierung den durch die Postreformen veränderten Rahmenbedingungen und einem liberalisierten Markt für Postdienstleistungen Rechnung getragen.

Das Begriffsverständnis entspricht dem des BDSG. Im Verhältnis zum Postgeheimnis, dass nur die näheren Umstände des Postverkehrs schützt, geht der Schutzbereich der PDSV weiter und umfasst auch offenkundige Daten.[256] Der geschützte Personenkreis wird „sektorspezifisch" in § 1 Abs. 1 S. 1 PDSV auf die

---

251 Battis in Sachs, GG, Art. 143b Rn. 6; Uerpmann/Wittzack in v. Münch/Kunig, Grundgesetz, 6. Aufl. 2012, Art. 143b GG Rn. 4.

252 Postgesetz vom 22. Dezember 1997 (BGBl. I, S. 3294), das zuletzt durch Art. 4 Abs. 106 des Gesetzes vom 7. August 2013 (BGBl. I, S. 3164) geändert worden ist.

253 BR.-Drs. 147/99 Gesetzentwurf, A. Zielsetzung.

254 BR.-Drs. 147/99 Gesetzentwurf, B. Lösung.

255 BGBl. I, S. 2494.

256 Stern, Anh. § 41 § 1 PDSV Rn. 5.

am Postverkehr beteiligten Personen begrenzt und weicht insoweit vom BDSG ab.

2. Das Recht der Europäischen Union

Ausgangspunkt für die Entwicklung eines europäischen Rechtsrahmens für das Postwesen war das Grünbuch über die Entwicklung des Binnenmarktes für Postdienste von 1991.[257] Es stellte eine umfangreiche Bestandsaufnahme der Unterschiede, Gemeinsamkeiten und Defizite der europäischen Postmärkte dar.[258] Unterschiede in der Leistungsqualität der Postdienste, sowie Ungleichgewichte und Unterschiede in den Bereitstellungsbedingungen der postalischen Universaldienste wurden als Problemfelder erkannt.[259] Die Entwicklung einer einheitlichen Strategie und einer gemeinschaftsweiten Universaldienstkonzeption zur Verbesserung der Kommunikation in Europa wurde in den Fokus der Bemühungen gerückt.[260] In der Entschließung des Rates vom 07.02.1994 wurde die Liberalisierung des Postmarktes als eines der Hauptziele in der Entwicklung der Postdienste benannt.[261] Gleichzeitig steht die Sicherung der Dienstleistungen und Qualität des Universaldienstes im Mittelpunkt, was durch nationale Regulierungsbehörden sichergestellt werden soll.[262]

---

257 Grünbuch über die Entwicklung des Binnenmarktes für Postdienste, 1991 KOM 476 endg.

258 v. Danwitz, Europarechtliche Grundlagen in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar Rn. 2 f.

259 RL 97/67/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über gemeinsame Vorschriften für die Entwicklung des Binnenmarktes der Postdienste der Gemeinschaft und die Verbesserung der Dienstqualität, Erwägung 5 ff.

260 Grünbuch über die Entwicklung des Binnenmarktes für Postdienste, 1991 KOM 476 endg., S. 195 ff.

261 Richtlinie 2002/39/EG des Europäischen Parlaments und des Rates vom 10. Juni 2002, 94/C 48/02.

262 Richtlinie 2002/39/EG des Europäischen Parlaments und des Rates vom 10. Juni 2002, 94/C 48/02.

Eine Harmonisierung erfolgte durch die Postdienst-Richtlinie 97/67/EG vom 15.12.1997.[263] Einen weiteren Liberalisierungsschritt stellte die RL 2002/39/EG vom 01.06.2002 dar.[264]

a) Die RL 97/67/EG, geändert durch die RL 2002/39/EG, sowie die RL 2008/6/EG

Die Richtlinie 97/67/EG vom 15.12.1997 war gemäß ihrem Art. 27 bis zum 31.12.2004 befristet und wurde zur weiteren Liberalisierung des Postmarktes von der RL 2002/39/EG vom 10.06.2002 geändert. Eine weitere Änderung fand durch die RL 2008/6/EG vom 20.02.2008 statt.[265] Mit dieser Regelung sollten eine schrittweise Öffnung der Postmärkte und die Verwirklichung des Binnenmarktes für Postdienste erreicht werden.[266]

Die Sicherheit der Lieferkette stand zu dem Zeitpunkt nicht im Fokus der Regelungen. Auch Spezialregelungen für Fragen des Datenschutzes und der Datenverarbeitung bei der Erbringung von Postdiensten wurden nicht geschaffen.

Im Mittelpunkt der RL 97/67/EG stand eine Harmonisierung der Rahmenbedingungen für einen europäischen Postmarkt innerhalb der Gemeinschaft.[267] Insbesondere die Schaffung und Ausgestaltung eines gemeinschaftlichen Univer-

263 RL 97/67/EG des Europäischen Parlaments und des Rates vom 15.12.1997 über gemeinsame Vorschriften für die Entwicklung des Binnenmarktes der Postdienste der Gemeinschaft und die Verbesserung der Dienstqualität.

264 ABl. EG Nr. L 17, RL 2002/39/EG vom 10.06.2002.

265 RL 2008/6/EG des Europäischen Parlaments und des Rates vom 20.02.2008 zur Änderung der Richtlinie 97/67/EG im Hinblick auf die Vollendung des Binnenmarktes der Postdienste der Gemeinschaft.

266 RL 97/67/EG des europäischen Parlaments und des Rates vom 15.12.1997 über gemeinsame Vorschriften für die Entwicklung des Binnenmarktes der Postdienste der Gemeinschaft und die Verbesserung der Dienstqualität, Erwägungsgrund Nr. 8.

267 RL 97/67/EG des europäischen Parlaments und des Rates vom 15.12.1997 über gemeinsame Vorschriften für die Entwicklung des Binnenmarktes der Postdienste der Gemeinschaft und die Verbesserung der Dienstqualität, Erwägungsgründe 1–10; v. Danwitz, Europarechtliche Grundlagen in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar Rn. 13.

saldienstes im Postwesen sollten die Grundlage der Harmonisierung bilden.[268] Dafür wurden dem Subsidiaritätsprinzip folgend ein Mindeststandard und ein Rahmen für Universaldienste formuliert.[269] Einen wichtigen Beitrag zur Konsolidierung des Postrechts innerhalb der Gemeinschaft leistet die Richtlinie darüber hinaus durch zahlreiche Begriffsbestimmungen in Art. 2 der Richtlinie.

Die RL 2002/39/EG vollzieht einen weiteren Schritt hin zur Schaffung einen Binnenmarktes für Postdienste, indem – im Kern – die Gewichts- und Preisgrenze im reservierten Bereich abgesenkt wird.[270] Diese weitere Liberalisierung des Postmarktes soll Wachstumschancen des Postmarktes nutzen und erweitern, gleichzeitig jedoch geordnet erfolgen, um weiterhin einen qualitativ hochwertigen Universaldienst zu gewährleisten, der als wichtiges Element der Infrastruktur wichtig für die allgemeine wirtschaftliche Entwicklung ganzer Regionen ist.[271]

In der RL 2008/6/EG steht weiterhin die Sicherung des Universaldienstes im Mittelpunkt der Änderungen, die weiterhin die Qualität und die flächendeckenden Leistungen in einem liberalisierten Marktumfeld gewährleisten sollen.

Mit Kapitel 9a „Bereitstellung von Informationen“ beschäftigt sich die Richtlinie erstmalig im Postbereich mit dem Austausch von Informationen zwischen den Postdiensteanbietern und den nationalen Regulierungsbehörden. Der neu eingefügte Art. 22a stellt in Abs. 1 die Anforderung an die Mitgliedstaaten sicherzustellen, dass die nationalen Regulierungsbehörden alle Informationen von den Postdiensteanbietern bekommen, um die Einhaltung der Richtlinie und der

---

268 RL 97/67/EG des europäischen Parlaments und des Rates vom 15.12.1997 über gemeinsame Vorschriften für die Entwicklung des Binnenmarktes der Postdienste der Gemeinschaft und die Verbesserung der Dienstqualität Erwägungsgründe 11–21; v. Danwitz, Europarechtliche Grundlagen in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar Rn. 13.

269 Bericht der Kommission an das europäische Parlament und den Rat über die Anwendung der Postrichtlinie (RL 97/67/EG) KOM(2002) 632 endgültig, S. 3.

270 v. Danwitz, Europarechtliche Grundlagen Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar Rn. 14.

271 Richtlinie 2002/39/EG des Europäischen Parlaments und des Rates vom 10.06.2002, Erwägungsgründe (11) ff.

auf ihrer Grundlage getroffenen Entscheidungen sicherzustellen sowie zu statistischen Zwecken. Art. 22a Abs. 2 präzisiert den vorangegangenen Absatz: Die Informationen müssen umgehend bereitgestellt werden, gegebenenfalls vertraulich. Weiterhin wird für die Regulierungsbehörde der Grundsatz der Verhältnismäßigkeit betont und eine Begründung der Regulierungsbehörde gefordert. In Art. 22a Abs. 3 wird auf den Informationsaustausch zwischen nationalen Regulierungsbehörden und der Europäischen Kommission abgestellt und der Informationszugang der Kommission sichergestellt.

Art. 22a Abs. 4 verweist auf die europäischen und nationalen Rechtsvorschriften über das Geschäftsgeheimnis, um die Vertraulichkeit der ausgetauschten Informationen sicherzustellen.

b) Zwischenergebnis

Im Mittelpunkt der Postrichtlinie stehen der Aufbau und die Sicherung eines Minimalstandards für Universaldienstleistungen im Postbereich. Eine zentrale Rolle spielen dabei die nationalen Regulierungsbehörden, die die Einhaltung der gesetzlichen Regelungen überwachen sollen.

Die Änderungsrichtlinien spiegeln dabei die schrittweise geordnete Liberalisierung des Marktes für Postdienstleistungen und die Schaffung eines Binnenmarktes für Postdienstleistungen bei gleichzeitiger Absicherung des Standards für Universaldienstleistungen wider.

Die Sicherheit der postalischen Lieferkette findet in den Richtlinien keinen konkreten Niederschlag. Auch datenschutzrechtliche Fragestellungen werden auf unionaler Ebene in den Richtlinien nicht sektorspezifisch geregelt. Lediglich die Notwendigkeit der Sicherstellung des Informationsflusses zwischen den Postdiensteanbietern und den nationalen Regulierungsbehörden sowie den nationalen Regulierungsbehörden und der Europäischen Kommission findet durch die Änderungsrichtlinie RL 2008/6/EG Eingang in das Regelwerk.

Insgesamt haben die EU-Richtlinien große Auswirkungen auf die Postmärkte in der Union hin zu einem Binnenmarkt und einer flächendeckenden hochwerti-

gen Versorgung mit Postdienstleistungen gehabt.[272] Der Markt für Postdienste ist kundenfreundlicher, innovativer und wettbewerbsorientierter geworden.[273]

3. Internationale Rechtsgrundlagen – Weltpostvertrag

Die internationale Rechtsgrundlage im Postrecht bildet der Weltpostvertrag. Viele Standards des internationalen Postverkehrs werden darüber hinaus vom Weltpostverein WPV (engl. UPU Universal Postal Union) gesetzt.

Der erste allgemeine Postvertrag wurde auf dem Weltpostkongress 1874 in Bern mit Wirkung zum 01.07.1875 geschlossen und ist damit auch Gründungsakt des allgemeinen Postvereins.[274] Auf dem Kongress 1978 in Paris wurde dieser in Weltpostverein (Union postale universelle) umbenannt.[275]

Der Weltpostvertrag hat die Rechtsgrundlagen des Weltpostverkehrs gelegt und ist juristisch als völkerrechtlicher Vertrag einzustufen.[276]

4. Zwischenergebnis

Das nationale Recht bildet weiterhin den Kern des Postrechts für Deutschland. Dieses hat seine Grundlage jedoch im Weltpostvertrag und durch eine weitgehende Harmonisierung durch die Europäische Union in den Richtlinien der Union, die durch das PostG und die Verordnungen in nationales Recht umgesetzt wurden.

---

272 KOM(2008) 884 endg., Bericht der Kommission an den Rat und das Europäische Parlament über die Anwendung der Postrichtlinie, S. 8 f.

273 KOM(2008) 884 endg., Bericht der Kommission an den Rat und das Europäische Parlament über die Anwendung der Postrichtlinie, S. 8 f.

274 Kämmerer, Die Rechtsgrundlagen des Weltpostvereins in Jahrbuch des Postwesens 1959, S. 9 (11).

275 Kämmerer, Die Rechtsgrundlagen des Weltpostvereins in Jahrbuch des Postwesens 1959, S. 9 (11).

276 Kämmerer, Die Rechtsgrundlagen des Weltpostvereins in Jahrbuch des Postwesens 1959, S. 9 (11).

III. Begriffsbestimmungen

Die Bestimmung der grundlegenden Begriffe des Postrechts, legt nicht nur die Basis für eine tiefergehende Forschung, sondern setzt gleichzeitig den Umfang fest, indem durch Abgrenzung der verschiedenen Postdienste und Arten der Forschungsgegenstand klarer umschrieben und definiert wird.

Grundlage für diese Festlegung bildet der Begriff des Universaldienstes in § 11 PostG sowie Art. 3 RL 97/67/EG. § 2 PDSV enthält hingegen Definitionen für den Begriff des Dienstanbieters und der am Postverkehr Beteiligten. Schließlich definiert Art. 2 Nr. 1 RL 97/67/EG den Begriff der Postdienste.

1. Der Begriff des Universaldienstes

Regelungen zum Universaldienst finden sich im europäischen Recht in der RL 97/67/EG in Art. 3 sowie im nationalen Recht in § 11 PostG. Ihm kommt die Aufgabe zu, eine Grundversorgung mit Postdienstleistungen sicherzustellen.[277]

a) Art. 3 RL 97/67/EG

Die Richtlinie 97/67/EG dient der Verwirklichung des Binnenmarktes im Postsektor, die aufgrund unterschiedlicher Leistungsqualität notwendig wurde.[278] Art. 3 Abs. 1 RL 97/67/EG versteht unter einem Universaldienst eine Einrichtung, die *„ständig flächendeckend postalische Dienstleistungen einer bestimmten Qualität zu tragbaren Preisen für alle Nutzer bietet"*.

Gemäß Art. 2 Nr. 13 RL 97/67/EG sind *„Anbieter von Universaldienstleistungen eine öffentliche oder private Stelle, die in einem Mitgliedstaat die Leistungen des postalischen Universaldienstes ganz oder teilweise erbringt und der Kommission gemäß Art. 4 mitgeteilt wurde"*.

---

277 v. Danwitz in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar Rn. 1; Windhorst in Sachs, GG, Art. 87 f. GG Rn. 8.

278 Erwägungsgründe der RL 97/67/EG.

b) § 11 PostG

§ 11 PostG definiert den Universaldienst als *„ein Mindestangebot an Postdienstleistungen nach § 4 Nr. 1, die flächendeckend in einer bestimmten Qualität und zu einem erschwinglichen Preis erbracht werden. Der Universaldienst ist auf lizenzpflichtige Postdienstleistungen und Postdienstleistungen, die zumindest in Teilen beförderungstechnisch mit lizenzpflichtigen Postdienstleistungen erbracht werden können, beschränkt. Er umfaßt nur solche Dienstleistungen, die allgemein als unabdingbar angesehen werden"*. Damit folgt man den Vorgaben des Grundgesetzes aus Art. 87f sowie der RL 97/67/EG.

Definiert wird ein Ordnungsrahmen bzw. eine Untergrenze an Leistungen, die erbracht werden müssen, und in welcher Weise diese zu erfolgen hat. Damit soll eine Grundversorgung sichergestellt werden.[279] Eine genaue Ausformung des Rechtsrahmens findet schließlich durch die Post-Universaldienstleistungsverordnung statt.

c) Zwischenergebnis

Für den Universaldienst legt das Unionsrecht mit der RL 97/67/EG die Mindestanforderungen fest, oberhalb derer den Mitgliedstaaten ein Gestaltungsspielraum bleibt.[280] Die Definitionen des Universaldienstes decken sich dabei im Wortlaut weitgehend. Darüber hinaus ist der nationale Rechtsbegriff richtlinienkonform auszulegen.[281] Folglich ist eine Übereinstimmung des unionalen und des nationalen Universaldienstbegriffes festzustellen.[282] Universaldienstleister in Deutschland ist die Deutsche Post AG.[283]

---

279 v. Danwitz in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar § 11 Rn. 6; BT-Drs. 12/7269, S. 5 zu Nr. 3.

280 So auch v. Danwitz in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar § 11 Rn. 11 f.

281 v. Danwitz in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar § 11 Rn. 13.

282 So auch v. Danwitz in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar § 11 Rn. 71.

283 Vgl. v. Danwitz in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar § 11 Rn. 4 ff.

2. Dienstanbieter

§ 2 Nr. 1 PDSV definiert als Diensteanbieter *„alle, die ganz oder teilweise geschäftsmäßig Postdienste erbringen oder daran mitwirken"*. Diese weite Definition umfasst jede Erbringung von Postdienstleistungen unabhängig von der Einordnung als Universaldienstleister, Kurier- Express oder Paketbeförderer, oder ob die Dienstleistung in der Öffentlichkeit angeboten wird.[284] Um einen umfassenden Datenschutz zu gewährleisten, sind die Beteiligten einbezogen, ebenfalls Subunternehmen sowie alle anderen Mitwirkenden.[285]

3. Am Postverkehr Beteiligte

Gemäß § 2 Nr. 2 PDSV sind am Postverkehr Beteiligte *„diejenigen, die mit einem Diensteanbieter einen Vertrag über Postdienste schließen oder geschlossen haben (Kunden)"*, sowie *„Personen, die Postdienste eines Diensteanbieters nutzen, einschließlich der Empfänger und Ersatzempfänger von Postsendungen"*. Kunden in diesem Sinne sind damit natürliche sowie auch juristische Personen, soweit das Postgeheimnis sich auf sie erstreckt.[286]

4. Postdienste

Gemäß Art. 2 Nr. 1 RL 97/67/EG sind Postdienste solche Dienste, die *„im Zusammenhang mit der Abholung, dem Sortieren, dem Transport und der Zustellung von Postsendungen"* stehen. Welche Dienstleistungen im Sinne des Universaldienstes als Postdienstleistung verstanden werden, ergibt sich aus der Post-Universaldienstleistungsverordnung (PUDLV) und umfasst insbesondere die Beförderung von Briefen, Paketen, Zeitungen und Zeitschriften.

---

284 So auch Stern, Anh. § 41, § 2 PDSV Rn. 3.

285 Stern, Anh. § 41, § 2 PDSV Rn. 4.

286 Stern, Anh. § 41, § 2 PDSV Rn. 6.

IV. Der Datenschutz im Postrecht

Ausgangspunkt für den Schutz von Daten und Informationen ist das Recht auf informationelle Selbstbestimmung, das sich in Deutschland aus dem Allgemeinen Persönlichkeitsrecht (APR) in Art. 1 GG Abs. 1 i. V. m. Art. 2 Abs. 1 GG ableitet.[287] Im Besonderen kommt der Schutz des Betriebsgeheimnisses und im Postbereich das Brief-, Post- und Fernmeldegeheimnis aus Art. 10 GG hinzu.[288]

Der Schutz personenbezogener Daten natürlicher Personen wird im BDSG grundsätzlich etabliert und durch ein Verbot der Erhebung, Verarbeitung oder Nutzung mit Erlaubnisvorbehalt in § 4 BDSG gesichert.

Spezialgesetzlich für den Postbereich finden sich Regelungen in Abschnitt 9 des Postgesetzes. Von besonderer Bedeutung sind dabei das Postgeheimnis in § 39 PostG sowie die Regelungen zum Datenschutz in § 41 PostG und dem Anhang zu § 41, mit der Postdienste-Datenschutzverordnung (PDSV).

1. Das Postgeheimnis, § 39 PostG

Das Postgeheimnis gemäß § 39 PostG bildete vor den Postreformen und der Privatisierung der Post die einfachgesetzliche Konkretisierung des grundrechtlich geschützten Postgeheimnisses.[289] Diese Rolle wandelte sich mit dem Ausscheiden der Deutschen Bundespost als grundrechtsverpflichtetem und rückte die Schutzpflichten des Staates in den Mittelpunkt. Damit entstand eine einfachgesetzliche Verpflichtung von Anbietern von Postdienstleistungen zur Wahrung des Postgeheimnisses.

---

287 Das APR wird unter 4. Teil. E. III. 1.) besprochen.

288 Art. 10 GG wird unter 4. Teil. E. III. 3.) besprochen.

289 Stern, § 39 Rn. 4 ; Ohnheiser, Postrecht; vgl. auch § 5 PostG Rn. 2 Stober/Moelle/Müller-Dehn, in Stern Postrecht Teil H § 5 PostG Rn. 7.

a) Der Schutzbereich des Postgeheimnisses, § 39 Abs. 1 PostG

Durch das Postgeheimnis gemäß § 39 Abs. I PostG sind die *„näheren Umstände des Postverkehrs bestimmter natürlicher oder juristischer Personen sowie der Inhalt von Postsendungen"* geschützt.

Dies umfasst im Kern den Schutz von Postsendungen und meint damit alle in den Geltungsbereich des PostG fallenden Gegenstände, neben Paketen unter anderem auch Briefe und Postkarten.[290] Es ist für den Schutz unerheblich, ob die Postsendungen geöffnet oder verschlossen sind.[291]

Geschützt werden die näheren Umstände des Postverkehrs. Dazu *„gehören alle Verbindungsdaten, die nicht den Inhalt einer konkreten Postsendung selbst betreffen"*.[292] Dies umfasst persönliche Angaben wie Absender und Empfänger, die Aufgabe der Postsendung betreffende Informationen wie das Aufgabedatum, den Ort, die Art und Weise der Dienstleistungsinanspruchnahme sowie Angaben zur Sendung, wie Stückzahlen und Mengen.[293]

Nicht umfasst werden abweichend vom Datenschutz offenkundige Tatsachen, wie die Anschrift einer Person, wenn sich nicht Rückschlüsse auf die postalische Nutzung schließen lassen.[294] Ebenfalls nicht umfasst sind Angaben ohne einen konkreten Bezug zum Postverkehr einer Person (wie z. B. statistische Angaben).[295]

Der geschützte Personenkreis umfasst sowohl natürliche als auch juristische Personen. Die Geschäftsfähigkeit natürlicher Personen spielt dabei keine Rolle.[296] Nicht rechtsfähige Personenvereinigungen werden über das hinter ihnen stehende personale Substrat mitgeschützt.[297]

---

290 BR-Drs. 147/97, S. 45 zitiert in Stern, § 39 Rn. 14.

291 Stern, § 39 Rn. 12.

292 Stern, § 39 Rn. 10.

293 Stern, § 39 Rn. 10; OVG Koblenz, NJW 1981, S. 837; Ohnheiser, Postrecht, vgl. § 5 PostG Rn. 4; 2 Stober/Moelle/Müller-Dehn, in Stern, Postrecht Teil H § 5 PostG Rn. 21.

294 Stern, § 39 Rn. 11.

295 Stern, § 39 Rn. 11.

296 Stern, § 39 Rn. 12.

297 BR-Drs. 147/97, S. 45 zitiert in Stern, § 39 Rn. 12.

Das Postgeheimnis dient den Interessen des geschützten Personenkreises, deswegen kann auch eine geschützte Person darauf verzichten.[298]

b) Verpflichtete des Postgeheimnisses, § 39 Abs. 2 PostG

Verpflichtete sind gemäß § 39 Abs. 2 PostG alle in der Erbringung und Mitwirkung geschäftsmäßig tätigen Postdienste. Die Verpflichtung ist für weitere Veränderungen auf dem Postmarkt offen und soll ebenfalls zukünftige Organisationsformen und Anbieter umfassen.[299] Die Formulierung ist weit zu verstehen und soll alle in der postalischen Lieferkette Beteiligten umfassen. Nicht umfasst sind staatliche Stellen, die auch weiterhin durch das Post- und Briefgeheimnis aus Art. 10 GG gebunden werden.[300]

c) Verhaltensregeln für Verpflichtete, § 39 Abs. 3 PostG

§ 39 Abs. 3 PostG präzisiert das Postgeheimnis dahingehend, dass in Satz 1 die Kenntnisnahme vom Inhalt von Postsendungen an die Erforderlichkeit für die Erbringung der Postdienstleistung gekoppelt wird. Für die so gewonnenen Informationen wird in Satz 2 eine Zweckbindung an die Erbringung der Postdienstleistung festgelegt. Geschützt werden soll vor jedweder nicht postbetrieblichen Verwendung der für die Erbringung der Postdienstleistung gewonnenen Informationen.[301]

Eine Ausnahme von dieser Zweckbindung wird in Satz 3 lediglich aufgrund einer ausdrücklichen Ermächtigungsgrundlage im Gesetz gewährt, die sich auch auf Postsendungen oder den Postverkehr bezieht. Damit wird der Vorrang des Postgeheimnisses vor anderen staatlichen Eingriffsrechten und Auskunftsansprüchen festgelegt, die sich nicht auf den Postbereich beziehen und sichergestellt, dass eine Abwägung mit den im Postgeheimnis geschützten Rechtsgütern statt-

298 Stern, § 39 Rn. 13; Ohnheiser, Postrecht § 5 PostG Rn. 6; Stober/Moelle/Müller-Dehn, in Stern, Postrecht Teil H § 5 PostG Rn. 8.

299 Ebenso Stern, § 39 Rn. 16.

300 Stern, § 39 Rn. 17.

301 Stern, § 39 Rn. 24.

findet.[302] Eine solche Ermächtigung findet sich im PostG selbst in § 42 (Kontrolle und Durchsetzung von Verpflichtungen), ebenfalls eine Ermächtigung enthält § 5 Abs. 1 ZollVerwG.[303]

§ 39 Abs. 3 S. 4 PostG hat lediglich in Bezug auf den Vorrang der Anzeigepflicht aus § 138 StGB deklaratorische Wirkung.

d) Ausnahmen vom Postgeheimnis, § 39 Abs. 4 PostG

§ 39 Abs. 4 PostG legt Ausnahmen von den Verboten des 3. Absatzes, aus betrieblichen Gründen (Satz 1) sowie zur Auslieferung an Ersatzempfänger (Satz 2) fest.

Gemäß Nr. 1 dürfen Postunternehmen *„bei entgeltbegünstigten Postsendungen das Vorliegen tariflicher Voraussetzungen"* prüfen. Damit soll sichergestellt werden, dass sich Kunden unter dem Schutz des Postgeheimnisses keine ungerechtfertigten Vermögensvorteile verschaffen können.[304]

Nr. 2 erlaubt die Sicherung beschädigter Postsendungen. Die Art der Sicherungsmaßnahmen ist vom Umfang der Beschädigung abhängig und kann auch eine Öffnung der Sendung notwendig machen.[305]

Nr. 3 erlaubt es den Postunternehmen, Einsicht zu nehmen und verschlossene Sendungen ggf. zu öffnen, wenn bei unanbringlichen Postsendungen der Absender oder Empfänger nicht anders zu ermitteln ist.[306]

Nr. 4 erlaubt einen Eingriff, um *„körperliche Gefahren abzuwenden, die von einer Postsendung für Personen und Sachen ausgehen*". Gemeint ist eine konkrete Gefahrenabwehr, der Tatbestand stellt keine Grundlage für allgemeine Maßnahmen der Gefahrenabwehr da.[307]

---

302 BR-Drs. 147/97, S. 46, zitiert in Stern, § 39 Rn. 26 ff.; zu § 5 ZollVG siehe 4. Teil. C. 2.) c) cc).

303 Stern, § 39 Rn. 31 ff. Eine Übersicht weitere Ermächtigungen findet sich ebenfalls bei Stern, § 39 Rn. 17 ff.

304 Stern, § 39 Rn. 51. Stober/Moelle/Müller-Dehn, in Stern, Postrecht Teil H § 5 PostG Rn. 29.

305 Stern, § 39 Rn. 52: Altmannsperger, § 5 PostG, S. 29 ff.

306 Stern, § 39 Rn. 53.

307 Stern, § 39 Rn. 54.

e) Mitteilungsrechte, § 39 Abs. 5 PostG

§ 39 Abs. 5 PostG begründet keine Auskunftspflichten von Postunternehmen gegenüber Dritten, sondern eine weitere Ausnahme vom Postgeheimnis, um Ansprüche aus einer Postdienstleistung geltend machen zu können oder *„um die Verfolgung von Straftaten zu ermöglichen, die beim Postverkehr zum Schaden eines Postunternehmens begangen wurden*".[308]

Die Geltendmachung von Ansprüchen umfasst Zahlungsansprüche, Schadens- und Aufwendungsersatzansprüche sowie Ansprüche aufgrund von Leistungsstörungen.[309] *„Mitteilungen über den Postverkehr"* umfassen lediglich die Weiterleitung der Versandmodalitäten. Eine Berechtigung zur Öffnung von Postsendungen ergibt sich daraus nicht.[310] Die Adressaten der Mitteilung werden in der Regelung nicht benannt, der Kreis dürfte sich zur Geltendmachung von Ansprüchen auf Rechtsanwälte, Gerichte und Strafverfolgungsbehörden erstrecken.[311]

Die Mitteilung zur Verfolgung von Straftaten umfasst auch nur solche und keine Ordnungswidrigkeiten.[312] Weiterhin muss die Straftat laut Abs. 5 *„beim Postverkehr zum Schaden eines Postunternehmens begangen"* worden sein. Damit muss die Straftat einen Bezug zur Erbringung der Postdienstleistung aufweisen. Der Schaden kann unmittelbar oder auch nur mittelbar, muss aber tatsächlich entstanden sein.

f) Verhältnis zu anderen Rechtsnormen

Vor Kenntnisnahme des Inhaltes von Postsendungen schützen weiterhin § 202 StGB (Verletzung des Briefgeheimnisses) sowie § 206 StGB (Verletzung des Post- oder Fernmeldegeheimnisses), teils jedoch mit unterschiedlichem Schutzumfang so-

308 Stern, § 39 Rn. 59; Ohnheiser, Postrecht § 5 PostG Rn. 22.

309 Stern, § 39 Rn. 62.

310 Stern, § 39 Rn. 60.

311 Stern, § 39 Rn. 61.

312 Stern, § 39 Rn. 63.

wie mit unterschiedlichen Rechtsfolgen. Bei Verletzung des § 39 PostG können sich ein Schadensersatzanspruch aus §§ 823 ff. BGB ergeben sowie der Widerruf der Lizenz gemäß § 9 PostG.[313] Die Verletzung der §§ 202, 206 StGB ist mit einer strafrechtlichen Strafandrohung verbunden.[314]

2. Datenschutz, § 41 PostG

§ 41 PostG stellt die zentrale Norm für den Datenschutz im Postrecht dar.

a) § 41 Abs. I PostG, Verordnungsermächtigung

§ 41 Abs. 1 PostG regelt ein Bündel allgemeiner datenschutzrechtlicher Fragestellungen. § 41 S. 1 PostG enthält eine Ermächtigung für die Bundesregierung zum Erlass einer Rechtsverordnung zum „Schutz personenbezogener Daten der am Postverkehr Beteiligten". Aus der Formulierung „erlässt" ist sogar auf eine Pflicht zu schließen, diesen Rechtsbereich zu regeln.[315]

§ 41 Abs. 1 S. 2 PostG weist gesondert auf das Verhältnismäßigkeitsprinzip, insbesondere das Erforderlichkeitsprinzip sowie die Zweckbindung im Datenschutz hin.

§ 41 Abs. 1 S. 3 PostG fordert Höchstfristen für die Speicherung personenbezogener Daten, die die Interessen des jeweiligen Unternehmens und der Betroffenen berücksichtigen. Grundsätzlich sind dabei Daten, die keiner Höchstfrist unterliegen, mit Erreichen des Verwendungszwecks zu vernichten.[316]

313 Stern, § 39 Rn. 22.

314 Stern, § 39 Rn. 22.

315 Stern, § 41 Rn. 12.

316 Stern, § 41 Rn. 21 f.

b) Datenschutz juristischer Personen, § 41 Abs. 1 S. 4 PostG

§ 41 Abs. 1 S. 4 PostG stellt dem Postgeheimnis unterliegende Einzelangaben juristischer Personen personenbezogenen Daten gleich. Diese Gleichstellung wird nochmals in § 1 Abs. 1 S. 2 PDSV wiederholt.

Damit wird von der Regelung des § 3 Abs. 1 BDSG abgewichen, die lediglich die personenbezogenen Daten natürlicher Personen schützt und hiermit den Wirkungsbereich des BDSG prägt und durchzieht. Juristischen Personen gleichgestellt sind nicht-rechtsfähige Personengruppen, die unmittelbar und nicht erst über ihr personales Substrat geschützt sind.[317]

Eine vollkommene Gleichstellung des Schutzes natürlicher und juristischer Personen wird damit jedoch nicht erreicht, da sich die Schutzbereiche unterscheiden.[318] Während sich bei natürlichen Personen der Schutz auf alle personenbezogenen Daten erstreckt, schützt § 41 Abs. 1 S. 4 PostG nur die Daten, die unter das Postgeheimnis fallen.[319] Umgesetzt wird dieser Schutz in § 1 Abs. 1 S. 2 PDSV im Anwendungsbereich der PDSV, der sich ebenfalls auf juristische Personen erstreckt wird.

Mit dieser Regelung trägt der Gesetzgeber dem Schutzbedürfnis juristischer Personen bei der Inanspruchnahme von Postdiensten, besonders im wirtschaftlichen Bereich, Rechnung.

c) Zulässigkeit betrieblicher Datenverarbeitung, § 41 Abs. 2 PostG

§ 41 Abs. 2 PostG stellt eine Ermächtigungsgrundlage zur Erhebung, Verarbeitung und Nutzung von Daten natürlicher und juristischer Personen für bestimmte Fälle der *„betrieblichen Abwicklung von geschäftsmäßigen Postdiensten“* dar.

---

317 Ebenso Stern, § 41 Rn. 25.

318 Stern, § 41 Rn. 25.

319 Zum Schutzbereich des Postgeheimnisses siehe II. 4.) a) aa) Der Schutzbereich des Postgeheimnisses, § 39 Abs. I PostG; Stern, § 41 Rn. 25.

d) Zweckänderung der Datenverarbeitung und Nutzung, § 41 Abs. 3 PostG

§ 41 Abs. 3 PostG erlaubt bei Einwilligung des Kunden, die aus § 41 Abs. 2 Nr. 1 PostG gewonnenen Daten für Werbung, Kundenberatung und Marktforschung einzusetzen, soweit diese dafür erforderlich sind.

e) Kopplungsverbot § 41 Abs. 4 PostG

Die Angewiesenheit des Kunden auf die Postdienstleistung führt zu einer besonders starken Stellung der Postunternehmen. Dass diese ihre Stellung im Hinblick auf die Gewinnung von Daten ausnutzen, soll § 41 Abs. 4 S. 1 PostG verhindern, indem eine Kopplung des Postdienstes an die Angabe von Daten, die nicht zwingend für die Erbringung der Dienstleistung notwendig sind, untersagt wird[320]. Flankiert wird das Kopplungsverbot von Informations- und Kundenrechten.

f) Zwischenergebnis

§ 41 PostG gewährleistet einen umfassenden Schutz personenbezogener Daten im postalischen Bereich. Der geschützte Personenkreis wird im Vergleich zum allgemeinen Datenschutzrecht um juristische Personen erweitert. Die Möglichkeiten der Datenverarbeitung werden hingegen möglichst auf die für den Postverkehr notwendigen Vorgänge begrenzt.

3. Zwischenergebnis

Die §§ 39 und 41 PostG tragen als lex specialis zum allgemeinen Datenschutzrecht dem asymmetrischen Verhältnis zwischen Postkunden und Postunternehmen sowie der herausragenden Bedeutung von Postdienstleistungen für Warenströme und Kommunikation Rechnung. Das Verbot mit Erlaubnisvorbehalt aus § 4 BDSG wird durch klar begrenzte Erlaubnistatbestände umgesetzt und ausgefüllt. Das Kopplungsverbot sowie ein weiter präzisierter Erforderlichkeits-

[320] Stern, § 41 Rn. 46.

grundsatz erweitern den Schutz personenbezogener Daten über das allgemeine Datenschutzrecht hinaus.

V. Zwischenergebnis

Das Postrecht steht exemplarisch für den Wandel des besonderen Verwaltungsrechts im europäischen Kontext. Als Recht für den Zweig der Verwaltung „Bundespost" konzipiert, hat es im Zuge der Harmonisierung des europäischen Binnenmarktes und der Privatisierung der Bundespost weitreichende Veränderungen erfahren.

Der Schutz personenbezogener Daten sowie des Brief- und Postgeheimnisses gegenüber dem Bürger wurde über diesen Transformationsprozess hinaus erhalten und ausgebaut und einfachgesetzlich verankert und präzisiert.

C. Zollrecht

Die Sicherung von Grenzen und die Kontrolle der Bewegungen von Waren und Menschen bilden ein Merkmal moderner territorialer Staatlichkeit. Die Erhebung von Abgaben für die Ein-, Durch- oder Ausfuhr von Waren innerhalb eines bestimmten Gebietes bildet bis heute in vielen Staaten eine wichtige Einnahmequelle. Gleichzeitig ermöglichen Abgaben an neuralgischen Punkten (Grenzen, Brücken, Häfen, Märkten) die Steuerung von Warenbewegungen. Dies ermöglicht die Förderung von Wirtschaftszweigen, Produktgruppen oder Orten, auf die bestimmte Tätigkeiten konzentriert werden können, aber auch den Schutz heimischer Industrien. Neben finanziellen Interessen, Steuerungs- und Lenkungsfunktionen treten aber auch immer mehr sicherheitspolitische Aufgaben in den Vordergrund der Arbeit des Zolls.

I. Historische Einführung

Bereits das Römische Reich kannte Abgaben, die an Zollstätten – damals zwar noch eher als Benutzungsgebühr denn als Abgabe – entrichtet wurden.[321] Für die Kaiserzeit ist bereits eine schuldrechtliche Bindung an den Zollschuldner und nicht mehr eine dingliche Bindung an die Ware feststellbar.[322] Das Mittelalter hindurch wurden Finanzzölle zur Erzielung staatlicher Einnahmen an Brücken, Straßen, Märkten oder Hafenanlagen als Benutzungsgebühren oder Schutzgebühren erhoben.[323]

Die Erhebung von Zöllen an staatlichen Grenzen ist eine Errungenschaft des 17. Jahrhunderts und fällt mit der Schaffung von einheitlichen staatlichen Wirt-

[321] Rüsken in Rüsken, Zollrecht, Einführung, S. 13 Rn. 30.

[322] Rüsken in Rüsken, Zollrecht, Einführung, S. 13 Rn. 30; Schwarz/Wockenfoth, Zollrecht, Einleitung Rn. 2.

[323] Witte/Wolffgang, Lehrbuch des Europäischen Zollrechts, S. 1.

schaftsgebieten zusammen.[324] Diese staatlichen Zollgebiete ermöglichten eine merkantilistische Wirtschaftspolitik, die durch die Erhebung von Schutzzöllen die heimische Produktion förderte und den eigenen Markt gegen Importe abschirmte.[325]

In Deutschland führte Preußen 1806 erstmals ein Grenzzollsystem ein.[326] Davon ausgehend folgte 1818 das Preußische Zollgesetz, das von den im Deutschen Zollverein vereinigten Staaten 1818 übernommen wurde und 1838 vom Vereinszollgesetz abgelöst wurde, welches die Rechtseinheit im Deutschen Zollverein verwirklichte.[327] Leitend waren weiterhin fiskalische Erwägungen sowie der Schutzzollgedanke, der sich nach dem Ersten Weltkrieg durch nationalistische Ideologien weiter verfestigte.[328]

Die Nachkriegszeit war geprägt von dem Bestreben der Errichtung einer Zollunion in Europa.[329] Damit verbunden ist inzwischen ein liberales Leitbild prägend, das auf den Abbau von Zöllen und die Schaffung von Freihandelszonen hinwirkt, um so das Handelsvolumen und – damit verbunden – Wirtschaftskraft und Wohlstand zu steigern.

II. Die Europäische Union und die Entwicklung hin zu einem europäischen Binnenmarkt

Die europäische Integration war und ist auf ein Zusammenwachsen der nationalen Märkte und auf einen freien Verkehr von Menschen, Waren, Kapital und Dienstleistungen angelegt.

---

324 Witte/Wolffgang, Lehrbuch des Europäischen Zollrechts, S. 1.

325 Schwarz/Wockenfoth, Zollrecht, Einleitung Rn. 7 f.

326 Rüsken in Rüsken, Zollrecht, Einführung, S. 14 Rn. 33 f.

327 Rüsken in Rüsken, Zollrecht, Einführung, S. 14 Rn. 33 f.

328 Rüsken in Rüsken, Zollrecht, Einführung, S. 15 Rn. 35.

329 Rüsken in Rüsken, Zollrecht, Einführung, S. 15 Rn. 37 f.

Art. 9 des Vertrages zur Gründung der Europäischen Wirtschaftsgemeinschaften vom 25.03.1957 legt bereits die Gründung der Zollunion sowie die Einführung eines gemeinsamen Zolltarifs fest. Zum 01.07.1968 waren die Zolltarife der Gründungsmitgliedstaaten so weit angeglichen, dass eine Zolltarifunion bestand.[330] Eine weitergehende Harmonisierung wurde durch den Erlass von Verordnungen herbeigeführt, die schließlich mit der VO Nr. 2913/92 des Rates vom 12.10.1992 zum Zollkodex der Gemeinschaften als einheitliches Regelwerk zusammengefasst wurden. Dieser stellte jedoch noch an vielen Stellen einen Kompromiss der geltenden nationalen Rechtslage mit weiterhin vielen Verweisen ins nationale Recht und eine Konsolidierung vieler europäischer Vorschriften dar.[331] Die weitere Harmonisierung dieser Rechtsvorschriften, eine Anpassung an den technischen Fortschritt und die veränderten wirtschaftlichen und sicherheitspolitischen Rahmenbedingungen sollten durch den modernisierten Zollkodex mit der Verordnung Nr. 450/2008 vom 23.04.2008 erfolgen.[332] Die Anpassung bzw. Erstellung der IT-Systeme und der damit einhergehende Erlass der Durchführungsvorschriften sollte bis 2013 erfolgen. Die Anpassung der Regelungen an den Vertrag von Lissabon, fehlender Fortschritt bei der Einführung von IT-Systemen sowie zwischenzeitliche Rechtsänderungen haben dazu geführt, dass der Modernisierte Zollkodex (MZK) in der Form nicht mehr vollständig in Kraft treten konnte und stattdessen durch einen neuen Zollkodex der EU ersetzt wurde.[333]

III. Veränderte Anforderungen an den Zoll

„Traditionsgemäß ist die wichtigste Aufgabe des Zolls die Erhebung der Zölle und Agrarabgaben, also der Beitrag zum Gemeinschaftshaushalt; auch die Erhebung eines Teils der Mehrwertsteuern und Verbrauchssteuern für die Haushalte der Mitgliedstaa-

330 Weerth, Europäische Rechtsquellen des Zollrechts in AW-Prax 2002, S. 102.

331 Dazu ausführlicher Lux/Larrieu, Der Vorschlag für einen modernisierten Zollkodex – Teil I in ZfZ 2006, S. 301 ff.

332 Lux/Larrieu, Der Vorschlag für einen modernisierten Zollkodex – Teil I in ZfZ 2006, S. 302 ff.

333 Witte, Der neue Zollkodex der EU in AW-Prax 2012, S. 125.

ten gehört nach wie vor zu seinen wichtigsten Aufgaben. Gleichzeitig steht der Zoll heute jedoch im Mittelpunkt von Globalisierungsprozessen, die ihn im internationalen Handel zu einem Schlüsselfaktor für die Wettbewerbsfähigkeit von Wirtschaftsunternehmen und Ländern machen."[334]

1. Bedeutungsverlust des Zolls als Einnahmequelle

In Europa ist die klassische Rolle des Zolls als staatliche Einnahmequelle immer weiter auf dem Rückzug. Mit der Übertragung der Einnahmen aus Zöllen an die Europäischen Gemeinschaften ist sie aus dem Fokus der Mitgliedstaaten gerückt, stellt jedoch die einzige primäre Einnahmequelle der EG dar. Der Anteil der Zölle am Gesamthaushalt ist kontinuierlich rückläufig, was trotz gestiegenen Handelsvolumens auf eine Senkung der Zölle und den Abschluss von Präferenzabkommen und die einseitige Gewährung von Präferenzen zurückzuführen ist und ebenfalls als Indiz dafür gewertet werden kann, dass für die Mitgliedstaaten wie auch für die Gemeinschaft die Bedeutung von Zöllen als Einnahmequelle zurückgeht. 1997 lag der Anteil der Zölle am Gemeinschaftshaushalt bei 19,1 %, 1999 bei 17,3 %. In absoluten Zahlen fielen die Einnahmen von 14,193 Mrd. € 1997 auf 12 Mrd. € 2004.[335]

2. Zunehmende Steuerungs- und Lenkungsfunktion des Zolls

Mit dem Zollkodex der Gemeinschaften und dem europäischen Binnenmarkt ist der Zoll zunehmend als Instrument der europäischen Integration in den Mittelpunkt gerückt. Durch die Abschaffung der Grenzkontrollen war eine fortschreitende Vereinheitlichung der Rechtsvorschriften notwendig geworden, um an allen Außengrenzen ein einheitliches Kontrollniveau zu schaffen und die Effizienz des Binnenmarktes zu steigern. Eine administrative Zusammenarbeit der Behörden sollte die Qualität und Einheitlichkeit der Rechtsanwendung sicherstellen.

---

[334] KOM (2003) 452 endg., S. 9.

[335] Mitteilung der Kommission vom 8 Februar 2001, KOM(2001) 51 endg., S. 6.

Der Aufbau eines Kommunikationsnetzes wie auch eines Datenaustauschnetzes fand dafür Eingang in die Binnenmarktstrategie.[336]

Die Verwaltung der Außengrenzen wird als Teil einer umfassenden Handelspolitik gesehen, die den Handel fördern soll, indem Handelshemmnisse abgebaut werden und die Behörden Ressourcen effizienter nutzen.[337] Der Zoll übernimmt dabei direkt an der Außengrenzen neben seiner klassischen fiskalpolitischen Rolle unter anderem den Schutz des geistigen Eigentums oder die Kontrollen im Umwelt- und Gesundheitsbereich, denn sobald Waren im Binnenmarkt zirkulieren, können Versäumnisse nur schwer wieder korrigiert werden.[338] Dem Zoll kommt so eine Aufgabe in der Regulierung des Handels und eine Kontrollfunktion in der korrekten Anwendung der Gemeinschaftspolitiken zu.[339] Dadurch soll eine Weiterentwicklung hin zu einem europäischen „Heimatmarkt" realisiert werden.[340]

3. Zunahme des Handelsvolumens und Veränderungen in Osteuropa

Bereits Ende der 1990er-Jahre nahm das Handelsvolumen durch den Zusammenbruch des Ostblocks und den wachsenden Handel mit den ehemaligen Ostblockstaaten erheblich zu.[341]

Mit der „Customs 2000"-Initiative rückten durch den Anstieg von Kriminalität an den Außengrenzen sicherheitspolitische Aspekte auf die Agenda. Der Drogenhandel sollte bekämpft sowie die finanziellen Interessen der Gemeinschaft durch

---

336 Mitteilung der Kommission an den Rat KOM(93) 632 endg. „Die optimale Gestaltung des Binnenmarkts": Strategisches Programm" vom 22. Dezember 1993, i ff.

337 Mitteilung der Kommission an den Rat KOM(93) 632 endg. „Die optimale Gestaltung des Binnenmarkts": Strategisches Programm" vom 22. Dezember 1993, 2 ff.

338 Mitteilung der Kommission KOM(2001) 51 endg., S. 6 f.

339 Bericht der Kommission an den Rat und das Europäische Parlament, KOM(1998) 471 endg. Vom 24.07.1998 über die Durchführung des Programms Zoll 2000, S. 2 f.

340 Entscheidung Nr. 210/97/EG „Zoll 2000", S. 1.

341 Witte, Risikomanagement im Zollrecht – rechtliches Neuland oder bekanntes Terrain?, S. 41 ff.

Maßnahmen gegen Steuer- und Zollbetrug geschützt werden.[342] Als Instrumentarium zur Erreichung dieser Ziele sollte eine Umstellung der Zollverfahren auf EDV erfolgen, weiterhin sollten Risikoanalyseverfahren, Auswahlverfahren sowie Verfahren zur nachträglichen Kontrolle entwickelt werden.[343]

Diese Strategie wurde weiterverfolgt und präzisiert: Der Zoll sollte im nächsten Schritt auf eine papierlose Zollverwaltung und eine vollständige Nutzung von Informationstechnologie – in dem Zusammenhang wurde vermehrt der Begriff des „e-Zoll" verwendet – umgestellt werden.[344] Die Aus- und Weiterbildung der Zollbeamten zu diesem Zweck und der Umgang mit neuen Arbeitstechniken wie Risikoanalysen sollten die Grundlage für die Erfüllung der Herausforderungen des Zolls werden.[345] Das Aktionsprogramm wurde 1999 für die EU-Beitrittskandidaten ebenfalls geöffnet, um dauerhaft ein vergleichbares Schutzniveau an den zukünftigen Außengrenzen der EU aufzubauen.[346]

Mit dem Aktionsprogramm „Zoll 2007" lag der Schwerpunkt im Zollbereich noch auf der Betrugsbekämpfung, aufgrund gestiegener Betrugsfälle und Aktivitäten der organisierten Kriminalität in diesem Bereich.[347] Die Programmaktivitäten bezüglich der Kommunikations- und Informationsaustauschsysteme (CCN/CSI; DDS, NEVV; TARIC; TCO/TCT; EBTI/RTCE/EVCTA; TQS; IPR/AV; SUSPENSIONS) werden in Art. 5 der Entscheidung Nr. 253/2003/EG konkret benannt und aufgebaut.

---

342 Mitteilung der Kommission an den Rat „KOM(93) 632 endg. „Die optimale Gestaltung des Binnenmarkts": Strategisches Programm" vom 22. Dezember 1993, S. iiif.

343 Entscheidung Nr. 210/97/EG „Zoll 2000", S. 4 ff.

344 Mitteilung der Kommission KOM(2001) 51 endg., S. 14 ff.

345 Mitteilung der Kommission an den Rat „KOM(93) 632 endg. „Die optimale Gestaltung des Binnenmarkts": Strategisches Programm" vom 22. Dezember 1993, S. 52 f.

346 Entscheidung Nr. 105/200/EG des Europäischen Parlaments und des Rates vom 17. Dezember 1999, S. 3.

347 Entscheidung Nr. 253/2003/EG vom 11.02.2003 über ein Aktionsprogramm für das Zollwesen der Gemeinschaft („Zoll 2007"), S. L 37/1.

4. Veränderte Sicherheitslage durch den 11. September 2001

Die Anschläge auf das World Trade Center in New York und das Pentagon in Washington vom 11.11.2001 durch die Terrororganisation Al-Qaida veränderten die internationale Sicherheitslage. Der Schutz vor terroristischen Anschlägen rückte in den Mittelpunkt der öffentlichen Aufmerksamkeit.

Die EU-Kommission hat die Bedrohungsszenarien kategorisiert und die Bedrohungen durch gewöhnliche Straftäter und Terroristen, die Gesundheitsrisiken für Verbraucher, die Gefahren ausgehend von gefährlichen Produkten, die Risiken verbunden mit Umwelt- und Gesundheitsgefahren sowie die Risiken für die öffentliche Sicherheit als größte Bedrohungen für die Sicherheit der Gemeinschaft identifiziert.[348] Unmittelbar wird dabei im Zusammenhang mit terroristischen Aktivitäten die Verbringung verbotener Waren, wie atomarer, biologischer, chemischer Waffen oder Sprengstoff, in das Zollgebiet der Gemeinschaft in verbrecherischer Absicht als Bedrohung eingestuft. Weiterhin werden Formen des illegalen Handels zur Versorgung und Finanzierung von Terrororganisationen oder dem organisierten Verbrechen als Bedrohungsszenario verfolgt.

Ein ausreichender Schutz durch bis dato bestehende Konzepte wurde dabei von der Kommission weitgehend verneint. Defizite wurden bei den Zollkontrollen wie auch bei der Gleichmäßigkeit des Schutzniveaus an den Außengrenzen der Gemeinschaft ausgemacht.[349] Infolgedessen wurde die Entwicklung von Verfahren zum Schutz vor Anschlägen beschleunigt und rückte für den Zoll in den Mittelpunkt der Aufmerksamkeit. Dafür sollten die Tätigkeiten des Zolls vollständig reorganisiert und die Prozesse rationalisiert werden. Dies sollte durch eine Konzentration auf Risiken geschehen, die vor dem Passieren einer Ware ermittelt werden müssen. Die Ermittlung und die Kontrolle sonstiger Risiken sollten an andere Orte ausgelagert werden.[350] Die Entwicklung gemeinsamer Konzepte der

348 KOM(2003) 452 endg., S. 44 ff.

349 KOM(2003) 452 endg., S. 45 ff.

350 KOM(2003) 452 endg., S. 48.

Zollbehörden für Konzentrierungs- und Kooperationsmechanismen für die von Waren ausgehenden Gefahren, die Festlegung erforderlicher Mindeststandards für die Ausstattung der Zollbehörden mit Personal und Ausrüstung sowie eine verstärkte Zusammenarbeit mit den übrigen an den Außengrenzen tätigen Behörden sollte den Zoll auf die Bedrohungsszenarien besser ausrichten.[351]

Durch die Nutzung von Informationstechnologien und Risikoanalyseverfahren sollte der Schutz der Gesellschaft vor schädlichen und gefährlichen Erzeugnissen sichergestellt werden und gleichzeitig mit den Bedürfnissen des Handels in einem globalisierten Handelsverkehr und dem Bedürfnis nach Handelserleichterungen und einer schnellen Abfertigung in Einklang gebracht werden.[352] Dem Zoll fällt dadurch die Schlüsselrolle zu, zum einzigen Eingangsportal für alle sicherheitsrelevanten Aspekte (wie Gesundheits- und Umweltschutz) zu werden, um Doppelungen bei der Anmeldung von Waren zu vermeiden und deren Abfertigung zu beschleunigen. Über eine gemeinsame Schnittstelle sollen die nötigen Daten den zuständigen Behörden zugänglich gemacht werden.[353] Die Zollverfahren sollen dafür radikal vereinfacht und an die Bedürfnisse papierloser Verfahren, den Informationsaustausch der Behörden untereinander und mit den Wirtschaftsbeteiligten sowie an die Risikoanalyseverfahren angepasst werden.[354]

Mit zunehmendem Handel und seiner wirtschaftlichen Bedeutung rücken die Sicherheit der gesamten Lieferkette und die Rolle des Zolls bei der Bekämpfung des internationalen Terrorismus immer weiter in den Blickpunkt.[355] Ein europaweites elektronisches Zollsystem soll ein vollständig papierloses Umfeld für den Zoll schaffen und so eine zügige Kommunikation zwischen Behörden untereinander und zwischen Behörden und Wirtschaftsbeteiligten ermöglichen.[356]

---

351 KOM(2003) 452 endg., S. 56 ff.

352 KOM(2003) 452 endg., S. 5.

353 KOM(2003) 452 endg., S. 8.

354 KOM(2003) 452 endg., S. 11 ff.

355 Vgl. Europäische Kommission, Generaldirektion Steuern und Zollunion, Sicherheit der Lieferkette: Die Rolle des europäischen Zolls bei der Terrorismusbekämpfung, S. 1 ff.

356 Entscheidung Nr.70/2008/EG, KOM(2008) 169 endg.

5. Zwischenergebnis

Die Aufgaben des Zolls sind heute vielfältiger und seine Bedeutung trotz fallender Einnahmen aus Zöllen weiter gestiegen. Die herausragende Bedeutung des Binnenmarktes für die europäische Integration weist dem Zoll wichtige Steuerungs- und Lenkungsfunktionen der Gemeinschaftspolitiken zu.

Der durch die Globalisierung zunehmende internationale Handel und seine Bedeutung für die europäische Wirtschaft und damit verbundene Bedürfnisse nach Handelserleichterungen und schnellen und effizienten Abfertigungen an den Grenzen der Union auf der einen Seite und gleichzeitig dadurch auf der anderen Seite auch angestiegene Wirtschaftskriminalität und Aktivitäten des organisierten Verbrechens an den Außengrenzen sowie durch den internationalen Terrorismus verursachte Gefahren sowohl für die Wirtschaft als auch für die Sicherheit der Bürger lassen dem Zoll eine Schlüsselposition für die wirtschaftliche Entwicklung wie auch für die Sicherheit in der Union zukommen. Der Zoll wird dadurch zu einem „Wächter an den Pforten der Gemeinschaft".

IV. Die Rechtsgrundlagen

Das Zollrecht ist gekennzeichnet durch einen vielschichtigen Normenaufbau, bestimmt durch internationale Abkommen, Rechtsakte der Europäischen Union sowie nationale Gesetzgebung.

1. Das internationale Recht

Das General Agreement on Tariffs and Trade (GATT) und dessen Nachfolger, die Welthandelsorganisation (WTO) bilden die Grundlage des internationalen Außenhandelsrechts. Der WTO gehören inzwischen 157 Staaten an.[357] Der Weltzollorganisation (World Customs Organisation = WCO) gehören 179 Zoll-

[357] Stand 01.08.2014 (WTO-Homepage).

organisationen weltweit an und stehen für 98 % des Welthandels.[358] Das Hauptvertragswerk bildet die revidierte Kyoto-Konvention, die am 03.02.2006 in Kraft getreten ist und sich in einen verpflichtenden Hauptteil (Body of the Convention) und einen ebenfalls verpflichtenden allgemeinen Annexteil (Generals Annex) sowie weitere spezielle Annexteile (Specific Annexes) gliedert. Die Sicherheit des globalen Handels wie auch weitere Handelsvereinfachungen sollen durch das Framework of Standards to Secure and Facilitate Global Trade weiter vorangebracht werden.

Das „Framework of Standards" erkennt den internationalen Terrorismus wie auch das organisierte Verbrechen als Gefahr für die Sicherheit der Lieferkette und damit auch für den gesamten globalen Handel und die Weltwirtschaft.[359] Dem Zoll wird für die Sicherheit der Lieferkette eine einzigartige Rolle zugeschrieben, da er die Möglichkeit besitzt, Waren beim Grenzübertritt zu kontrollieren, wofür ein internationaler Rahmen geschaffen werden soll.[360]

Eine Säule des Framework sind die Zusammenarbeit und der Informationsaustausch der Zollverwaltungen untereinander, wofür ein elektronisches, automatisiertes Informationsaustauschsystem aufgebaut werden soll.[361] Weiterhin soll ein einheitliches Risikomanagement eingeführt werden und Informationen sollen dabei so früh wie möglich zu den Zollverwaltungen gelangen, um gefährliche Güter möglichst vor der Ankunft im Zielgebiet zu identifizieren.[362]

Die zweite Säule legt den Schwerpunkt auf die Zusammenarbeit zwischen den Zollverwaltungen und den Wirtschaftsbeteiligten, insbesondere einem AEO (Authorized Economic Operator)-Standard.[363] Die Maßnahmen sollen die Lieferkette sicherer machen und gleichzeitig den globalen Handel erleichtern.[364]

---

358 Stand 01.08.2014 (WTO Homepage).

359 Framework of Standards to Secure and Facilitate Global Trade, S. 1 ff

360 Framework of Standards to Secure and Facilitate Global Trade, S. 6.

361 Framework of Standards to Secure and Facilitate Global Trade, S. 6 ff.

362 Framework of Standards to Secure and Facilitate Global Trade, S. 6 ff.

363 Framework of Standards to Secure and Facilitate Global Trade, S. 33 ff.

364 Framework of Standards to Secure and Facilitate Global Trade, S. 1 ff.

2. Das Recht der Europäischen Union

Die Grundlage des Europäischen Zollrechts bildet das primäre Unionsrecht. Dies sind der Vertrag über die Europäische Union (EUV) sowie der Vertrag über die Arbeitsweise der Europäischen Union (AEUV). Als Lissaboner Vertrag bilden beide gleichrangig die Grundlage der Europäischen Union.[365] Die verschiedenen nebeneinanderstehenden Verordnungen zum Zollrecht wurden durch den am 01.01.1994 in Kraft getretenen Zollkodex der Gemeinschaften (VO (EWG) 2913/92) gebündelt. Schließlich ist zum 30.10.2013 der Zollkodex der Union – Verordnung 952/2013 – (Unionszollkodex bzw. UZK) in Kraft getreten, seit dem 01.05.2016 anwendbar und soll bis 2020 das bisherige Verfahren ersetzen.

a) Vertrag über die Europäische Union

Der Vertrag über die Europäische Union legt die europäischen Werte und Leitideen fest, bildet so das Fundament der Union und gibt ihr gleichsam eine Geschäftsgrundlage.[366]

Die Durchlässigkeit von Grenzen, infolgedessen die wirtschaftlichen, politischen, kulturellen und gesellschaftlichen Verflechtung irreversibel zunehmen und so dauerhaften Frieden, Sicherheit und Wohlstand in Europa garantieren, gehört zu den Kernanliegen des europäischen Gedankens. Die Errichtung eines europäischen Binnenmarktes wird deswegen bereits in Art. 3 Abs. 3 EUV unter den Zielen der Union festgelegt.

Die Union als Rechtsraum und als Raum der Sicherheit wird in ebenfalls Art. 3 Abs. 2 EUV statuiert. Die Notwendigkeit von Kontrollen an den Außengrenzen zur Kriminalitätsverhütung und Bekämpfung wird als Voraussetzung dafür mitgenannt. Art. 3 EUV stellt dabei keine Kompetenznorm, sondern einen rechtsverbindlichen Programmsatz dar, der sich an die Union und ihre Organe richte.[367]

---

365 Ruffert in Callies/Ruffert, EUV, Art. 1 AEUV Rn. 1 ff.; Streinz in Streinz, EUV, Art. 1 AEUV Rn. 1ff.; Schwarze in Schwarze, EU, Art. 1 AEUV Rn. 1ff.

366 Callies in Callies/Ruffert, EUV, Art. 2 EUV Rn. 31 f.; Callies, Europa als Wertegemeinschaft – Integration und Identität durch europäisches Verfassungsrecht in JZ 2004, S. 33 (1036, 1040).

367 Pechstein in Streinz, EUV, Art. 3 EUV Rn. 2 ff.

b) Vertrag über die Arbeitsweise der Europäischen Union (AEUV)

Während der EUV die „verfassungsrechtlichen Vorschriften" im Fokus hat, soll der Vertrag über die Arbeitsweise der Europäischen Union die Zuständigkeiten, die Arbeitsweise und Teile des materiellen Rechts regeln.

Art. 3 Abs. 1, lit. a) AEUV weist der Union die ausschließliche Zuständigkeit für die Zollunion zu. In Art. 26 ff. AEUV werden der Binnenmarkt und in Art. 28 ff. AEUV der freie Warenverkehr in ihren Grundsätzen geregelt. Die Grundlage für die Zusammenarbeit im Zollwesen zwischen den Mitgliedstaaten sowie den Mitgliedstaaten und der Kommission findet sich in Art. 33 AEUV. Sie ist lex specialis gegenüber der Verwaltungszusammenarbeit in Art. 197 AEUV und Ausdruck des europäischen Verwaltungsverbundes.[368] Vom Begriff des Zollwesens umfasst ist dabei die *„Gesamtheit der spezifischen Regelungen über den internationalen Warenhandel der Union"*.[369] Die Vorschrift dient dabei nicht als Ermächtigungsgrundlage für materiell-rechtliche Regelungen, sondern stellt einen Kompetenztitel für Verfahren und Organisation der Zusammenarbeit von Behörden untereinander dar.[370] Formen der Zusammenarbeit können neben der Amtshilfe vielfältige Formen des Austauschs oder der gegenseitigen Anerkennung sein.[371]

Die gemeinsame Handelspolitik ist im Fünften Teil, Titel 2 AEUV (Art. 206–207) festgelegt. Art. 206 AEUV bildet die Grundlage einer liberalen Handelspolitik, die durch Beseitigung von Beschränkungen im globalen Handelsverkehr zur Entwicklung des Handels beitragen soll. Der EuGH sieht die Norm in seiner Rechtsprechung als verbindlich an und überprüft die Handelspolitik der EU auf ihre Vereinbarkeit.[372]

---

368 Terhechte in Schwarze, EU-Kommentar, Baden-Baden 2012, Art. 33 AEUV Rn. 1 ff.

369 Ohler in Streinz, EUV/AEUV München 2012, Art. 33 AEUV Rn. 2 ff.

370 Ohler in Streinz, EUV/AEUV München 2012, Art. 33 AEUV Rn. 2 ff.

371 Ohler in Streinz, EUV/AEUV München 2012, Art. 33 AEUV Rn. 9.

372 Osteneck in Schwarz, EU Art. 207 AEUV Rn. 4; Rechtsprehung dazu: EuGH, Rs. C-112/80, Dürdeck/HZA Frankfurt/M, Slg. 1981, 1095, 1119 f.; Rs. 245/81, Edeka/BR Deutschland, Slg. 1982, 2745, S. 2757.

c) Vom Zollkodex der Gemeinschaften über den modernisierten Zollkodex zum Unionszollkodex

Mit der Bündelung gemeinschaftsrechtlicher zollrechtlicher Vorschriften stellte der Zollkodex der Gemeinschaften einen großen Fortschritt im europäischen Zollrecht dar. Die sich verändernde sicherheitspolitische Lage wie auch der technische Fortschritt machen ständige Anpassungen der Gesetzgebung auf diesem Gebiet jedoch notwendig. So trat der Modernisierte Zollkodex (MZK) am 11.05.2005 in Kraft. Die Einführung von funktionierenden IT-Systemen und entsprechenden Abläufen und der Erlass der damit verbundenen Durchführungsverordnung wurde bis spätestens 26.06.2013 veranschlagt. Probleme mit der technischen Umsetzung und die das Gesetz überholende technische Entwicklung sowie – mit dem Vertrag von Lissabon – die veränderte politische und juristische Situation haben zu einer kompletten Neufassung des Zollkodex – Unionszollkodex (UZK) geführt.

aa) Der Zollkodex der Gemeinschaften

Die wichtigste Errungenschaft des Zollkodex im Vergleich zur vorherigen Rechtslage ist die Zusammenfassung der zollrechtlichen Vorschriften in dieser Verordnung. Präzisiert und ergänzt wird der Zollkodex durch die Zollkodex-Durchführungsverordnung (ZK-DVO) Nr. 2454/93. In vielen Bereichen stellt er jedoch noch einen Kompromiss verschiedener nationaler Zollverfahren dar, was z. B. das Bestehen paralleler Zollverfahren erklärt.[373] Den an vielen Stellen nicht genügend harmonisierten nationalen Rechtsordnungen wird durch Verweise ins nationale Recht Rechnung getragen und dadurch werden Regelungsspielräume eröffnet.

Die durch die Sicherheitsänderungen in den Zollkodex eingebrachten Regelungen spiegeln das Bemühen wieder, die Sicherheit der Lieferkette zu erhöhen und gleichzeitig Handelserleichterungen durchzusetzen. Die Vorabanmeldung soll zu einer Erhöhung der Sicherheit beitragen, während der „Zugelassene Wirtschaftsbeteiligte (ZWB) (im Folgendem wird der Englische Begriff des AEO, Authorized Economic Operator, benutzt) den Handel erleichtern soll.

[373] Lux/Larrieu, Der Vorschlag für einen modernisierten Zollkodex – Teil I – in ZfZ 2006, S. 302 f.

bb) Der Modernisierte Zollkodex

Der Modernisierte Zollkodex (MZK) sollte das Zollrecht weiter vereinheitlichen und erneuern.[374] So wurden viele Verweise ins nationale Recht gestrichen und viele Zollvorschriften weiter harmonisiert.[375] Neben dem Zollkodex sollten vier weitere Verordnungen ersetzt und in das Regelwerk integriert werden[376]. Er ist am 24.06.2008 in Kraft getreten, war jedoch nicht vollständig anwendbar. Übergangsweise sollten die letzten Vorschriften des MZK zusammen mit der Durchführungsverordnung spätestens bis zum 24.06.2013 in Kraft treten und anwendbar sein. Ein nicht erfolgter Erlass der Durchführungsvorschriften aufgrund fehlender IT-Systeme und die Anpassung an den Vertrag von Lissabon haben zu einer kompletten Überarbeitung des Regelwerks geführt (nun als Zollkodex der EU), sodass der MZK nie vollständig anwendbar war.[377]

Der MZK sollte unter Miteinbeziehung von Informationstechnologien die Zollverfahren vereinfachen und zwischen den Mitgliedstaaten – besonders im Hinblick auf die Informationssysteme und den Datenaustausch – interoperabel gestalten, um so den Handel zu erleichtern und gleichzeitig Sicherheit zu gewährleisten.[378]

Im Bereich der Risikoanalyse sollte ein gleichwertiges Schutzniveau durch vereinbarte gemeinsame Risikokriterien herbeigeführt werden.[379] Art. 4 Nr. 25 ZK definiert hierfür erstmals den Begriff des Risikos, während Art. 4 Nr. 26 ZK das Risikomanagement erstmalig definiert. Die Risikoanalyse wird in Art. 13 ZK eingeführt. Mit Ausnahme von Stichprobenkontrollen wird die Risikoanalyse unter Verwendung automatisierter Datenverarbeitungsmethoden durchgeführt

374 Lux/Larrieu, Der Vorschlag für einen modernisierten Zollkodex – Teil II – in ZfZ 2006, S. 340.

375 Lux/Larrieu, Der Vorschlag für einen modernisierten Zollkodex – Teil II – in ZfZ 2006, S. 340.

376 Lux/Larrieu, Der Vorschlag für einen modernisierten Zollkodex – Teil I – in ZfZ 2006, S. 302.

377 Witte, Der neue Zollkodex der EU in AW-Prax 2012, S. 125.

378 Lux/Larrieu, Der Vorschlag für einen modernisierten Zollkodex – Teil I – in ZfZ 2006, S. 304 f.

379 Witte, Zollkodex 2005 Teil 1 in AW-Prax 2005, S. 236.

und bedarf dafür eines unionsweiten IT-Systems.[380] Dafür benötigte Daten sollen vorab elektronisch angemeldet und mit Mitteln der EDV verarbeitet werden, um eine frühzeitige Risikoanalyse zu ermöglichen.[381]

cc) Der Zollkodex der EU (Unionszollkodex – UZK)

Zum 20.02.2012 wurde mit dem Vorschlag für eine Verordnung zur Festlegung des Zollkodex der Europäischen Union eine komplette Neufassung des MZK vorgelegt.[382] Ein Inkrafttreten des UZK wurde vor dem 24.06.2013 anvisiert, um ein Inkrafttreten der Anwendbarkeit des MZK zu verhindern, dessen IT-Systeme nur zum Teil fertiggestellt waren.[383] Der UZK ist seit dem 01.05.2016 anwendbar.

Die neue elektronische Datenverarbeitungsumgebung soll bis spätestens 31.12.2020 einsatzbereit sein.[384] Dies verschiebt den bisherigen Termin der letztmöglichen Anwendbarkeit des MZK und soll so den Verwaltungen und den Wirtschaftsbeteiligten genug Zeit verschaffen, um ihre Investitionen zu tätigen und die Systeme auf die elektronischen Verfahren umzustellen.[385]

Die Neufassung des Zollkodex ermöglichte es zudem, Regelungen des MZK zu ersetzen, die sich als schwierig in der Umsetzung erwiesen haben.[386] Durch den Vertrag von Lissabon ist die Regelung der Durchführungsbestimmungen in einem einheitlichen Rechtsakt nicht mehr möglich, stattdessen wird zwischen delegierten Verordnungen (Art. 290 AEUV) und Durchführungsverordnungen (Art. 291 Abs. 2 AEUV) unterschieden. Der UZK stellt dabei als Verordnung im Sinne des Art. 289 AEUV einen im ordentlichen Gesetzgebungsverfahren erlassen Rechtsakt (Basisrechtsakt) dar, der die Ermächtigungen zum Erlass einer de-

380 Witte, Zollkodex 2005 Teil 2 in AW-Prax 2005, S. 284 f.

381 Witte, Zollkodex 2005 Teil 2 in AW-Prax 2005, S. 284 f.

382 COM(2012) 64 final.

383 COM(2012) 64 final, S. 3.

384 COM(2012) 64 final, S. 3.

385 COM(2012) 64 final, S. 3.

386 COM(2012) 64 final, S. 3.

legierten Verordnung oder einer Durchführungsverordnung enthalten soll.[387] Die Unterscheidung, ob es sich um eine Regelung ohne Gesetzescharakter handelt und ob nicht wesentliche Vorschriften geändert werden sollen und es sich darum um einen delegierten Rechtsakt handelt oder ob es einheitlicher Bedingungen zur Durchführung bedarf und darum eine Durchführungsverordnung erlassen werden sollte, dürfte im Einzelnen schwierig abzugrenzen sein.[388] Durchführungsbefugnisse sollen der Kommission im Bereich der Anwendung der Datenverarbeitung oder der gemeinsamen Risikokriterien übertragen werden.[389] Delegierte Rechtsakte sollen *„in Bezug auf die Bestimmung der zollbezogenen Daten, die mit Mitteln der elektronischen Datenverarbeitung auszutauschen und zu speichern sind, auf die Entwicklung elektronischer Systeme für diesen Zweck und auf die Einrichtung anderer Mittel für den Austausch und die Speicherung"* erlassen werden.[390]

3. Nationale Gesetzgebung

Der nationale Gesetzgeber regelt grundsätzlich alle Bereiche, die durch Verweis im ZK der nationalen Gesetzgebung zugewiesen sind. Mit fortschreitender Harmonisierung des Zollrechts verliert dieser Bereich jedoch immer weiter an Bedeutung. In den Bereich der nationalen Gesetzgebung fällt jedoch insbesondere die Verwaltungsorganisation, die im Zollverwaltungsgesetz (ZollVG) sowie im Gesetz über die Finanzverwaltung (FVG) geregelt ist. Das ZollVG sowie die Zollverordnung (ZollV) ergänzen zudem die Regelungen des Unionszollrechts.

4. Zwischenergebnis

Der zollrechtliche Schwerpunkt verlagert sich immer weiter vom nationalen ins unionale Recht. Mit jeder Novelierung zollrechtlicher Vorschriften auf unionaler Ebene nimmt der Grad an Harmonisierung und gemeinsamen Vorschriften zu.

387 Fuchs, Modernisierter Zollkodex und Komitologie in ZfZ 2011, S. 282 f.

388 Reuter, Modernisierung des Modernisierten Zollkodex in ZfZ 2012, S. 149 f.

389 COM(2012) final 64, S. 12.

390 COM(2012) final 64, S. 16.

Die Spielräume für nationale Regelungen werden so immer kleiner. Eine Anpassung der nationalen Vorschriften an den UZK steht noch aus.

V. Zwischenergebnis

Die sich immer weiter beschleunigende Globalisierung von Warenströmen sowie neue Herausforderungen an die Sicherheit der Lieferkette haben auch zu immer kürzeren Intervallen der Erneuerung des Zollrechts geführt. Das Tempo der Veränderungen lässt sich gut an der Tatsache ablesen, dass der MZK nicht vollständig in Kraft treten konnte, bevor er ersetzt wurde. Im Zollrecht findet eine Kumulierung der Aufgaben zur Sicherung der Grenzen und Interessen der Union an ihren Außengrenzen statt. Eine immer größere Rolle spielt dabei die Vernetzung der Zollverwaltungen und betroffenen Behörden untereinander. So soll mittels elektronischer Datenverarbeitung, insbesondere einer einheitlichen Risikoanalyse, überall an den Grenzen der Union das gleiche Sicherheitsniveau hergestellt werden.

Bei der inzwischen erreichten Regelungsdichte auf unionaler Ebene kann man von einem einheitlichen europäischen Rechtsgebiet sprechen.

3. Teil |
Der „IST-Zustand“ des Sicherheitsstandards der postalischen Lieferkette

Nach Festlegung des die postalische Lieferkette betreffenden Rechtsrahmens und der Grundlagen im Datenschutz-, im Post- und im Zollrecht, gilt es davon ausgehend, die sicherheitsrelevanten Ist-Prozesse der postalischen Lieferkette aus juristischer Perspektive zu untersuchen.

So ist im Importprozess dafür das Verfahren der Zollanmeldung im Postverkehr zu untersuchen. Das zollrechtliche Verfahren bildet dabei den Ausgangspunkt für das bisherige Sicherheitsniveau. Nach diesem richten sich der Umfang und die Qualität der erhobenen Daten sowie darauf aufbauend der Umfang der Sicherheitskontrollen und damit verbundenen Risikoanalyse.

Erst auf den Ergebnissen der gegenwärtigen Prozesse und Sicherheitslage aufbauend ist es möglich, Grenzen und Varianten der Risikoanalyse und von Sicherheitskontrollen aufzuzeigen.

A. Das Verfahren der Zollanmeldung im Postverkehr

„Zur Gewährleistung gleicher Wettbewerbsbedingungen zwischen Postbetreibern und anderen Betreibern sollte ein einheitlicher Rahmen für die Zollabfertigung von Briefsendungen und Postsendungen geschaffen werden, um den Einsatz elektronischer Systeme zu ermöglichen. Im Hinblick auf die Erleichterung des Handels sowie die Verhinderung von Betrug und den Verbraucherschutz sind geeignete, umsetzbare Vorschriften für die Anmeldung von Brief- und Postsendungen bei den Zollbehörden festzulegen, wobei die Verpflichtung der Postbetreiber zur Bereitstellung eines Universalpostdienstes gemäß den einschlägigen Vorschriften des Weltpostvereins gebührend zu berücksichtigen ist."[391]

I. Die summarische Anmeldung

Die Zollstelle führt grundsätzlich das Risikomanagement aufgrund der Daten durch, die mit der summarischen Anmeldung (Art. 127 UZK) vor dem körperlichen Verbringen der Waren in das Zollgebiet der EU abgegeben werden.

II. Die Ausnahme von der Vorabanmeldung gemäß Art. 104 delegierte Verordnung (EU) 2015/2446

Für die Zollanmeldung im Postverkehr ergibt sich aus Titel IV Kapitel 1 Art. 104 Abs. 2 der delegierten Verordnung (EU) 2015/2446 eine Befreiung von der Verpflichtung zur Abgabe einer summarischen Eingangsanmeldung.[392]

---

391 DELEGIERTE VERORDNUNG (EU) 2015/2446 DER KOMMISSION vom 28. Juli 2015 zur Ergänzung der Verordnung (EU) Nr. 952/2013 des Europäischen Parlaments und des Rates mit Einzelheiten zur Präzisierung von Bestimmungen des Zollkodex der Union, Erwägungsgrund Nr. 6.

392 Nach dem ZK richtete sich die Befreiung nach Art. 36a ZK, 36c ZK i. V. m. Art. 181c, lit. d), 237 ZK-DVO im Postverkehr für bestimmte Waren, die als angemeldet galten.

Diese Befreiung gilt bis zum 31.12.2020 und betrifft Postsendungen deren Gewicht 250 g nicht übersteigt. Für Postsendungen deren Gewicht 250 g übersteigt, werden keine Sanktioen verhängt. Bei Gestellung der Waren wird eine Risikoanalyse vorgenommen, soweit verfügbar anhand der diese Waren betreffenden Anmeldung zur vorübergehenden Verwahrung oder der Zollanmeldung.

1. Fiktion der Anmeldung nach Art. 138 delegierte Verordnung (EU) 2015/2446

Nach Art. 138 e–f) delegierte Verordnung (EU) 2015/2446 gelten Briefesendungen sowie Waren in Postsendungen, die gemäß den Art. 23 bis 27 der Verordnung (EG) Nr. 1186/2009 von den Einfuhrabgaben befreit sind, als zur Überlassung zum zollrechtlich freien Verkehr gemäß Art. 141 delegierte Verordnung (EU) 2015/2446 angemeldet.

Nach Art. 23 Verordnung (EG) Nr. 1186/2009 sind von den Eingangsabgaben vorbehaltlich des Art. 24 Verordnung (EG) Nr. 1186/2009 Sendungen von Waren mit geringem Wert, die unmittelbar aus einem Drittland an einen Empfänger in der Gemeinschaft versandt werden befreit. Als „Waren mit geringem Wert" im Sinne von Art. 23 Abs. 1 Verordnung (EG) Nr. 1186/2009 gelten Waren, deren Gesamtwert je Sendung 150 € nicht übersteigt. Art. 24 Verordnung (EG) Nr. 1186/2009 schließt alkoholische Erzeugnisse, Parfums und Toilettewasser, Tabak und Tabakwaren von der Befreiung aus.

Von den Eingangsabgaben befreit sind vorbehaltlich der Art. 26 und 27 Verordnung (EG) Nr. 1186/2009 nach § 25 Abs. 1 Verordnung (EG) Nr. 1186/2009 Waren, die in Sendungen von einer Privatperson aus einem Drittland an eine andere Privatperson im Zollgebiet der Gemeinschaft gerichtet werden, sofern es sich um Einfuhren handelt, denen keine kommerziellen Erwägungen zugrunde liegen. Als „Einfuhren, denen keine kommerziellen Erwägungen zugrunde liegen" im Sinne des Art. 25 Abs. 1 gelten nach Abs. 2 Einfuhren in Sendungen, die gelegentlich erfolgen; sich ausschließlich aus Waren zusammensetzen, die zum persönlichen Ge- oder Verbrauch des Empfängers oder von Angehörigen seines

Haushalts bestimmt sind und weder ihrer Art noch ihrer Menge nach zu der Annahme Anlass geben, dass die Einfuhr aus geschäftlichen Gründen erfolgt und der Empfänger vom Absender ohne irgendeine Bezahlung zugesandt erhält.

Die Befreiung nach Art. 25 Abs. 1 Verordnung (EG) Nr. 1186/2009 wird je Sendung bis zu einem Gesamtwert von 45 €, einschließlich des Wertes der in Art. 27 Verordnung (EG) Nr. 1186/2009 genannten Waren, gemäß Art. 26 Abs. 1 Verordnung (EG) Nr. 1186/2009 gewährt. Übersteigt der Gesamtwert mehrerer Waren je Sendung den in Abs. 1 angegebenen Betrag, so gilt gemäß Art. 26 Abs. 2 Verordnung (EG) Nr. 1186/2009 die Befreiung bis zur Höhe dieses Betrages für diejenigen Waren, für die sie bei gesonderter Einfuhr gewährt worden wären; eine Aufteilung des Wertes der einzelnen Waren ist hierbei nicht zulässig.

Weitere mengenmäßige Bewchränkungen legt Art. 27 Verordnung (EG) Nr. 1186/2009 fest.

2. Zollanmeldung für Waren in Postsendungen nach Art. 144 delegierte Verordnung (EU) 2015/2446

Nach Art. 144 delegierte Verordnung (EU) 2015/2446 kann ein Postbetreiber für die Überlassung von Waren in Postsendungen zum zollrechtlich freien Verkehr eine Zollanmeldung mit einem reduzierten Datensatz gemäß Anhang B abgeben. Voraussetzung dafür ist, dass der Wert der Waren höchstens 1000 € beträgt, kein Antrag auf Erlass oder Erstattung gestellt wurde und diese keinem Verbot oder keiner Beschränkung unterliegen.

3. Notwendiger Datensatz

Der notwendige Datensatz für die Zollanmeldung richtet sich gemäß Art. 144 delegierte Verordnung (EU) 2015/2446 nach dem reduzierten Datensatz im Anhang B. Die Spalte F4c legt für Postsendungen einen Mindestdantensatz fest, der den Angaben der CN 23 Zollinhaltserklärung entspricht.

Die Zollinhaltserklärung CN 23 sieht folgenden Datensatz vor: die Absenderanschrift, die Anschrift des Endempfängers, das Land des Empfängers, ein detaillierte Beschreibung des Inhaltes, die Menge, die Nettogewichte und das Bruttogewicht (Paketgewicht), den Warenwert und die Währung, die Zolltarifnummern und den Ursprung der Waren, das deutsche Inlandporto (also 3,90 € bis 2 kg, 5,90 € bis 10 kg, 8,90 € bis 20 kg, 12,90 € bis 30 kg) die Art der Sendung, das Datum und die Unterschrift.

Der vollständige Datensatz nach Anhang B Spalte F4a sieht deutlich umfangreichere Informationspflichten vor. So werden unter anderem die Referenznummer/UCR, die Versender Sammelbeförderungsverträge, die Kennummer des Versenders und des Empfängers verlangt.

III. Zwischenergebnis

Nach Art. 104 Abs. 2 der delegierten Verordnung (EU) 2015/2446 ist der Postverkehr von der Abgabe einer summarischen Eingangsanmeldung befreit. Nach Art. 138 e–f) delegierte Verordnung (EU) 2015/2446 besteht eine Anmeldungsfiktion für Postsendungen und bestimmte Waren in Postsendungen. Der Datensatz für eine Anmeldung richtet sich weiter nach dem Datensatz der Zollinhaltserklärung CN 23.

B. Datenschutzrechtliche Konsequenzen des Verfahrens der Zollanmeldung im Postverkehr

Die Ausnahmetatbestände der delegierten Verordnung (EU) 2015/2446, führen zu unterschiedlichen Datensätzen, die für eine Risikoanalyse überhaupt zur Verfügung stehen. Es gilt zu untersuchen, welche Konsequenzen sich für den Datenschutz, besonders unter den Gesichtspunkten der Datenvermeidung und Datensparsamkeit als wesentlichen Ordnungsprinzipien des Datenschutzrechts, durch die Verwendung der unterschiedlichen Datensätze ergeben könnten. Daraus lässt sich ein Überblick über mögliche Auswirkungen und Konsequenzen für den Schutz von Daten durch die Anwendung der qualitativ und quantitativ unterschiedlichen Datensätze ableiten.

Hierzu ist zunächst der Anwendungsbereich des Bundesdatenschutzgesetzes zu untersuchen. Anschließend sind die Grundsätze der Datenvermeidung und Datensparsamkeit herauszuarbeiten und die Datensätze daran zu messen.

I. Anwendungsbereich des BDSG

Zunächst ist zu untersuchen, ob und inwieweit die Datensätze in den Anwendungsbereich des BDSG fallen. Der Zweck und der Anwendungsbereich des Gesetzes sind in § 1 BDSG geregelt. Das Gesetz gilt gemäß § 1 Abs. 2 BDSG *„für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch 1. öffentliche Stellen des Bundes, 2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie a) Bundesrecht ausführen oder b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt, 3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es*

sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten."

1. Territoriale Geltung

§ 1 Abs. 5 S. 2 BDSG stellt das Territorialprinzip her, indem es Firmen mit Sitz in anderen Staaten (Nicht-EU-Länder und Nicht-Vertragsstaaten) von der Privilegierung nach dem Sitzprinzip ausnimmt.[393]

2. Personenbezogenheit der Daten

Es müssten gemäß § 1 Abs. 1 BDSG personenbezogene Daten vorliegen. Der Begriff der personenbezogenen Daten ist in § 3 Abs. 1 BDSG legaldefiniert und meint *„Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)"*. Eine solche Definition findet sich ebenfalls in anderen Gesetzen.[394] Die besonderen Arten personenbezogener Daten sind in Art. 3 Abs. 9 BDSG aufgezählt: Dies *„sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben"*.

Unter Einzelangaben versteht man jede Information, die sich auf einzelne bestimmte oder bestimmbare Personen bezieht.[395] Darunter fallen auch die Adresse oder Anschrift sowie Namen, oder diesen ersetzende Angaben oder Nummern, falls sich ein Personenbezug herstellen lässt.[396] Aggregierte, d. h. zusammengefasste, Daten sind keine personenbezogenen Daten.[397] Die Einbeziehung der persönlichen und sachlichen Verhältnisse verdeutlicht die umfassende Anwendung

393 Caspar, Geoinformationen und Datenschutz am Beispiel des Internetdienstes Google Street View in DÖV 2009, S. 965.

394 So in § 203 Abs. 2 S. 2 StGB, sowie in § 16 Abs. 1 des Gesetzes über die Statistik für Bundeszwecke.

395 Gola/Schomerus, BDSG, § 3 Rn. 2.

396 Gola/Schomerus, BDSG, § 3 Rn. 3.

397 Gola/Schomerus, BDSG, § 3 Rn. 3.

des Begriffs der personenbezogenen Daten.[398] Geschützt sind vom BDSG zudem nur natürliche Personen. Juristische Personen sowie Personengruppen sind nicht umfasst und werden nur vom allgemeinen Persönlichkeitsrecht geschützt.[399]

Im Weiteren ist zu untersuchen, inwieweit Angaben der CN 23 Zollinhaltserklärung sowie sowie der vollständige Datensatz nach Anhang B Spalte 4a delegierte Verordnung (EU) 2015/2446 in den Anwendungsbereich des BDSG fallen.

a) CN 23

Es ist zu untersuchen, ob der Datensatz der Zollinhaltserklärung CN 23 (der Anhang B Spalte F4c delegierte Verordnung (EU) 2015/2446 entspricht) in den Anwendungsbereich des BDSG fällt.

Insbesondere die Adressangaben stellen hier unstrittig personenbezogene Daten dar.[400] Es kann sich zwar im Einzelfall bei den Betroffenen um juristische Personen handeln, jedoch grundsätzlich auch um natürliche Personen, weswegen die Angaben weiter zu untersuchen sind. Diese Angaben stellen folglich (für den Fall von Angaben einer natürlichen Person) personenbezogene Daten dar.

Die weiteren Angaben, das Land des Empfängers, eine detaillierte Beschreibung des Inhalts, die Menge, die Nettogewichte und das Bruttogewicht (Paketgewicht), der Warenwert und die Währung, die Zolltarifnummern und der Ursprung der Waren, das deutsche Inlandsporto (also 3,90 € bis 2 kg, 5,90 € bis 10 kg, 8,90 € bis 20 kg, 12,90 € bis 30 kg), die Art der Sendung und das Datum beziehen sich auf die Postsendung und stellen damit isoliert verarbeitet nicht personenbezogene Sachdaten dar.

Auf der Zollinhalterklärung gemeinsam abgegeben und miteinander verknüpft, lassen die Sachdaten zusammen mit den Identifizierungsdaten jedoch auch Rückschlüsse auf die wirtschaftlichen oder persönlichen Verhältnisse zu und sind deswegen als personenbezogen zu qualifizieren.

---

398 Gola/Schomerus, BDSG, § 3 Rn. 5.

399 Gola/Schomerus, BDSG, § 3 Rn. 11.

400 Schaffland/Wiltfang, BDSG, § 3 Rn. 5.

b) Vollständiger Datensatz Anhang B, Spalte 4a delegierte Verordnung (EU) 2015/2446

Weiter ist der vollständige Datensatz Anhang B, Spalte 4a delegierte Verordnung (EU) 2015/2446 zu untersuchen.

Es handelt beim vollständigen Datensatz nach Anhang B, Spalte 4a, um einen gegenüber der CN 23 Zollinhaltserklärung ausgebauten Datensatz, sodass dieser erst Recht als personenbezogen zu qualifizieren ist.

Die zusätzlichen Informationen über den Empfänger und Versender sind unstrittig als personenbezogen zu qualifizieren, denn sie enthalten potenziell eine Information über eine natürliche Person, die sie identifizierbar macht.

Isoliert betrachtet stellen die weiteren sendungsbezogenen Daten keine personenbezogenen Daten dar. Sie beziehen sich nicht auf eine Person, sondern auf die zu befördernde Postsendung. *„Angaben, die eine Sache bestimmen oder beschreiben, sind Angaben über diese Sache, aber keine Angaben über Personen, die zu der Sache objektiv eine spezifische Beziehung haben, zu deren Existenz und Natur die Verarbeitung selbst aber keinerlei Kontext herstellt."*[401] Es handelt sich bei den Angaben, deren Informationswert sich auf die Postsendung bezieht, somit zunächst um Sachdaten, die isoliert verarbeitet keine personenbezogenen Daten darstellen.[402]

Fraglich erscheint, inwieweit diese Angaben miteinander verknüpft einen Informationsgehalt über die sozialen oder wirtschaftlichen Verhältnisse aufweisen. Hier ist die Verarbeitung des gesamten Datensatzes im Zusammenhang zu betrachten. Werden die Sachdaten gemeinsam mit den Identifikationsdaten und sonstigen personenbezogenen Daten gemeinsam erhoben und miteinander verknüpft, erlauben sie Rückschlüsse auf die berufliche Tätigkeit, wirtschaftliche oder private Verhältnisse und ermöglichen so eine Profilbildung. Damit ist der Datensatz des Anhangs B Spalte 4a der delegierten Verordnung (EU) 2015/2446 in seiner Gesamtheit als personenbezogen einzustufen.

---

401 Dammann in Simitis, BDSG, § 3 Rn. 59. MMR 2010, S. 17 ff. 20 ff.

402 Dammann in Simitis, BDSG, § 3 Rn. 59.

c) Zwischenergebnis

Die Datensätze des Anhangs B Spalte 4a der delegierten Verordnung (EU) 2015/2446 wie auch der Zollinhaltserklärung CN 23 sind in ihrer Gesamtheit aufgrund der gemeinsam abgegebenen Datensätze und ihrer möglichen Verknüpfungen und dadurch möglichen Rückschlüsse als personenbezogen zu qualifizieren.

3. Normadressaten

Des Weiteren gilt das Gesetz gemäß § 1 Abs. 2 BDSG für die Verarbeitung von *„Daten durch 1. öffentliche Stellen des Bundes, 2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie a) Bundesrecht ausführen oder b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt, 3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten."*

a) Die Zollbehörden

Die Zollbehörden stellen gemäß § 1 FVG unstrittig öffentliche Stellen des Bundes dar.[403]

b) Die Deutsche Post AG (DPAG)

Weiterhin könnte die DPAG Normadressat sein. Dies könnte als nicht-öffentliche Stelle gemäß § 1 Abs. 2 Nr. 3 BDSG der Fall sein. Nicht-öffentliche Stellen sind in § 2 Abs. 4 BDSG als *„natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen"*, definiert. Ein Ausschluss gilt für die Nutzung von Daten für persönliche oder familiäre Tätigkeiten. Dies ist hier nicht der Fall.

[403] Witte in Witte, ZK, Art. 4, S. 84.

Weiterhin ist dies der Fall, insofern eine Verarbeitung der Daten unter Einsatz von Datenverarbeitungsanlagen gemäß § 1 Abs. 2 Nr. 3 BDSG erfolgt.

4. Zwischenergebnis

Das BDSG ist auf die Untersuchung des Anhangs B Spalte 4a der delegierten Verordnung (EU) 2015/2446 sowie der Zollinhaltserklärung CN 23 anwendbar.

II. § 3a BDSG, Datenvermeidung und Datensparsamkeit

Die Grundsätze der Datenvermeidung und Datensparsamkeit sind in § 3a BDSG niedergelegt. *„Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert".*

1. Schutzumfang

Diese Grundsätze stellen Programmsätze bzw. Zielvorgaben dar.[404] Der Datenschutz soll damit präventiv zu einem Datenschutz durch Technik werden.[405] Die Datenverarbeitung soll dabei so gestaltet werden, dass möglichst wenig personenbezogene Daten, und das – falls möglich – anonymisiert und pseudonymisiert, für einen bestimmten Vorgang verwendet werden.

Die Zielvorgabe der Datenvermeidung ist zweistufig aufgebaut.

---

404 Gola/Schomerus, BDSG, § 3a Rn. 2; jedoch streitig, anders Scholz in Simitis, BDSG, § 3a Rn. 27 f.

405 Bizer, Datenschutz als Gestaltungsaufgabe in DuD 2007, S. 725.

Auf der ersten Stufe sollen möglichst keine personenbezogenen Daten erhoben werden. Wo keine personenbezogenen Daten erhoben werden, müssen keine besonderen Anstrengungen zu ihrem Schutz erhoben werden.

Auf der zweiten Stufe gilt es die datenverarbeitenden Prozesse so zu organisieren und die datenverarbeitenden Systeme so auszuwählen, dass die Erhebung und Verwendung der Daten minimiert wird. Hier kann man von Datensparsamkeit sprechen.[406] Die Verfahren und Systeme sind unter den Gesichtspunkten der Qualität und Quantität der Erhebung personenbezogener Daten zu untersuchen. Die Datenmenge ist so weit es geht zu reduzieren, und soweit möglich, zu anonymisieren und zu pseudonymisieren. Die Eingriffstiefe ist damit zu verringern. Die Prüfung geht dabei über das Erforderlichkeitsprinzip hinaus, indem eine aktive Gestaltung der technischen Prozesse zur Reduzierung der Datenmenge gefordert wird.

Dieses Ziel kann erreicht werden, indem man

- auf die Erhebung bestimmter personenbezogener Daten verzichtet
- ihre Ausgabe in einer bestimmten Form unterbindet (z. B. als Ausdruck)
- Daten schnellstmöglich wieder löscht oder Verfallsdaten festlegt
- sie anomymisiert und pseudonymisiert
- auf die Verknüpfung bestimmter Datensätze verzichtet
- den Zugang zu den Daten möglichst begrenzt und den beteiligten Akteuren nur die für sie notwendigen Daten zukommen lässt
- eine verteilte Speicherung vornimmt und dadurch eine Form der informationellen Gewaltenteilung vornimmt – eine Datentrennung kann die Zweckbindung der Verarbeitung sichern.[407]

406 Scholz in Simitis, BDSG, § 3a Rn. 31.

407 Scholz in Simitis, BDSG, § 3a Rn. 33 ff.

Die Auswahl und Gestaltung von Datenverarbeitungssystemen umfasst den Hardware- und den Softwarebereich.[408] Die Datenverarbeitungssysteme sind so zu gestalten, dass sie die Privatsphäre von vornherein schützen. Die Standardeinstellungen sind in der Grundeinstellung entsprechend einzustellen.

2. Untersuchung der gegenwärtigen Situation

An diesen Vorgaben ist die gegenwärtige Situation zu messen und zu untersuchen.

Art. 138 e–f) delegierte Verordnung (EU) 2015/2446

Durch die Fiktion des Art. 138 e–f) delegierte Verordnung (EU) 2015/2446 kommt der vollständige Datensatz aus Anhang B, Spalte 4a delegierte Verordnung (EU) 2015/2446 nicht zur Anwendung. Die Folge ist, dass der reduzierte Datensatz gleich der CN 23 Zollinhaltserklärung erhoben wird.

Eine Rücknahme der Fiktion würde zu einer massiven quantitativen wie auch qualitativen Ausweitung der Erfassung und Verarbeitung personenbezogener Daten führen.

3. Zwischenergebnis

Die bisherigen Ausnahmeregelungen führen im Vergleich zur Anwendung des vollständigen Datensatzes aus Anhang B, Spalte 4a delegierte Verordnung (EU) 2015/2446 zur Erhebung von weniger personenbezogenen Daten und erfüllen damit die Zielvorgabe der Datenvermeidung und Datensparsamkeit. Die Rücknahme der Ausnahmeregelung würde zu einer Anwendung des vollständige Datensatzes aus Anhang B, Spalte 4a delegierte Verordnung (EU) 2015/2446 und damit zu einer quantitativ und qualitativ intensivierten Verarbeitung personenbezogener Daten führen. Diese müsste neben den Grundsätzen der Verhältnismäßigkeit und Erforderlichkeit im eigentlichen Sinne auch an den Zielvorgaben der Datenvermeidung und Datensparsamkeit gemessen werden. Unter den Gesichts-

[408] Scholz in Simitis, BDSG, § 3a Rn. 39.

punkten der Datenvermeidbarkeit und Datensparsamkeit müssten in der Folge Systeme, Verfahren, technische Prozesse und Programme zur Risikoanalyse entsprechend ausgestaltet werden.

III. Ergebnis

Der derzeitige Status quo erfüllt die gesetzlichen Vorgaben an Datenvermeidung und Datensparsamkeit. Die Angaben der Zollinhaltserklärung CN 23 sind weniger umfangreich, enthalten jedoch noch die wesentlichen Angaben zur Sendung.

C. Risikoanalyse

Die Risikoanalyse ist ein Instrument zur Identifikation von Risiken durch EDV-gestützte Auswertung von Datensätzen. Eine Risikoanalyse ist dabei kein Spezifikum zur Sicherung der Lieferkette, sondern ein Instrument, das mit steigender Zunahme elektronischer Datenverarbeitung in immer weitere Lebensbereiche vordringt. Für die Sicherung der Lieferkette, ist zwischen einer gesetzlich verankerten Risikoanalyse durch die Zollbehörden und einer weitergehenden Risikoanalyse durch Postdiensteanbieter zu unterscheiden.

I. Die „zollrechtliche Risikoanalyse“

Der Zollkodex bildet den Ausgangspunkt für die Risikoanalyse im Zollrecht, in dem diese mit der ÄnderungsVO (EG) Nr. 648/2005 des Europäischen Parlaments und des Rates vom 13.04.2005 verankert wurde. Die Risikoanalyse hat hier Eingang gefunden in die Vorschriften Art. 4 Nr. 4a ZK, Art. 13 Abs. 2 ZK, Art. 36b Abs. 1 ZK, sowie Art. 182d Abs. 1 ZK. Ziel war es, aufgrund gemeinsamer Risikokriterien ein gleichwertiges Schutzniveau an den Grenzen der Gemeinschaft herzustellen.[409] Abgelöst wurden die Regelungen von Art. 5 Nr. 25, 12, 46, 47 UZK.

1. Begriffsbestimmungen

Voraussetzung für ein Verständnis der Risikoanalyse ist zunächst die Bestimmung der Begriffe „Risikoanalyse“ und „Risiko“.

a) Begriff der Risikoanalyse

Der Begriff der Risikoanalyse wird im UZK nicht legaldefiniert. Eine Annäherung bietet der Begriff des Risikomanagements aus Art. 5 Nr. 25 UZK: *„Risiko-*

[409] Verordnung EG Nr. 648/2005, S. 1.

management ist die systematische Ermittlung von Risiken, auch durch Stichproben, und die Anwendung aller für die Risikobegrenzung erforderlichen Maßnahmen."

Art. 4 Nr. 26 ZK war sogar im Hinblick auf Datenverarbeitung präziser: *„Risikomanagement: die systematische Ermittlung des Risikos und Durchführung aller zur Begrenzung des Risikos erforderlichen Maßnahmen. Dazu gehören Tätigkeiten wie das Sammeln von Daten und Informationen, die Analyse und Bewertung von Risiken, das Vorschreiben und Umsetzen von Maßnahmen sowie die regelmäßige Überwachung und Überarbeitung dieses Prozesses und seiner Ergebnisse auf der Basis internationaler, gemeinschaftlicher und einzelstaatlicher Quellen und Strategien."*

b) Begriff des Risikos

Der Begriff des Risikos ist hingegen in Art. 5 Nr. 7 UZK definiert: *„Risiko ist die Wahrscheinlichkeit, dass im Zusammenhang mit dem Eingang, dem Ausgang, dem Versand, der Beförderung oder der Endverwendung von zwischen dem Zollgebiet der Union und Ländern oder Gebieten außerhalb dieses Gebiets beförderten Waren oder mit im Zollgebiet der Union befindlichen Nicht-Unionswaren, ein Ereignis und die Auswirkungen eintreten, durch die die vorschriftsmäßige Anwendung von Maßnahmen der Union oder ihrer Mitgliedstaaten verhindert wird, die finanziellen Interessen der Union und ihrer Mitgliedstaaten bedroht werden oder die Sicherheit und der Schutz der Union und ihrer Bewohnern, die Gesundheit von Menschen, Tieren oder Pflanzen, die Umwelt oder die Verbraucher gefährdet werden".*

In der Literatur wurde die bisherige Definition des Art. 4 Nr. 25 ZK[410] als unvollständig kritisiert, da sie nur die Sicherheit der Gemeinschaft, die öffentliche Verwaltung, die Umwelt und die Verbraucher erwähnte.[411] Art. 5 Abs. 2 ZK listete jedoch zusätzlich als Verbots- oder Beschränkungsgründe die öffentliche Sittlich-

[410] Art. 4 Nr. 25 ZK: Risiko „die Wahrscheinlichkeit des Eintretens eines Vorfalls im Zusammenhang mit dem Eingang, dem Ausgang, dem Versand, der Beförderung und der besonderen Verwendung von Waren, die zwischen dem Zollgebiet der Gemeinschaft und Drittländern befördert werden, sowie im Zusammenhang mit dem Vorhandensein von Waren ohne Gemeinschaftsstatus, sofern dieser Vorfall die ordnungsgemäße Durchführung von Gemeinschafts- oder nationalen Maßnahmen verhindert oder den finanziellen Interessen der Gemeinschaft und ihrer Mitgliedstaaten schadet oder die Sicherheit der Gemeinschaft, die öffentliche Gesundheit, die Umwelt oder die Verbraucher gefährdet".

[411] Siehe auch Witte, Zollkodex 2005 in AW-Prax 2005, S. 237; Henke in Witte, ZK, Art. 13 Rn. 21.

keit, Ordnung oder Sicherheit zum Schutze der Gesundheit und des Lebens von Menschen, Tieren oder Pflanzen, des nationalen Kulturguts von künstlerischem, geschichtlichem oder archäologischem Wert oder des gewerblichen und kommerziellen Eigentums auf. Diese Aufzählung entsprach auch den Verbotsgründen in Art. 36 AEUV und war als grundsätzliche Wertung des Unionsrechts zu betrachten, dessen Einschränkung kaum intendiert gewesen sein kann.[412] Diese Berwertung ist auch auf den neuen Art. 5 Nr. 7 UZK zu übertragen.

Weiterhin hätte die Definition klarstellend um die handelspolitischen Maßnahmen bisher in Art. 1 Nr. 7 ZK-DVO verankert *(„nichttarifäre Maßnahmen, die im Rahmen der gemeinsamen Handelspolitik durch Gemeinschaftsvorschriften über die Regelungen für die Ein- und Ausfuhr von Waren getroffen worden sind, wie Überwachungs- und Schutzmaßnahmen, mengenmäßige Beschränkungen oder Höchstmengen sowie Ein- und Ausfuhrverbote")*, ergänzt werden können.[413]

2. Rechtsgrundlagen für die zollrechtliche Risikoanalyse

Art. 46 UZK „Risikomanagement und Zollkontrollen" bildet die Grundlage für die zollrechtliche Risikoanalyse:

„(1) Zu diesen Zollkontrollen gehören insbesondere die Beschau der Waren, die Entnahme von Proben und Mustern, die Überprüfung der Richtigkeit und Vollständigkeit der in einer Anmeldung oder Mitteilung gemachten Angaben sowie des Vorhandenseins, der Echtheit, Richtigkeit und Gültigkeit von Unterlagen, die Prüfung der Buchführung der Wirtschaftsbeteiligten und der sonstigen Aufzeichnungen, die Kontrolle der Beförderungsmittel, des Gepäcks und der sonstigen Waren, die von oder an Personen mitgeführt werden, sowie die Durchführung von behördlichen Nachforschungen und dergleichen.

(2) Mit Ausnahme von Stichproben erfolgen Zollkontrollen in erster Linie auf der Grundlage einer Risikoanalyse mit Mitteln der elektronischen Datenverarbeitung mit dem Ziel, anhand von auf einzelstaatlicher Ebene, Unionsebene und – soweit

412 Ebenso Witte, Zollkodex 2005 in AW-Prax 2005, S. 237.

413 Witte, Zollkodex 2005 in AW-Prax 2005, S. 237.

verfügbar – internationaler Ebene entwickelten Kriterien Risiken zu ermitteln und abzuschätzen und die erforderlichen Abwehrmaßnahmen zu entwickeln.

(3) Zollkontrollen werden innerhalb einesgemeinsamen Rahmens für das Risikomanagement durchgeführt, der auf dem Austausch risikobezogener Informationen und der Ergebnisse von Risikoanalysen zwischen den Zollverwaltungen beruht und gemeinsame Risikokriterien und Standards, Kontrollmaßnahmen und vorrangige Kontrollbereiche festlegt.

Auf diesen Informationen und Kriterien beruhende Kontrollen erfolgen unbeschadet anderer Kontrollen, die gemäß Abs. 1 oder gemäß anderen geltenden Vorschriften durchgeführt werden.

(4) Die Zollbehörden wenden Risikomanagementverfahren an, um die Höhe des Risikos zu bestimmen, das mit den der zollamtlichen Kontrolle oder Überwachung unterliegenden Waren verbunden ist, und um zu entscheiden, ob die Waren besonderen Zollkontrollen unterzogen werden und wo diese gegebenenfalls durchgeführt werden.

Dazu gehören Tätigkeiten wie das Sammeln von Daten und Informationen, die Analyse und Bewertung von Risiken, das Vorschreiben und Umsetzen von Maßnahmen sowie die regel mäßige Überwachung und Überprüfung dieses Prozesses und seiner Ergebnisse auf der Grundlage internationaler, unionsinter ner und einzelstaatlicher Quellen und Strategien.

(5) Die Zollbehörden tauschen risikobezogene Informationen und Ergebnisse von Risikoanalysen aus, wenn:

a) eine Zollbehörde die Risiken als beträchtlich einschätzt und eine Zollkontrolle für erforderlich erachtet und die Kontrolle ergeben hat, dass das Ereignis, das den Tatbestand eines Risikos schafft, eingetreten ist, oder

b) die Kontrolle zwar nicht ergeben hat, dass das Ereignis, das den Tatbestand eines Risikos schafft, eingetreten ist, die Zollbehörde jedoch der Auffassung ist, dass ein hohes Risiko an einem anderen Ort in der Union besteht.

(6) Bei der Festlegung von gemeinsamen Risikokriterien und Standards, der in Abs. 3 genannten Kontrollmaßnahmen und vorrangigen Kontrollbereiche ist alles Folgende zu berücksichtigen:

a) ein angemessenes Verhältnis zum Risiko,

b) die Dringlichkeit der erforderlichen Durchführung der Kontrollen,

c) die wahrscheinlichen Auswirkungen auf die Handelsströme, auf einzelne Mitgliedstaaten und auf die Kontrollressourcen.

(7) Die gemeinsamen Risikokriterien und Standards gemäß Abs. 3 umfassen alle folgenden Elemente:

a) eine Beschreibung der Risiken,

b) die Risikofaktoren oder -indikatoren, die bei der Auswahl von Waren oder Wirtschaftsbeteiligten für Zollkontrollen zu berücksichtigen sind,

c) die Art der von den Zollbehörden durchzuführenden Zollkontrollen,

d) die Dauer der Anwendung der unter Buchstabe c genannten Zollkontrollen.

(8) Unbeschadet der übrigen üblicherweise von den Zollbehörden durchgeführten Kontrollen umfassen die vorrangigen Kontrollbereiche bestimmte Zollverfahren, Arten von Waren, Verkehrswege, Beförderungsart oder Wirtschaftsbeteiligte, die in einem bestimmten Zeitraum einem höheren Maß der Risikoanalyse und Zollkontrollen unterworfen sind."

Diese Norm wurde im Vergleich zur Vorgängerregelung Art. 13 ZK deutlich ausgebaut und beschreibt den Vorgang und Ablauf der Risikoanalyse, als auch die Riskokriterien und Standards, die bisher teilweise in der ZK-DVO zu finden waren.

II. Die „Risikoanalyse durch Postdiensteanbieter"

Eine Risikoanalyse durch Postdiensteanbieter zur allgemeinen Gefahrenabwehr ist bisher gesetzlich weder geregelt noch verankert. Sie ist dabei nicht nur von der Risikoanalyse durch Zollbehörden zu unterscheiden, sondern sicherlich in Abhängigkeit vom Schwerpunkt der Datenverarbeitung von weiteren Security-

und Sicherheitsmanagement-Maßnahmen innerhalb eines Postdiensteanbieters zur Sicherung der eigenen Betriebsstätten und des Betriebsablaufs.

III. Zwischenergebnis

Eine mögliche Risikoanalyse zur allgemeinen Gefahrenabwehr durch Zollbehörden oder Postdienstleister unterscheidet sich deutlich in ihrem gegenwärtigen Regelungsniveau.

Es liegt ein Rechtsrahmen für eine Risikoanalyse durch Zollbehörden vor, auf den für eine Ausgestaltung der Risikoanalyse durch Zollbehörden zur allgemeinen Gefahrenabwehr innerhalb der postalischen Lieferkette zurückgegriffen werden kann.

Ein Äquivalent für eine Risikoanalyse durch Postdiensteanbieter existiert nicht.

D. Analyse des bestehenden Sicherheitsniveaus innerhalb der postalischen Lieferkette

Es gilt zu untersuchen, ob und inwieweit ein Risikomanagement bisher zur Sicherung der postalischen Lieferkette zum Einsatz kommt.

I. Gegenwärtige Anwendung der Risikoanalyse

Eine automatisierte Datenverarbeitung zwecks Risikoanalyse wird gegenwärtig weder durch den Zoll noch durch die DPAG durchgeführt. Auf Seiten der DPAG ist so lediglich ein „Herausfiltern" optisch auffälliger Pakete durch die Mitarbeiter möglich. Für weitergehende Untersuchungen fehlen das Prozedere und auch die dafür notwendigen Geräte.[414]

Im Rahmen der Gestellung werden Gestellungspflichtige Pakete gemäß §§ 4, 5 ZollVG dem Zollbeamten zur Prüfung vorgelegt, der eine „manuelle" Risikoanalyse durchführt. Das bedeutet, diese Risikoanalyse erfolgt ohne den Einsatz elektronischer Datenverarbeitung.

II. Zwischenergebnis

Der bisherige Sicherheitsstandard der postalischen Lieferkette wird nicht durch ein automatisiertes Risikomanagement gestützt, sondern durch die individuelle Bewertung eines Zollbeamten. Die Effektivität einer solchen Prüfung im Vergleich zu einem automatisierten Verfahren ist bisher nicht erforscht. Offensichtlich ist jedoch, dass das Verfahren inzwischen deutlich von dem Risikomanagement in anderen Transportzweigen abweicht. Ein Informationsaustausch zwischen den Zollbehörden und ein einheitlicher Standard innerhalb der Union sind so kaum zu gewährleisten.

414 InPoSec AP 2.4 – Deliverable, S. 13 f.

E. Ergebnis

Die hohen Stückzahlen an Postsendungen und die Besonderheiten des Universaldienstes an Preis, Qualität und Schnelligkeit führen zu Ausnahmen bei der Postverzollung und den dazu notwendigen Eingangsanmeldungen. Diese wiederum führen dazu, dass zu den betroffenen Sendungen wenig bis keine Daten vorliegen. Datenschutzrechtlich führt dies zu einem optimalen Zustand unter Gesichtspunkten der Datenvermeidung und Datensparsamkeit. Zollrechtlich werden die Möglichkeiten einer automatisierten Risikoanalyse, wie sie in anderen Wirtschaftzweigen üblich ist, nicht genutzt. Es findet so vielmehr eine manuelle Risikoanalyse durch einen Zollbeamten statt. Den Anforderungen an ein einheitliches Sicherheitsniveau an den Grenzen der Gemeinschaft wird man so kaum gerecht werden können.

4. Teil |
Möglichkeiten einer Risikoanalyse innerhalb der postalischen Lieferkette zwecks allgemeiner Gefahrenabwehr

Seitdem Masseninfrastruktur in den Anschlägen von London vom 07.07.2005 und Madrid vom 11.03.2004 in den Fokus des internationalen Terrorismus getreten ist, ist ihre Verwundbarkeit mehr als offensichtlich geworden. Hinzu treten auch Anschläge auf die postalische Lieferkette wie z. B. die Anthrax-Anschläge in den Vereinigten Staaten 2001.[415]

Ausgehend vom derzeitigen Status quo des Sicherheitsstands innerhalb der postalischen Lieferkette ist deswegen weiterhin der datenschutzrechtliche Rahmen für einen weitergehenden Schutz der postalischen Lieferkette zu untersuchen. Dafür sind weitergehende Sicherheitsmaßnahmen in den Blick zu nehmen und auf ihre Vereinbarkeit mit dem geltenden Recht hin zu untersuchen.

Erläutert werden sollen daher die Möglichkeiten der betroffenen Parteien Postdienstleister und Zollbehörden, die postalische Lieferkette mittels einer automatisierten Risikoanalyse zu schützen. Neben der Bestimmung möglicher Szenarien und deren Folgen für die Lieferkette gilt es vor allem, die Erlaubnistatbestände für die Verwendung von Daten zu diesem Zweck zu untersuchen. Weiterhin ist zu klären, welche Daten unter datenschutzrechtlichen Gesichtspunkten von welcher Stelle überhaupt verarbeitet werden können.

[415] Quelle: http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax.

A. Anforderungen an die Sicherheit postalischer Lieferketten

Aufgrund der Menge an Postsendungen ist die physische Untersuchung jeder einzelnen Sendung wirtschaftlich und logistisch unmöglich. Informationssysteme werden daher benötigt, um eine Vorabauswahl zu treffen, welche Sendungen risikoreich und daher zu untersuchen sind und bei welchen ein Risiko so gering ist, dass stichprobenartige Kontrollen ausreichen.[416]

So sind Risikomanagement- und Risikoanalyseverfahren dazu geeignet, die Sicherheit der postalischen Lieferkette durch Identifizierung und Wertung potenziell gefährdeter bzw. gefährlicher Sendungen zu verbessern.[417]

Die Risikoanalyse ermöglicht so eine Trennung der Sendungsströme entsprechend ihres Risikos. Risikoarme Sendungen können so schneller abgefertigt werden. Risikoreiche Sendungen können genauer untersucht werden.

Grundvoraussetzung dafür ist das Vorhandensein eines zu untersuchenden Datenkranzes (z. B. CN 23), der eine Risikoanalyse ermöglicht.

[416] InPoSec AP 7.1, S. 10 ff.

[417] InPoSec AP 7.1, S. 10 ff.

B. Verarbeitungsszenarien

Um die Möglichkeiten und Grenzen der Datenverwendung aus datenschutzrechtlicher Sicht aufzuzeigen und zu strukturieren, ist es sinnvoll, einzelne denkbare Szenarien aufzuzeigen und zu untersuchen und die einzelnen Verarbeitungsschritte entsprechend den Möglichkeiten der Risikoanalyse zu konkretisieren.

I. Grundlegende Verarbeitungsschritte

Zu untersuchen ist dabei die Möglichkeit, Daten zu erheben, zu verarbeiten und zu nutzen und festzulegen, ob und wie weit dies möglich sein kann.

Unter Erheben ist dabei im Sinne des § 3 Abs. 3 BDSG die Beschaffung von Daten zu verstehen.[418] Über die Abgabe einer Postsendung mit einer CN 23 Zollinhaltserklärung gelangen die darauf erfassten Informationen in den Herrschaftsbereich der DPAG, die diese Daten zu bestimmten Zwecken verarbeiten und nutzen kann. Aufgrund der weiten Definition des „Erhebens“ ist mit dieser Abgabe der Sendung von einer Erhebung auszugehen, da die Post die Möglichkeit hat, diese Informationen zur Kenntnis zu nehmen (beispielsweise durch das Ablesen der Daten durch einen Mitarbeiter oder durch Einspeisen der Informationen in ein Programm oder Informationssystem).

Nutzen ist gemäß § 3 Abs. 5 BDSG als Auffangtatbestand zu verstehen und meint alle Vorgänge, die nicht ein Erheben oder Verarbeiten sind. Bezogen auf die Risikoanalyse geht es konkret um ein Auswerten der Daten mittels EDV. Dabei werden die einzelnen Daten auf Grundlage vorheriger Wertungen mathematisch miteinander in Beziehung gesetzt, um bestimmte Risikoprofile zu erstellen. Hierbei ist von einer Nutzung der Daten auszugehen.

Verarbeiten im Sinne des § 3 Abs. 4 BDSG meint bezogen auf die Vorgänge einer Risikoanalyse vor allem das Speichern von Daten sowie ihre Weitergabe an

[418] Siehe 2. Teil A. IV. 3.) a).

Dritte.[419] Dies beinhaltet einen Informationsaustausch zwischen Postdienstleistern und Zollbehörden.

II. Datenverarbeitungsszenarien

Legt man zunächst als Parameter den Personenbezug von Daten sowie die möglichen verarbeitenden Stellen – Postdiensteanbieter und Zollbehörde – zugrunde, ergeben sich vier mögliche Szenarien, die zu untersuchen sind: Die Verwendung von Sachdaten durch Postdiensteanbieter sowie die Verwendung personenbezogener Daten durch Postdiensteanbieter, des Weiteren die Verwendung von Sachdaten durch Zollbehörden sowie die Verwendung personenbezogener Daten durch die Zollbehörden.

1. 1. Szenario: Verwendung von Sachdaten durch Postdiensteanbieter

Zunächst kommt die Verwendung von Sachdaten durch Postdiensteanbieter zwecks Risikoanalyse in Frage. Legt man den Datensatz der CN 23 Zollinhaltserklärung zu Grunde, so liegen isoliert betrachtet bereits mögliche zu verarbeitende Sachdaten vor. Betrachtet und verwendet man sie ohne Personenbezug, stehen das Land des Empfängers, eine detaillierte Beschreibung des Inhaltes, die Menge, die Nettogewichte und das Bruttogewicht (Paketgewicht), der Warenwert und die Währung, die Zolltarifnummern und der Ursprung der Waren, das deutsche Inlandsporto sowie die Art der Sendung und das Datum zur Verfügung.

[419] Siehe 2. Teil A. IV. 3.) b).

2. 2. Szenario: Verwendung personenbezogener Daten durch Postdiensteanbieter

Weiterhin ist die Verwendung personenbezogener Daten durch Postdiensteanbieter zu untersuchen. Legt man auch hier den Datensatz der Zollinhaltserklärung CN 23 zugrunde, liegen neben den Sachdaten als personenbezogene Daten die Absenderanschrift und die Anschrift des Endempfängers (diese enthalten Namen und Adressen) sowie die Unterschrift der Versenders vor.

3. 3. Szenario: Verwendung von Sachdaten durch Zollbehörden

Weiterhin kommt eine Datenverarbeitung durch die Zollbehörden in Betracht. Den Zollbehörden liegen durch die Zollinhaltserklärung CN 23 dieselben Sachdaten vor wie den Postdiensteanbietern.

4. 4. Szenario: Verwendung personenbezogener Daten durch Zollbehörden

Auch eine Verwendung personenbezogener Daten durch die Zollbehörden kommt in Betracht. Hier liegen den Zollbehörden ebenfalls die personenbezogenen Daten der Zollinhaltserklärung CN 23 vor.

C. Datenschutzrechtliche Anforderungen an eine Risikoanalyse innerhalb der postalischen Lieferkette

Die Analyse der datenschutzrechtlichen Anforderungen an die Risikoanalyse innerhalb der postalischen Lieferkette erfordert die Untersuchung möglicher Verbote und Beschränkungen, die sich im Datenschutz- wie auch im Post- und Zollrecht befinden können, sowie die Betrachtung möglicher Ermächtigungsgrundlagen in diesen Rechtsgebieten.

Die rechtlichen Möglichkeiten und Grenzen der Risikoanalyse innerhalb der postalischen Lieferkette sollen Anhand der vier formulierten Szenarien subsumiert und dargestellt werden.

I. Anforderungen an eine Ermächtigungsgrundlage

Eine Ermächtigungsgrundlage muss zunächst den allgemeinen Anforderungen an Bestimmtheit, Normenklarheit und Verhältnismäßigkeit genügen. Im Datenschutz bildet das Verbot der Verwendung von personenbezogenen Daten mit Erlaubnisvorbehalt in § 4 Abs. 1 BDSG den Ausgangspunkt der Betrachtung. Es bedarf daher eines Erlaubnistatbestandes, der die Verarbeitung unter Nennung der Datenart und des Zwecks für zulässig erklärt.[420] Fraglich ist, welchen „Präzisionsgrad" die Ermächtigung aufweisen muss. So wird gefordert, dass eine Ermächtigungsgrundlage die einzelnen Phasen konkret anspricht.[421] Es genügt demnach nicht, wenn die *„Verarbeitung bestimmter Informationen „stillschweigend" vorausgesetzt wird ".*[422]

---

[420] Gola/Schomerus in Gola/Schomerus, BDSG, § 4 BDSG, Rn. 8; Bergmann/Möhrle/Herb, Datenschutzrecht, § 4 Rn. 17.

[421] Gola/Schomerus in Gola/Schomerus, BDSG, § 4 BDSG, Rn. 7; Taeger in Taeger/Gabel, BDSG, § 4 BDSG, Rn. 24.

[422] Gola/Schomerus in Gola/Schomerus, BDSG, § 4 BDSG, Rn. 7; so auch Scholz/Sokol in Simitis, BDSG, § 4 BDSG, Rn. 15; Bergmann/Möhrle/Herb, Datenschutzrecht § 4 Rn. 17.

Weiterhin wird gefordert, dass die Ermächtigung eine Datenverarbeitung zwingend voraussetzen muss.[423] Enthält ein Erlaubnistatbestand keine klar genug formulierten Aussagen zur Datenverarbeitung, können die §§ 13–16 BDSG legitimierend herangezogen werden, wenn aus der Norm trotzdem hervorgeht, dass eine Abwägung zwischen den Interessen des Einzelnen und des Allgemeinwohls vorgenommen wurde.[424]

Andere lassen zumindest bei Eingriffen mit geringer Intensität, bei deren Aufgabenzuweisungsnorm zu deren Erfüllung die Verwendung von Daten erforderlich ist, als Erlaubnistatbestand zu.[425] Als noch ausreichende Ermächtigung wird § 38 JGG (i. V. m. § 13 BDSG) angesehen.[426] Daraus lässt sich schließen, dass es auf die exakte Formulierung, dass personenbezogene Daten erhoben, verarbeitet und genutzt werden dürfen, nicht ankommt. Wichtig ist jedoch, dass die Datenverarbeitung vorausgesetzt werden muss. Diese Auffassung wird auch durch das Unionsrecht untermauert, das zwischen den einzelnen Phasen (Erhebung, Verarbeitung, Nutzung) nicht unterscheidet.

---

423 Weichert in Däubler/Klebe/Wedde/Weichert, § 4 BDSG, Rn. 3.

424 Taeger in Taeger/Gabel, § 4 BDSG, Rn. 18.

425 Taeger in Taeger/Gabel, § 4 BDSG, Rn. 16; weiter gehen Bergmann/Möhrle/Herb, Datenschutzrecht, § 4 Rn. 17.

426 Taeger in Taeger/Gabel, § 4 BDSG, 2. Aufl. 2013 Rn. 27; § 38 JGG: „*(1) Die Jugendgerichtshilfe wird von den Jugendämtern im Zusammenwirken mit den Vereinigungen für Jugendhilfe ausgeübt.*
*(2) Die Vertreter der Jugendgerichtshilfe bringen die erzieherischen, sozialen und fürsorgerischen Gesichtspunkte im Verfahren vor den Jugendgerichten zur Geltung. Sie unterstützen zu diesem Zweck die beteiligten Behörden durch Erforschung der Persönlichkeit, der Entwicklung und der Umwelt des Beschuldigten und äußern sich zu den Maßnahmen, die zu ergreifen sind. In Haftsachen berichten sie beschleunigt über das Ergebnis ihrer Nachforschungen. In die Hauptverhandlung soll der Vertreter der Jugendgerichtshilfe entsandt werden, der die Nachforschungen angestellt hat. Soweit nicht ein Bewährungshelfer dazu berufen ist, wachen sie dar*über, daß der Jugendliche Weisungen und *Aufl. n nachkommt. Erhebliche Zuwiderhandlungen teilen sie dem Richter mit. Im Fall der Unterstellung nach § 10 Abs. 1 Satz 3 Nr. 5 üben sie die Betreuung und Aufsicht aus, wenn der Richter nicht eine andere Person damit betraut. Während der Bewährungszeit arbeiten sie eng mit dem Bewährungshelfer zusammen. Während des Vollzugs bleiben sie mit dem Jugendlichen in Verbindung und nehmen sich seiner Wiedereingliederung in die Gemeinschaft an.*
(3) Im gesamten Verfahren gegen einen Jugendlichen ist die Jugendgerichtshilfe heranzuziehen. Dies soll so früh wie möglich geschehen. Vor der Erteilung von Weisungen (§ 10) sind die Vertreter der Jugendgerichtshilfe stets zu hören; kommt eine Betreuungsweisung in Betracht, sollen sie sich auch dazu äußern, wer als Betreuungshelfer bestellt werden soll.“

Weiterhin müssen die Daten grundsätzlich beim Betroffenen direkt erhoben werden (§ 4 Abs. 2 S. 1 BDSG). Das bedeutet, dass der Betrofffene bei der Datenerhebung selbst und aktiv mitwirkt.[427] Da der Betroffene die Daten durch Beschriften einer Postsendung und durch Abgabe bei der Post selbst preisgibt und abgibt, ist der Grundsatz der Direkterhebung erfüllt.

II. Potenzielle Ermächtigungsgrundlagen

Potenzielle Ermächtigungsgrundlagen für eine Erhebung, Verarbeitung und Nutzung von Daten zwecks Risikoanalyse zur allgemeinen Gefahrenabwehr durch Postdiensteanbieter als auch die Zollbehörden werden nun untersucht.

1. Verwendung von Sachdaten

Zunächst soll die mögliche Verwendung von Sachdaten durch die Postdiensteanbieter und die Zollbehörde untersucht werden. Dabei sind mögliche Beschränkungen durch Datenschutz-, Post- und Zollrecht zu untersuchen.

a) Datenschutzrecht

Das Bundesdatenschutzgesetz regelt nur den Schutz personenbezogener Daten. Auch spezialgesetzlich findet hier kein Schutz von Sachdaten statt.[428] Ohne einen Personenbezug sind Sachdaten für das BDSG somit faktisch ohne Relevanz.[429]

Nach Datenschutzrecht ist damit eine Verwendung von Sachdaten sowohl durch Postdienstleister als auch Zollbehörden möglich.

---

427 Plath in Plath, BDSG, § 4 Rn. 7 f.

428 In etwa Harrings/Classen, EuZW 2008, S. 295, Europäische Informationsverwaltung durch behördliche Risikoanalyse Regelungs- und Rechtsschutzdefizite beim internationalen Informationsaustausch am Beispiel des zollrechtlichen AEO-Informationssystems zugleich Erwägungen zu einem unternehmensbezogenen Datenschutz, S. 298.

429 Roßnagel, Datenschutz in der künftigen Verkehrstelematik in NVZ 2006, S. 281 (282).

b) Postrecht

Weiterhin könnten im Postrecht Beschränkungen für die Verarbeitung von Sachdaten durch die Postdiensteanbieter vorliegen. § 42 PostG bezieht sich lediglich auf personenbezogene Daten und scheidet damit als Ermächtigungsgrundlage oder eventueller Ausschlussgrund aus. Die Datenverarbeitung von Zollbehörden wird im Postrecht nicht geregelt.

aa) § 39 PostG

Ein grundsätzliches Verbot für die Verwendung von Sachdachten durch Postdienstleister für eine Risikoanalyse könnte in § 39 PostG stehen.

(1) Anwendungsbereich des § 39 PostG

Zunächst müsste die Verarbeitung von Sachdaten durch Postdienstleister zwecks Risikoanalyse in den Anwendungsbereich des § 39 PostG fallen. Demnach unterliegen dem Postgeheimnis *„die näheren Umstände des Postverkehrs bestimmter natürlicher oder juristischer Personen sowie der Inhalt von Postsendungen“*. Zum Begriff des Inhalts von Postsendungen zählen auch Angaben zur Sendung. Darunter sind auch die Sachdaten der CN 23 Zollinhaltserklärung zu verstehen. Die detaillierte Beschreibung des Inhalts, die Menge, die Nettogewichte und das Bruttogewicht (Paketgewicht), der Warenwert, die Währung, die Zolltarifnummern und der Ursprung der Waren sowie die Art der Sendung beschreiben den Inhalt der Sendung. Das Land des Empfängers, das deutsche Inlandsporto und das Datum sind unter die näheren Umstände des Postverkehrs zu fassen.

Damit unterliegen alle Sachdaten § 39 Abs. 1 PostG.

Als Erbringerin geschäftsmäßiger Postdienste ist die DPAG auch Verpflichtete der Norm im Sinne des § 39 Abs. 2 PostG.

(2) Rechtsfolge des § 39 PostG

Weiterhin ist fraglich, welche Verpflichtung sich daraus für die Datenverwendung für eine Risikoanalyse durch Postdienstleister ergibt. Zunächst entsteht durch die Bindung ein generelles Kenntnisverschaffungsverbot, das die Kenntnisnahme an

ihre Erforderlichkeit für die Erbringung der Postdienstleistung koppelt.[430] Aus diesem Kenntnisverschaffungsverbot ergäbe sich in der Folge ein Verwertungsverbot von Daten zwecks Risikoanalyse. Daten, von denen man für diesen Zweck keine Kenntnis haben darf, dürfen auch nicht verwendet werden. Die Verwendung von Daten, deren Kenntnis man sich zu einem anderen Zweck verschaffen durfte, für die Risikoanalyse zu verwenden, widerspräche wiederum dem Zweckbindungsgrundsatz.

Folglich bedarf es als Voraussetzung für eine Risikoanalyse durch die Post einer „Kenntnisverschaffungserlaubnis". Diese könnte zunächst in der Formulierung des zum Erbringen der Postdienste erforderlichen Maßes in § 39 Abs. 3 PostG liegen. Dafür müsste die Verwendung der Sachdaten zwecks Risikoanalyse für den Postbetrieb notwendig sein.[431] Was unter dem erforderlichen Maß genau verstanden wird, wird im Gesetz nicht näher bestimmt. Auch in den Gesetzesvorlagen wird der Begriff nicht weiter präzisiert.[432]

Die „Vorgängerregelung" § 5 Abs. 2 PostG legte noch einen Erlaubnistatbestand bei Erforderlichkeit von Handlungen *„zur betriebsbedingten Abwicklung"* von Postdiensten fest.[433] Darunter wurden alle Maßnahmen verstanden, die zu einer ordnungsgemäßen Durchführung des Postbetriebes erforderlich waren.[434] Darunter verstand man insbesondere – parallel zum Erlaubnistatbestand von § 39 Abs. 4 Nr. 1–3 PostG – die Einsichtnahme zwecks Gebührenprüfung, die Zustellung an den Ersatzempfänger oder das Öffnen beschädigter Postsendungen.[435]

---

430 So auch Stern, § 39 Rn. 21.

431 Stern, § 39 Rn. 24.

432 Siehe dazu Abl. des Bundesministers für Post- u. Telekommunikation Nr. 87, 3.8.1989, (PostG § 5–12), sowie BR-Drs. 147/97 v. 14.03.1997 Gesetzentwurf der Bundesregierung; Entwurf eines Postgesetzes (PostG) + Anlagen (Beschlüsse).

433 Zitiert nach Ohnheiser, Postrecht § 5.

434 Ohnheiser, Postrecht, 4. Aufl., 1984, § 5 PostG Rn. 20.

435 Dazu genauer mit ausführlichem Zitierapparat Ohnheiser, Postrecht, 4. Aufl., 1984, § 5 PostG Rn. 20; sowie Altmannsperger, S. 34 f.

Zunächst könnte man anführen, dass es Postdienstleistern erlaubt sein muss, eine Risikoanalyse zwecks allgemeiner Gefahrenabwehr durchzuführen, um sich rechtstreu verhalten zu können. Ließe man diese nicht zu, beraubte man Postdienstleiter der Möglichkeit, Postsendungen herauszufiltern, die sie gesetzlich nicht befördern dürfen, weil diese einem Beförderungsverbot unterliegen. Eine solche Vereitelung rechtstreuen Verhaltens könne nicht von der Teleologie von § 39 PostG umfasst sein, deswegen gehöre die Anstrengung zu rechtstreuem Verhalten zum erforderlichen Maß des Betriebsablaufs.

Aufschluss darüber, was nicht unter dem Begriff zu subsumieren ist, kann die Systematik der Norm geben. § 39 Abs. 4 PostG regelt Erlaubnistatbestände, die über das erforderliche Maß in § 39 Abs. 3 PostG hinausgehen. Dazu gehören Vorgänge, die durchaus zum Betriebsablauf, jedoch nicht direkt zum „engen Übermittlungsvorgang" gehören (§ 39 Abs. 4 Nr. 1–3 PostG). Weiterhin wird in § 39 Abs. 4 Nr. 4 PostG ein Erlaubnistatbestand für die konkrete Gefahrenabwehr statuiert. Dieser Erlaubnistatbestand führt zum zwingenden Rückschluss, dass die konkrete Gefahrenabwehr nicht zu dem erforderlichen Maß des Postbetriebes zählt. Weiterhin kann durch einen „Erst-Recht-Schluss" die abstrakte oder allgemeine Gefahrenabwehr nicht zum erforderlichen Maß des Betriebsablaufs gezählt werden.

(3) Zwischenergebnis

Der Umfang des Begriffs des Postbetriebes und die dazugehörigen Maßnahmen sind nicht exakt festgelegt und der Begriff wird auch nicht einheitlich verwendet. Jedoch kann nicht davon ausgegangen werden, dass eine Risikoanalyse zur Gefahrenabwehr noch als erforderliches Maß zur Erbringung des Postdienstes angesehen wird. Der Begriff wurde in § 39 PostG vielmehr weiter verengt, sodass nur noch der tatsächliche Übermittlungsvorgang dazu gezählt werden kann, während selbst letztendlich für den Betriebsablauf und die Funktionsfähigkeit des Postdienstes notwendige Vorgänge explizit in § 39 Abs. 4 PostG geregelt wurden. Soweit Daten zur Gefahrenabwehr verwendet werden dürfen, werden diese Vorgänge im Gesetz auch durch spezielle Ermächtigungsgrundlagen explizit gedeckt. Eine Ermächtigung zur Gefahrenabwehr durch Generalklauseln ist hin-

gegen nicht der Fall und dürfte auch mit dem Bestimmtheitsgrundsatz schlecht vereinbar sein.

Damit ist die Risikoanalyse unter Verwendung von Sachdaten vom Postgeheimnis des § 39 PostG umfasst und ohne spezielle Ermächtigungsnorm nicht möglich. Eine solche Ermächtigungsnorm für die Post zur Verwendung von Sachdaten ist hingegen nicht ersichtlich.

bb) Zwischenergebnis

Nach Postrecht ist Postdienstleistern eine Risikoanalyse mit Sachdaten gemäß § 39 PostG untersagt.

c) Zollrecht

Das Zollrecht sieht grundsätzlich kein Verarbeitungsverbot für die Verwendung von Sachdaten im Zollbereich vor. Die Risikoanalyse richtet sich nach Art. 46 UZK. Die Bestimmungen richten sich dabei an die Zollbehörden und nicht an private Postdiensteanbieter. Restriktionen können sich jedoch aus dem Zollgeheimnis in Art. 12 UZK ergeben.

aa) Erhebung von Sachdaten durch die Zollbehörden

Zunächst verfügt der Zoll nicht über Sachdaten zu allen aus dem EU-Ausland verbrachten Postsendungen. Das Erheben der Daten erfolgt grundsätzlich durch die summarische Anmeldung. Insoweit verfügt der Zoll zunächst nur über Informationen, die über die CN 23 Zollinhaltserklärungen beigebracht werden. Zu allen anderen Paketen werden zunächst keine Sachdaten erhoben.

bb) Nutzung von Sachdaten durch die Zollbehörden

Bezüglich der Nutzung von Sachdaten durch die Zollbehörden bestehen zunächst keine generellen Restriktionen von Seiten des Post-, Datenschutz- oder Zollrechts. Die Risikoanalyse für den Zoll hat der Gesetzgeber in Art. 46 UZK geregelt, wonach sich folglich auch die Nutzung der Sachdaten richtet.

cc) Verarbeitung von Sachdaten durch Zollbehörden

Die Verarbeitung von Sachdaten durch Zollbehörden umfasst das Speichern und die Weitergabe der Daten. Bezüglich des Speicherns der Sachdaten bestehen keine Regelungen. Die Weitergabe von Sachdaten durch die Zollbehörden könnte durch Art. 12 UZK begrenzt werden.

(1) Art. 12 UZK

Art. 12 UZK soll die Personen, die am Zollverfahren teilnehmen, davor schützen, dass ihnen durch die notwendige Verwendung von Informationen innerhalb des Zollverfahrens kein Schaden, beispielsweise durch den Bruch des Berufs- oder Geschäftsgeheimnisses, entsteht.[436] Es ist lex specialis zum allgemeinen Amtsgeheimnis aus § 30 VwVfG.[437]

(a) Tatbestand

Gemäß Art. 12 S. 1 UZK fallen alle Angaben, *„die ihrer Natur nach vertraulich sind oder vertraulich mitgeteilt werden“*, unter die Geheimhaltungspflicht. *„Unter Angaben sind Informationen über Tatsachen, tatsächliche Umstände oder gegebene Verhältnisse zu verstehen“.*[438] Ihrer Natur nach vertraulich sind Informationen die geheim sind, d. h., wenn sie wenigen Personen bekannt sind und ein Geheimhaltungsinteresse besteht.[439] Demnach werden Angaben nicht geschützt, die offenkundig sind.[440] *„Offenkundig sind Sachverhalte, die allgemein bekannt sind.“*[441] Dies ist der Fall, wenn man sich diese Informationen aus zugänglichen Quellen verschaffen kann.[442] Art. 12 UZK dient dem Schutz von Individualinteressen.[443]

---

436 Wamers in Rüsken, Zollrecht, Art. 15 ZK Rn. 2 f.

437 Wohl Wamers in Rüsken, Zollrecht, Art. 15 ZK Rn. 25.

438 Schulmeister in Witte, ZK, Art. 15 Rn. 7.

439 Schulmeister in Witte, ZK, Art. 15 Rn. 8; Wamers in Rüsken, Zollrecht, Art. 15 ZK Rn. 42 f.

440 Wamers in Rüsken, Zollrecht, Art. 15 ZK Rn. 41.

441 Wamers in Rüsken, Zollrecht, Art. 15 ZK Rn. 41.

442 Wamers in Rüsken, Zollrecht, Art. 15 ZK Rn. 41.

443 Wamers in Rüsken, Zollrecht, Art. 15 ZK Rn. 4.

Er geht jedoch über den Schutz personenbezogener Daten hinaus und umfasst auch ggf. Sachdaten wie Geschäftsgeheimnisse, Know-how, Forschungsergebnisse etc.[444] Art. 12 UZK beinhaltet weiterhin den Schutz des Informanten.[445]

Laut Art. 12 Abs. 1 S. 2 UZK dürfen *„Außer im Falle von Art. 47 Abs. 2 diese Informationen von den zuständigen Behörden nicht ohne ausdrückliche Zustimmung der Person oder der Behörde, die sie übermittelt hat, weitergegeben werden"*. Verschwiegenheitsverpflichtete sind damit nicht nur Zollbehörden, sondern auch weitere Behörden, die im Rahmen von Zollkontrollen nach dem UZK tätig werden.[446] *„Unter Weitergabe ist jede Mitteilung an Dritte zu verstehen."*[447] Das Weitergabeverbot entfällt bei ausdrücklicher Zustimmung, wenn das Geheimhaltungsinteresse nicht mehr vorhanden ist oder die Angaben anonymisiert werden.[448]

Der Verweis auf Art. 47 Abs. 2 UZK bildet eine Ausnahmeregelung für die Risikoanalyse.

(b) Subsumtion

Fraglich erscheint, ob der Datenkranz der CN 23 Zollinhaltserklärung unter Art. 12 UZK zu fassen ist. Dafür müsste es sich dabei um vertrauliche Angaben handeln. Allgemein zugänglich und damit offenkundig sind das Land des Empfängers, eine detaillierte Beschreibung des Inhaltes, die Menge, die Nettogewichte und das Bruttogewicht (Paketgewicht), der Warenwert und die Währung, die Zolltarifnummern und der Ursprung der Waren, das deutsche Inlandsporto sowie die Art der Sendung und das Datum nicht. Ob ein Geheimhaltungsinteresse besteht, lässt sich allgemein nicht feststellen, sondern bedarf einer Einzelfallprüfung. Es kann sich im Einzelnen um Geschäfts- und Betriebsgeheimnisse handeln, die einen Rückschluss über Warenbewegungen und Geschäftsvorgänge zulassen.

---

444 Sowohl auch Wamers in Rüsken, Zollrecht, Art. 15 ZK Rn. 4.

445 Schulmeister in Witte, ZK, Art. 15 Rn. 11.

446 Schulmeister in Witte, ZK, Art. 15 Rn. 13; Wamers in Rüsken, Zollrecht, Art. 15 ZK Rn. 47 ff.

447 Schulmeister in Witte, ZK, Art. 15 Rn. 15.

448 Schulmeister in Witte, ZK, Art. 15 Rn. 15 ff.

Zum Zwecke der Risikoanalyse ist eine Weitergabe von Daten, falls notwendig, jedoch nach Art. 12 Abs. 1 S. 2 UZK gerechtfertigt.

(2) Zwischenergebnis

Eine Weitergabe von Sachdaten zum Zwecke der Risikoanalyse ist von der Durchbrechung des Zollgeheimnisses durch Art. 12 Abs. 1 S. 2 UZK iVm Art. 47 Abs. 2 UZK gedeckt.

d) Zwischenergebnis

Postdiensteanbietern ist es grundsätzlich untersagt, Sachdaten zu verarbeiten. Während das Datenschutzrecht und das Zollrecht hierzu keine Regelungen treffen, sind Sachdaten vom Schutz des Postgeheimnisses von § 39 PostG umfasst, das zu deren Verwendung zwecks Risikoanalyse zur Gefahrenabwehr keine Ermächtigungstatbestände vorsieht.

Zur Verwendung von Sachdaten durch Zollbehörden treffen das Datenschutzrecht wie auch das Postrecht keine Aussagen. Das Zollrecht hingegen regelt die Risikoanalyse durch Zollbehörden in Art. 47 UZK. Restriktionen bezüglich der Erhebung und Nutzung von Sachdaten werden nicht aufgestellt. Eine Weitergabe kann gegebenenfalls unter das Zollgeheimnis in Art. 12 UZK fallen wird jedoch von Art. 12 Abs. 1 S. 2 UZK i. V. m. Art. 47 UZK durchbrochen.

2. Verwendung personenbezogener Daten

Weiterhin soll die mögliche Verwendung personenbezogener Daten durch Postdiensteanbieter und Zollbehörden untersucht werden.

Datenschutzrechtlicher Ausgangspunkt ist der Grundsatz des Verbots, der Erhebung, Verarbeitung und Nutzung personenbezogener Daten mit Erlaubnisvorbehalt gemäß § 4 Abs. 1 BDSG. Damit ist für jeden Schritt in der Datenverarbeitung eine Einwilligung des Betroffenen oder ein Erlaubnistatbestand notwendig. Für Postdienstleister ist dieses Verbot darüber hinaus in § 39 PostG spezialgesetzlich verankert.

a) Ermächtigungsgrundlagen für eine Datenerhebung

Ermächtigungsgrundlagen für die Erhebung von Daten können sowohl im Postrecht als auch im Datenschutz und Zollrecht liegen. In Frage kommt zunächst § 41 Abs. 2 PostG. Des Weiteren sind die einzelnen Absätze der §§ 3 und 5 PDSV auf Ermächtigungen hin zu untersuchen. Schließlich kommen für Postdiensteanbieter die Tatbestandsvarianten des § 28 Abs. 1 BDSG, § 29 BDSG sowie § 30 BDSG in Frage.

Weiterhin kommt für die Risikoanalyse der Zollbehörden § 47 Abs. 2 UZK sowie § 13 BDSG in Betracht.

aa) § 41 Abs. 2 PostG

Zunächst könnte § 41 Abs. 2 PostG eine Ermächtigungsgrundlage für die Datenerhebung zwecks Risikoanalyse durch die Postdienstleister enthalten.

(1) Einleitung

§ 41 Abs. 2 PostG bildet die Grundlage für die Datenverarbeitung im Zusammenhang mit der betrieblichen Abwicklung von geschäftsmäßigen Postdiensten. Den Erlaubnistatbeständen geht die Überlegung voraus, dass es sich um Verarbeitungsgründe handelt, in die der Betroffene mit Inanspruchnahme der Postdienstleistung einwilligt.[449] Die Ermächtigung ist gemäß § 41 Abs. 2 S. 1 im Zusammenhang mit der PDSV zu lesen.

(2) Tatbestand

Berechtigt sind nach § 41 Abs. 2 S. 1 PostG Unternehmen und Personen, die geschäftsmäßig Postdienste erbringen oder an der Erbringung mitwirken.

Die Erhebung, Verarbeitung oder Nutzung der Daten muss für die betriebliche Abwicklung von geschäftsmäßigen Postdiensten erforderlich sein. Für welche Fälle der betrieblichen Abwicklung der Gesetzgeber eine Datenverarbeitung erlaubt, wird in § 41 Abs. 2 S. 1 Nr. 1–4 PostG deutlich. Die Formulierung „näm-

[449] Stern, Anh. § 41, § 5 PDSV Rn. 3.

lich für“ lässt auf eine abschließende Aufzählung schließen.[450] Dem Willen des Gesetzgebers nach sollen die Datenverwendungsmöglichkeiten auf die „näheren Umstände des Postverkehrs“ beschränkt bleiben.[451] § 41 Abs. 2 S. 1 Nr. 1 PostG erlaubt die Datenverarbeitung für *„das Begründen, inhaltliche Ausgestalten und Ändern eines Vertragsverhältnisses“*. § 41 Abs. 2 S. 1 Nr. 2 PostG erlaubt *„das Ermitteln von Verkehrsdaten für Vertragszwecke“*. § 41 Abs. 2 S. 1 Nr. 3 PostG stellt auf *„das ordnungsgemäße Ausliefern von Postsendungen“* ab. § 41 Abs. 2 S. 1 Nr. 4 PostG stellt *„das ordnungsgemäße Ermitteln, Abrechnen und Auswerten sowie den Nachweis der Richtigkeit der Entgelte für geschäftsmäßige Postdienste“* und damit die Wirtschaftlichkeit und die Finanzierung in den Mittelpunkt.

Ausdrücklich vom Tatbestand ausgenommen ist in § 41 Abs. 2 S. 2 PostG die Datenverarbeitung, die sich auf den Inhalt von Postsendungen bezieht.

(a) § 41 Abs. 2 Nr. 1 PostG

Für eine Zulässigkeit der Datenerhebung entsprechend der Tatbestandsavariante des § 41 Abs. 2 Nr. 1 PostG müsste diese für das Begründen, inhaltliche Ausgestalten oder Ändern eines Vertragsverhältnisses erforderlich sein. Die Vorschrift weist teilweise parallele Tatbestandsvoraussetzungen und eine sich überschneidenden Intention zu § 28 Abs. 1 Nr. 1 BDSG auf. Hierbei sei folglich auf die Ausführungen und die Subsumtion zu § 28 Abs. 1 Nr. 1 BDSG verwiesen, weswegen § 41 Abs. 2 Nr. 1 PostG als Ermächtigungsgrundlage für die Datenerhebung zwecks Risikoanalyse nicht in Betracht kommt.[452]

(b) § 41 Abs. 2 Nr. 2 PostG

Auch die Tatbestandsvariante des § 41 Abs. 2 Nr. 2 PostG ist als Ermächtigungsgrundlage für die Datenerhebung wecks Risikoanalyse auszuschließen.[453]

---

450 Stern, § 41 Rn. 29

451 BR-Drs. 147/97 v. 14.03.1997 Gesetzentwurf der Bundesregierung; Entwurf eines Postgesetzes (PostG), S. 48.

452 Bzgl. § 28 Abs. 1 Nr. 1 BDSG, siehe 4. Teil. C. II. 2.) a) ff) (4) (a).

453 Vgl. § 5 Abs. 2 PDSV, 4. Teil. C. II. 2.) a) ee).

(c) § 41 Abs. 2 Nr. 3 PostG

Einen möglichen Anknüpfungspunkt für eine postalische Risikoanalyse stellt § 41 Abs. 2 S. 1 Nr. 3 BDSG dar. So könnte vom ordnungsgemäßen Ausliefern auch die Risikoanalyse mitumfasst sein.

(aa) Tatbestandsvoraussetzungen

Vom Begriff des Auslieferns von Postsendungen umfasst wird grundsätzlich die betriebliche Abwicklung der Postdienstleistung.[454] Darunter muss der gesamte Vorgang der Lieferkette umfasst sein sowie alle Phasen, die eine Datenverwendung erfordern, um die Postsendung beim Empfänger zuzustellen.

Weiterhin wird Erforderlichkeit als Kriterium statuiert. Dafür wird man hier eine unmittelbare Verbindung zwischen der betrieblichen Abwicklung und der Datenverwendung verlangen müssen. Weiterhin wird mindestens ein „Angewiesensein" auf die Datenverwendung vorliegen müssen.[455]

(bb) Subsumtion

Zunächst handelt es sich bei Postdiensteanbietern (im speziellen der DPAG) unzweifelhaft um Unternehmen, die geschäftsmäßig Postdienste erbringen. Das Erheben von Daten natürlicher und juristischer Personen wird ausdrücklich vom Tatbestand gedeckt.

Fraglich erscheint, ob eine Risikoanalyse vom Tatbestand des ordnungsgemäßen Auslieferns von Postsendungen mitumfasst ist. Dafür müssten Fragen der Sicherheit der Lieferkette der betrieblichen Abwicklung des Postdienstes zuzuordnen sein.

Für die Auslegung kann historisch die Genese des Postgesetzes herangezogen werden. Der Gesetzentwurf der Bundesregierung für das PostG sah eine Ermächtigung zur Übermittlung von Daten an Behörden aus Sicherheitsgründen vor. § 41 Abs. 3 war wie folgt formuliert: *„Die in Abs. 2 genannten Unternehmen und*

---

454 Vgl. BR-Drs. 147/97 v. 14.03.1997 Gesetzentwurf der Bundesregierung; Entwurf eines Postgesetzes (PostG), S. 48.

455 Siehe Tatbestandsvoraussetzungen § 28 BDSG, 4. Teil. C. II. 2.) a) ff).

Personen haben personenbezogene Daten, die sie für das Begründen, inhaltliche Ausgestalten oder Ändern eines Vertragsverhältnisses erhoben haben, im Einzelfall auf Ersuchen an die zuständigen Stellen zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes sowie des Zollkriminalamtes erforderlich ist. Mitteilungen an den Betroffenen über Ersuchen und Übermittlungen personenbezogener Daten nach Satz 1 sind nur mit Zustimmung dieser Stellen zulässig. "[456] Diese Regelung sollte den Bedürfnissen der betreffenden Behörden im Rahmen ihrer Aufträge Rechnung tragen.[457] Der Vorschlag fand jedoch keinen Eingang in die gültige Fassung. Begründet wurde dieser Änderungsantrag neben einem mangelndem Sachzusammenhang mit dem Postrecht und einer mangelnden Begründung mit einer fehlenden Abstufung, die einer Unterscheidung zwischen Schwerkriminalität und Bagatellität Rechnung getragen hätte.[458] Systematisch lassen der Inhalt und die Formulierung des Gesetzentwurfs den Rückschluss zu, dass die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung grundsätzlich nicht vom Tatbestand des ordnungsgemäßen Auslieferns von Postsendungen umfasst ist, weil diese sonst keiner besonderen Regelung wie in Abs. 3 bedurft hätte. Weiterhin entsprach es nicht dem Willen des Gesetzgebers, diesen Tatbestand im Postgesetz zu regeln.

Ein Vergleich mit dem BDSG lässt denselben Schluss zu. Auch das BDSG normiert in § 28 Abs. 2 Tatbestände zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit oder zur Verfolgung von Straftaten gesondert.

Als Abwehr von Gefahren für die öffentliche Sicherheit oder zur Abwehr von Straftaten lässt sich die Risikoanalyse folglich nicht als Bestandteil des Betriebsablaufs werten.

---

[456] BR-Drs. 147/97 v. 14.03.1997 Gesetzentwurf der Bundesregierung; Entwurf eines Postgesetzes (PostG), S. 18 f.

[457] BR-Drs. 147/97 v. 14.03.1997 Gesetzentwurf der Bundesregierung; Entwurf eines Postgesetzes (PostG), S. 48.

[458] BR-Drs. 147/3/97 v. 14.05.1997 Antrag des Landes Schleswig-Holstein.

Jedoch könnte die Abwehr von Gefahren, der die postalische Lieferkette ausgesetzt ist, auch als eigenes, aus der gewerblichen Tätigkeit resultierendes Interesse bzw. Bedürfnis oder als daraus resultierende Notwendigkeit gewertet werden. Von der Sicherheit der Lieferkette hängt in letzter Konsequenz auch die Fähigkeit zur Leistungserbringung – dem Ausliefern der Postsendungen – im Allgemeinen ab. Angriffe auf die postalische Lieferkette können das Ausliefern von Postsendungen teilweise oder ganz verhindern und unterbinden.

Jedoch würde dies zu einer zu weiten Auslegung der Tatbestände führen. Im Sinne eines effektiven Datenschutzes und die Tatsache berücksichtigend, dass Tatbestände zur Gefahrenabwehr durch Datenverwendung grundsätzlich eine gesonderte Regelung erfahren, ist der Tatbestand hier restriktiv auszulegen und die Datenverwendung zwecks Risikoanalyse zu verneinen.

(cc) Zwischenergebnis

Die Tatbestandsvariante des § 41 Abs. 2 Nr. 3 PostG kommt damit als Ermächtigungsgrundlage für das Erheben personenbezogener Daten durch Postdienste für eine Risikoanalyse nicht in Betracht.

(d) § 41 Abs. 2 Nr. 4 PostG

§ 41 Abs. 2 Nr. 4 PostG ist als Ermächtigungsgrundlage für die Erhebung personenbezogener Daten zwecks Risikoanalyse fernliegend.

(3) Zwischenergebnis

Damit kommt § 41 Abs. 2 PostG als Ermächtigungsgrundlage für eine Erhebung von personenbezogenen Daten zwecks Risikoanalyse nicht in Frage.

bb) § 3 Abs. 1 PDSV

Weiterhin ist § 3 Abs. 1 PDSV auf seinen Ermächtigungsgehalt hin zu untersuchen.

Gemäß § 3 Abs. 1 S. 1 PDSV dürfen Dienstanbieter *„im Zusammenhang mit der Erbringung von Postdiensten personenbezogene Daten der am Postverkehr Beteiligten erheben, verarbeiten und nutzen, soweit diese Verordnung es erlaubt oder der*

Beteiligte eine Einwilligung erteilt hat, die den Vorschriften des Bundesdatenschutzgesetzes und dieser Verordnung entspricht". Mit der Formulierung, „soweit diese Verordnung es erlaubt" scheidet § 3 Abs. 1 S. 1 PDSV als eigene Anspruchsgrundlage aus, weil er eine weitere Norm mit einem konkreten Erlaubnistatbestand benötigt. Es handelt sich somit eher um eine Verweisung, die keinen wirklichen eigenen Regelungsgehalt aufweist. Die Grundentscheidung, unter welchen Umständen (Tatbeständen) Daten verwendet werden dürfen, ist in § 41 PostG festgelegt, dem die Verordnung folgt.[459]

cc) § 3 Abs. 3 PDSV

Ein weiterer Erlaubnistatbestand für die Datenerhebung zwecks Risikoanalyse durch Postdienstleister könnte in § 3 Abs. 3 PDSV liegen. Dieser erlaubt es Dienstanbietern, *„personenbezogene Daten der am Postverkehr Beteiligten zum Zwecke der ordnungsgemäßen Zustellung oder Rückführung einer Postsendung"* zu erheben, zu verarbeiten und zu nutzen*, „soweit die Daten aus aktuellen allgemein zugänglichen Quellen stammen"*.

Allgemein zugängliche Quelle sind solche, aus denen sich ein unbestimmter Personenkreis Informationen beschaffen kann.[460] Dazu zählen unter anderem Printmedien, Rundfunk- und Fernsehen sowie das Internet.[461]

Die in der postalischen Lieferkette gewonnenen Daten stammen nicht aus allgemeinzugänglichen Quellen, sondern werden in der Regel vom Versender den Postdienstleistern zur Verfügung gestellt. Damit scheidet § 3 Abs. 3 PDSV als Ermächtigungsgrundlage für eine Erhebung von Daten für die Risikoanalyse durch die Postdienstleister aus.

---

459 BR-Drs. 202/02 v. 11.03.2002 Verordnung der Bundesregierung, Verordnung über den Datenschutz bei der geschäftsmäßigen Erbringung von Postdiensten (Postdienste-Datenschutzverordnung – PDSV), S. 6.

460 Stern, Anh. § 41, § 3 PDSV Rn. 1.; BVerfGE 27, S. 71 (83); 33, 52 (65); Begr. der Bundesregierung zu § 3 Abs. 1, S. 3 PDSV.

461 Stern, Anh. § 41, § 3 PDSV Rn. 13.

dd) § 5 Abs. 1 PDSV

Weiterhin könnte § 5 Abs. 1 PDSV als Ermächtigungsgrundlage für eine Datenerhebung zwecks Risikoanalyse durch die Postdiensteanbieter in Frage kommen.

Gemäß § 5 Abs. 1 PDSV dürfen Dienstanbieter *„personenbezogene Daten ihrer Kunden erheben, verarbeiten und nutzen, soweit es für das Begründen, inhaltliche Ausgestalten oder Ändern eines Vertragsverhältnisses über Postdienste erforderlich ist (Bestandsdaten)“*.

Die Verarbeitungsgründe des § 5 PDSV knüpfen an den Erlaubnistatbestand des § 41 Abs. 2 PostG an.

Unter Bestandsdaten versteht § 5 Abs. 1 PDSV Informationen, die zur Identifikation des Kunden sowie des Leistungsumfangs gehören, *„insbesondere Name, Anschrift, Geburtsdatum und Art des in Anspruch genommenen Postdienstes“*.[462]

Fraglich erscheint, ob die Risikoanalyse zum Begründen oder Ausgestalten des Vertragsverhältnisses notwendig ist. Die Risikoanalyse dient der Bewertung des Gefährdungspotenzials einer Postsendung. Es ist davon auszugehen, dass ein Postdienstleister keine gefährlichen Güter ohne sein Wissen – wenn überhaupt – befördern möchte.

Jedoch findet die Risikoanalyse zeitlich nach Abschluss des Vertragsverhältnisses statt, sodass sie für das Begründen zumindest nicht als erforderlich angesehen werden kann.

Auch das inhaltliche Ausgestalten des Vertragsverhältnisses wird unabhängig von einer potenziellen Risikobewertung vorgenommen. So richten sich z. B. Leistungen und Entgelte auch nicht nach einer Risikobewertung. Folglich ist die Risikoanalyse auch nicht Bestandteil des inhaltlichen Ausgestaltens des Vertragsverhältnisses.

Als Anspruchsgrundlage für die Erhebung von Daten zwecks Risikoanalyse scheidet § 5 Abs. 1 PDSV damit aus, da die Risikoanalyse unabhängig vom Begründen oder Ausgestalten des Vertragsverhältnisses vorgenommen wird.

---

[462] Stern, Anh. § 41, § 5 PDSV Rn. 5.

ee) § 5 Abs. 2 PDSV

Des Weiteren könnte § 5 Abs. 2 PDSV als Ermächtigungsgrundlage für eine Datenerhebung zwecks Risikoanalyse durch Postdiensteanbieter in Frage kommen.

Laut § 5 Abs. 2 PDSV dürfen Dienstanbieter *„personenbezogene Daten ihrer Kunden erheben, verarbeiten und nutzen, soweit es für den Zweck des Vertragsverhältnisses erforderlich ist (Verkehrsdaten)“*. Der Begriff der Verkehrsdaten ist weiter zu verstehen als der der Bestandsdaten und umfasst neben den rechtlichen Rahmenbedingungen auch die tatsächlichen Rahmenbedingungen der erbrachten Postdienstleistung.[463] Davon umfasst werden Daten, *„die zur Begründung, Durchführung und Beendigung eines Vertragsverhältnisses über Postdienstleistungen bestimmt sind“*.[464] *„Dabei gehört zur Durchführung eines Vertragsverhältnisses über Postdienstleistungen auch seine inhaltliche Ausgestaltung“*, wobei hier eine deutliche Überschneidung des Tatbestandes zu § 5 Abs. 1 PDSV besteht.[465] Die Abs. 1–4 des § 5 PDSV sollen keine inhaltliche Veränderung gegenüber der Vorgängerregelung § 3 Postdienstunternehmen-Datenschutzverordnung bewirken.[466] Von dieser Regelung umfasst war die *„Möglichkeit, zu postdienstlichen Zwecken innerbetriebliche Kundenverzeichnisse mit wesentlichen Daten anzulegen“*.[467]

Die Regelung hebt hier die Häufigkeit und den Umfang des in Anspruch genommenen Postdienstes besonders hervor. Diese Aufzählung ist jedoch exemplarisch nicht abschließend.[468]

---

463 Stern, Anh. § 41, § 5 PDSV Rn. 6.

464 BR-Drs. 540/96 v. 12.07.1996 Verordnung der Bundesregierung, Verordnung über den Datenschutz für Unternehmen, die Postdienstleistungen erbringen (Postdienstunternehmen – Datenschutzverordnung – PDSV), S. 7.

465 BR-Drs. 540/96 v. 12.07.1996 Verordnung der Bundesregierung, Verordnung über den Datenschutz für Unternehmen, die Postdienstleistungen erbringen (Postdienstunternehmen – Datenschutzverordnung – PDSV), S. 7.

466 BR-Drs. 202/02 v. 11.03.2002 Verordnung der Bundesregierung, Verordnung über den Datenschutz bei der geschäftsmäßigen Erbringung von Postdiensten (Postdienste-Datenschutzverordnung – PDSV), S. 7.

467 BR-Drs. 202/02 v. 11.03.2002 Verordnung der Bundesregierung, Verordnung über den Datenschutz bei der geschäftsmäßigen Erbringung von Postdiensten (Postdienste-Datenschutzverordnung – PDSV), S. 7.

468 Stern, Anh. § 41, § 5 PDSV Rn. 6.

Mit der Formulierung „soweit“ wird deutlich, dass die Datenerhebung erforderlich sein muss.[469] Daraus wird eine restriktive Handhabung der Norm abgeleitet.[470] Zulässig ist die Datenverwendung demnach nur dann, wenn das gleiche Ziel mit milderen Mitteln nicht zu erreichen ist und die Datenverwendung im Einzelfall aus ex-ante-Sicht unerlässlich ist.[471]

Zunächst müsste die Datenerhebung zwecks Risikoanalyse unter den Zweck des Vertragsverhältnisses fallen. Als erforderlicher Bestandteil zur Begründung oder Ausgestaltung eines Vertragsverhältnisses kann die Risikoanalyse nicht angesehen werden.[472]

Fraglich erscheint, ob eine Parallele zum Anlegen von innerbetrieblichen Kundenverzeichnissen mit wesentlichen Daten zu postdienstlichen Zwecken gezogen werden kann.

Bereits in der Gesetzesbegründung zum ersten PostG wurde deutlich, dass zwischen dem eigentlichen Betriebsablauf und der Verfolgung von Straftaten tatbestandlich zu trennen ist.[473] So ist auch hier davon auszugehen, dass Sicherheitsbelange einer gesonderten tatbestandlichen Regelung bedürfen und nicht von innerbetrieblichen Vorgängen umfasst werden.

Zuletzt könnte die Risikoanalyse dem Vertragszweck zuzuordnen sein, wenn sie unter den Vertragspartnern als vereinbart angesehen werden kann.

Es ist jedoch kaum davon auszugehen, dass der Vertragszweck für beide Vertragspartner ersichtlich die Risikoanalyse mitumfasst. Es sind ähnliche Wertungen zu ziehen wie bei den Tatbeständen der §§ 28 Abs. 1 BDSG und 41 Abs. 2 PostG.[474]

---

469 So auch Stern, Anh. § 41, § 5 PDSV Rn. 6.

470 Stern, Anh. § 41, § 5 PDSV Rn. 6.

471 Stern, Anh. § 41, § 5 PDSV Rn. 6; vgl. Stober/Moelle/Müller-Dehn, in Stern, Postrecht, Teil I § 10 PTReG Rn. 16.

472 Siehe § 5 Abs. 1 PDSV 4. Teil. C. II. 2.) a) dd).

473 BT-Drs. V/3295 v. 26.09.1986 Entwurf eines Gesetzes über das Postwesen, S. 14.

474 Vgl. § 28 Abs. 1 BDSG 4. Teil. C. II. 2.) a) ff) sowie 4. Teil. C. II. 2.) a) aa).

Folglich ist davon auszugehen, dass die Risikoanalyse dem Vertragszweck nicht zugeordnet werden kann.

Damit stellt § 5 Abs. 2 PDSV keine Ermächtigungsgrundlage für eine Erhebung personenbezogener Daten zwecks Risikoanalyse durch die Postdiensteanbieter dar.

ff) § 28 Abs. 1 BDSG

Eine Ermächtigung zur Erhebung personenbezogener Daten zwecks Risikoanalyse zur allgemeinen Gefahrenabwehr durch Postdiensteanbieter könnte § 28 Abs. 1 BDSG enthalten.

§ 28 Abs. 1 BDSG erklärt *„das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke“* für zulässig unter drei alternativen Voraussetzungen: *„wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist“, „soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt“, oder „wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt“.*

(1) Einleitung

§ 28 BDSG ist die Schlüsselnorm für die Datenverarbeitung im nicht-öffentlichen Bereich.[475] Aufgrund ihres Umfanges und unübersichtlicher sich widersprechender Formulierungen ist § 28 BDSG in der Literatur jedoch auch umfangreicher Kritik ausgesetzt.[476]

---

475 Simitis in Simitis, BDSG, § 28 Rn.1.

476 So im Detail Simitis in Simitis, BDSG, § 28 Rn. 2 ff. ebenso Taeger in Taeger/Gabel, BDSG, § 28 Rn. 4; Bergmann/Möhrle/Herb, Datenschutzrecht, § 28 Rn. 1.

Der Wortlaut der Überschrift spricht nur von der Datenerhebung und der Datenspeicherung, trotzdem ist mit dem Wortlaut von § 28 Abs. 1 BDSG davon auszugehen, dass das Erheben, das Speichern, das Verändern, das Übermitteln und das Nutzen mit umfasst sind.[477]

(2) Anwendungsbereich, § 27 BDSG

Zunächst muss der Anwendungsbereich des § 27 BDSG eröffnet sein. Dieser konkretisiert den in § 1 Abs. 2 Nr. 3 BDSG festgelegten Anwendungsbereich des BDSG.[478] Im Vergleich zu diesem, liegt der speziellere Reglungsbereich in der Unterscheidung zwischen den öffentlichen und den nicht-öffentlichen Stellen.

Demnach finden die Vorschriften des Abschnitts (3) Anwendung auf personenbezogene Daten, die *„unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden durch 1. nicht-öffentliche Stellen, 2. a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist“*. Ein Ausschluss von der Anwendung gilt, *„wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.“*

Eine nicht-öffentliche Stelle liegt gemäß § 2 Abs. 4 BDSG bei natürlichen Personen, juristischen Personen, Gesellschaften sowie Personenvereinigungen des

---

477 Taeger in Taeger/Gabel, BDSG, § 28 Rn. 27; Gola/Schomerus in Gola/Schomerus, BDSG, § 28 BDSG, 11. Aufl. 2012 Rn. 2.

478 Gola/Schomerus in Gola/Schomerus, BDSG, § 27 BDSG, 11. Aufl. 2012 Rn. 1.

privaten Rechts vor, soweit diese nicht unter § 2 Abs. 1–3 BDSG fallen.[479] *„Nimmt eine nicht-öffentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung war, ist sie insoweit öffentliche Stelle im Sinne*“ des Gesetzes.[480] Ein „Konzernprivileg“ ist im BDSG nicht verankert, demzufolge ist eine juristische – nicht wirtschaftliche – Perspektive relevant.[481] Weitere Normadressaten sind öffentlich-rechtliche Wettbewerbsunternehmen des Bundes und der Länder.[482]

Weiterhin muss es sich um eine automatisierte oder dateiengebundene Verwendung handeln.[483] Diese Voraussetzung ist eine Dopplung zu § 1 Abs. 2 Nr. 3.[484] Erweitert wird die Maßgabe in § 27 Abs. 2 BDSG für Daten, die offensichtlich einer automatisierten Datenverarbeitung entstammen.[485] Eine automatisierte Verarbeitung bedarf gemäß § 3 Abs. 2 BDSG des Einsatzes von Datenverarbeitungsanlagen. Dem Wortlaut von § 27 Abs. 1 BDSG nach müssen die

---

479 § 2 BDSG: (1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.
(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.
(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn 1. sie über den Bereich eines Landes hinaus tätig werden oder 2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht. Andernfalls gelten sie als öffentliche Stellen der Länder.

480 § 2 Abs. 2 S. 2 BDSG; Zu dieser Problematik ausführlich Schaffland/Wiltfang, BDSG, § 27 Rn. 10 ff.

481 So auch Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 27 Rn. 7; dazu ausführlich Schaffland/Wiltfang, BDSG, § 27 Rn. 24 ff.

482 Buchner in Taeger/Gabel, BDSG, § 27 Rn. 8 ff.; ausführlicher Simitis in Simitis, BDSG, § 27 Rn. 6ff.

483 Simitis in Simitis, BDSG, § 27 Rn. 24 f.; Plath in Plath, BDSG, § 27 Rn. 3.

484 Plath in Plath, BDSG, § 27 Rn. 4.

485 Dazu ausführlicher Schaffland/Wiltfang, BDSG, § 27 Rn. 5–8; Simitis in Simitis, BDSG, § 27 Rn. 27 ff.

Verarbeitung und die Nutzung automatisiert, die Erhebung hingegen kann manuell – wenn auch zum Zwecke der automatisierten Verwendung – erfolgen.[486]

(3) Verhältnis der Tatbestandsvarianten zueinander

Fraglich erscheint das Verhältnis der Tatbestandsvarianten des § 28 Abs. 1 BDSG zueinander. Unbestritten ist die Fokussierung auf die erste Tatbestandsvariante. Bei einer Verwendung von Daten für ein Schuldverhältnis wird hauptsächlich § 28 Abs. 1 S. 1 Nr. 1 BDSG zur Anwendung kommen, sodass die Varianten 2 und 3 grundsätzlich als Auffangklauseln von Nr. 1 dienen.[487]

Es stellt sich zunächst die Frage, ob und eventuell wie weit die Tatbestandsvarianten kumulativ angewendet werden können oder ob sie einander ausschließen.

Die weitestgehende Forderung geht von einer Sperrung von § 28 Abs. 1 S. 1 Nr. 2 und 3 BDSG allein schon bei Vorliegen eines Schuldverhältnisses aus.[488] Im Sinne eines effektiven Datenschutzes könnte man die Tatbestände durchaus restriktiv auslegen.[489] Eine Sperrung der Tatbestandsvarianten Nr. 2 und Nr. 3 bei Vorliegen eines Schuldverhältnisses lässt sich jedoch weder dem Wortlaut noch der Systematik der Norm entnehmen.[490] Der Wortlaut der Norm legt nicht einmal eine Priorisierung fest, geschweige denn eine Sperrung. Die Berufung auf berechtigte Interessen würde durch Sperrung bei Vorliegen eines Schuldverhältnisses faktisch unmöglich gemacht und damit auch der Erlaubnistatbestand von § 28 Abs. 1 Nr. 2 BDSG weitestgehend vereitelt. Es ist folglich davon auszugehen, dass man die Erlaubnistatbestände des § 28 Abs. 1 S. 1 Nr. 2 und 3 BDSG auch bei Vorliegen eines Schuldverhältnisses anwenden darf.[491]

---

486 Plath in Plath, BDSG, § 27 Rn. 7.

487 Sogar weitergehend Plath in Plath, BDSG, § 28; Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 14; wohl anders Simitis, § 28 Rn. 52 ff.

488 Wohl Simitis in Simitis, BDSG, § 28 Rn. 54 ff.

489 Taeger in Taeger/Gabel, BDSG, § 28 BDSG, Rn. 54.

490 Wohl anders Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 14.

491 So auch Taeger in Taeger/Gabel, BDSG, § 28 Rn. 107.

Des Weiteren ist damit das Verhältnis der Tatbestandsvarianten zueinander bei Vorliegen eines Schuldverhältnisses zu klären.

Eine Ansicht geht davon aus, dass es der verarbeitenden Stelle nicht freigestellt ist, beliebig zwischen den Tatbestandvarianten auszuwählen noch sie kumulativ anzuwenden, und dass sie folglich nebeneinander stehen.[492] Doch auch dies ist dem Wortlaut der Norm nicht zu entnehmen. Zunächst stehen die Tatbestandsvarianten diesem nach wertungsfrei nebeneinander. Richtig dürfte sein, auf die Schutz- und Vertraulichkeitspflichten innerhalb des Schuldverhältnisses abzustellen.[493] Eine Datenverwendung zur Begründung, Durchführung oder Beendigung eines Schuldverhältnisses, die nach § 28 Abs. 1 S. 1 Nr. 1 BDSG nicht zulässig ist, wird schwer durch die anderen Tatbestandsvarianten zu begründen sein und dürfte diesen vorgehen bzw. diese hier verdrängen. Werden vertragliche Schutzpflichten nicht verletzt, ist jedoch in engen Grenzen auch eine Anwendung der anderen Tatbestandsvarianten denkbar.[494] So ist eine Konstellation vorstellbar, bei der eine Verwendung von Daten für ein Schuldverhältnis erforderlich ist und parallel die gleiche Verwendung auch aus einem berechtigten Interesse der verarbeitenden Stelle erwächst. So sind durchaus Konstellationen denkbar, in denen die Tatbestandsvarianten kumulativ angewendet werden können.[495]

(4) Tatbestandsvoraussetzungen

Der Begriff des eigenen Geschäftszwecks deckt sich inhaltlich mit dem „inhaltlichen Zweck" des § 28 BDSG alter Fassung.[496] Das Gesetz bietet für die Auslegung keine Anhaltspunkte, sodass auf den Einzelfall abgestellt werden muss.[497] Der Be-

---

492 Simitis in Simitis, BDSG, § 28 Rn. 52 ff.

493 Bergmann/Möhrle/Herb, Datenschutzrecht, § 28 Rn. 217; Gola/Schomerus in Gola/Schomerus, BDSG, § 28 Rn. 9.

494 Wohl Bergmann/Möhrle/Herb, Datenschutzrecht, § 28 Rn.217; Gola/Schomerus in Gola/Schomerus, BDSG, § 28 Rn. 9.

495 Im Ergebnis auch Taeger in Taeger/Gabel, BDSG, § 28 Rn. 107.

496 Plath in Plath, BDSG, § 28 BDSG, Rn. 12; Taeger in Taeger/Gabel, BDSG, § 28 Rn. 30.

497 Plath in Plath, BDSG, § 28 BDSG, Rn. 13; Ambs in Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 28 BDSG, Rn. 4.

griff ist weit gefasst und es ist durchaus in der Verantwortung der verarbeitenden Stelle, den Verwendungszweck und einen Rahmen für die Datenverarbeitung zu setzen.[498] Die Formulierung verdeutlicht den „akzessorischen Charakter" der Datenverarbeitung, die als Hilfsmittel die Erfüllung des Vertragszieles unterstützen soll.[499] Sie ist „Mittel zum Zweck" „zur Erreichung eines dahinterstehenden Geschäftszwecks".[500] Eine Verwendung für anderweitige Ziele, wie die Nutzung von Auskunftsdateien, bleibt davon ausgeschlossen.[501] In Abgrenzung zu § 29 BDSG handelt es sich um ein Hilfsmittel, wenn die Verwendung kein Selbstzweck ist und damit kein eigener Geschäftszweck verfolgt wird.[502] Unschädlich ist, wenn neben den nach § 28 BDSG verfolgten Zweck noch andere Intentionen treten, sofern sich diese miteinander vereinbaren lassen und nicht einander zuwiderlaufen.[503] Für § 28 BDSG alter Fassung hieß es in der Begründung des Regierungsentwurfs: *„Maßgebend für die Zugehörigkeit zum Anwendungsbereich des 3. Abschnitts ist der Zweck der Datenverarbeitung. Die Vorschriften dieses Abschnittes gelten in allen denjenigen Fällen, in denen die Datenverarbeitung nicht als Selbstzweck ausgeübt wird – solche Fälle werden im 4. Abschnitt geregelt –, sondern als Hilfsmittel zur Optimierung der Erfüllung der Geschäftszwecke oder Ziele des Anwenders, die nicht in der Speicherung oder Weitergabe oder sonstigen Verarbeitung von personenbezogenen Daten bestehen."*[504]

Fraglich ist, wie man mit Datenverarbeitung zu eigenen als auch fremdem Zwecken umgeht. Neben § 28 BDSG könnten die §§ 29 ff. BDSG treten. Eine parallele Einschlägigkeit mehrerer Normen ist denkbar.[505] Eine Ansicht möchte

498 Simitis in Simitis, BDSG, § 28 BDSG, Rn. 23.

499 Simitis in Simitis, BDSG, § 28 BDSG, Rn. 22.

500 Gola/Schomerus in Gola/Schomerus, BDSG, § 28 BDSG, 11. Aufl. 2012 Rn. 4.

501 Simitis in Simitis, BDSG, § 28 BDSG, Rn. 22.

502 Schaffland/Wiltfang, BDSG, § 28 Rn. 3 ff.

503 Ambs in Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 28 BDSG, Rn. 4.

504 BT-Drucksache 7/1027 vom 21.9.1973, S. 27.

505 Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 12.

für jeden Vorgang den Zweck einzeln bestimmen, eine andere Ansicht stellt auf den Schwerpunkt der Datenverarbeitung im Allgemeinen ab.[506]

Für die erste Ansicht spricht, dass sich im BDSG die Ermächtigungsgrundlagen nach der bestimmten Anwendung richten und man sich demzufolge auch danach bei der Bestimmung der Ermächtigungsgrundlagen richten muss, um dem Willen des Gesetzgebers und den Anforderungen des Gesetzes gerecht zu werden.[507]

Für die zweite Ansicht, dass der Datenschutz auch in der Praxis handhabbar sein muss. Eine zu große Zersplitterung, führt zu einer Überregulierung und ist bei komplexen Datenverarbeitungsvorgängen kaum noch darstellbar.

Kollidieren während eines Vorgangs mehrere Intentionen, so wird auf den Schwerpunkt in diesem Bearbeitungsvorgang abzustellen sein. Dies darf freilich nicht zu einer generellen Anwendung einer Rechtsnorm – hier § 28 BDSG – für die gesamte Datenverarbeitung führen. Für die jeweiligen Verarbeitungsschritte wird der Schwerpunkt der Intention und damit die Ermächtigungsnorm einzeln zu bestimmen sein.

Eindeutig in den Ermächtigungsbereich einbezogen ist das Erheben personenbezogener Daten. Gemäß § 28 Abs. 1 S. 2 BDSG muss dafür der konkrete Zweck der Verwendung bereits festgelegt sein. Damit wird gleichzeitig der Rahmen für die Datenverarbeitung gesetzt.[508] Dieser gilt „dauerhaft“ für die erhobenen Daten. Zwecks einer besseren Nachvollziehbarkeit und Transparenz sollte dieser klar definiert und festgelegt sein.[509]

---

506 Für die erstgenannte Ansicht siehe Simitis in Simitis, BDSG, § 28 Rn. 24 ff., für die zweite Auffassung Plath in Plath, BDSG, § 28 BDSG, Rn. 14; zustimmend wohl Wedde in Däubler/Klebe/Wedde/Weichert, § 28 BDSG, Rn. 12.

507 Simitis in Simitis, BDSG, § 28 Rn. 26

508 Simitis in Simitis, BDSG, § 28 Rn. 38; Bergmann/Möhrle/Herb, Datenschutzrecht, § 28 Rn. 260 anders Taeger in Gabel/Taeger, § 28 BDSG, Rn.109.

509 Simitis in Simitis, BDSG, § 28 Rn. 42 ff.

(a) § 28 Abs. 1 Nr. 1 BDSG

Für § 28 Abs. 1 Nr. 1 BDSG muss zunächst ein rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis vorliegen. Sind die Beteiligten über mehrere Schuldverhältnisse miteinander verbunden, ist die Datenverarbeitung dieser Schuldverhältnisse grundsätzlich getrennt zu betrachten.[510] Weiterhin muss die Datenverarbeitung für die Begründung, Durchführung oder Beendigung des Schuldverhältnisses mit dem Betroffenen erforderlich sein. Es muss somit einen unmittelbaren Konnex zwischen dem Zweck des Schuldverhältnisses und der Verwendung der Daten geben.[511] Bei der Feststellung des Vertragszweckes ist maßgeblich, was beide Seiten vereinbart haben.[512] Die Norm geht von dem Leitbild aus, dass beide Seiten ein Interesse an der Vertragserfüllung haben und das damit auch zumindest ein Mindestmaß an Datenverarbeitung in beiderseitigem Interesse liegt.[513]

So geht man bei Kredit- wie auch bei Versicherungsverträgen davon aus, dass zur Zweckbestimmung dieser Verträge gehört, auch Auskünfte über Bonität und Kreditwürdigkeit einzuholen.[514]

Die Datenerhebung muss weiterhin objektiv erforderlich sein. Als Maßstab dient dabei die konkrete Zweckbestimmung des Schuldverhältnisses. Die Verwendung der Daten zur Erfüllung des Vertragszweckes und inwieweit sie dafür benötigt werden, kann Hinweise für ihre Erforderlichkeit geben. Eine absolute Notwendigkeit der Datenerhebung muss hingegen nicht gegeben sein, Gesichtspunkte der Effizienz und Wirtschaftlichkeit sind mit abzuwägen.[515] Auf der anderen Seite wird eine reine „Förderlichkeit“ in der Regel nicht ausreichen.[516] Nicht

---

510 Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 19.

511 Simitis in Simitis, BDSG, § 28 Rn. 57.

512 Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 16.

513 Taeger in Taeger/Gabel, § 28 Rn. 48

514 Schaffland/Wiltfang, BDSG, § 28 Rn. 62 ff.

515 Im Ergebnis auch Plath in Plath, BDSG, § 28 BDSG, Rn. 24ff; wohl anders Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 15, sowie Schaffland/Wiltfang, BDSG, § 28 Rn. 18, 86.

516 Im Ergebnis auch Plath in Plath, BDSG, § 28 BDSG, Rn. 20.

erforderlich ist die Verwendung personenbezogener Daten, wenn die Ziele auch ohne sie erreicht werden können.[517] Es ist letztendlich auf ein „Angewiesensein" auf die Datenverarbeitung abzustellen.[518]

Die Bestimmung der konkreten Daten lässt sich nicht generalisieren oder für bestimmte Vertragsarten typisieren, sondern es ist immer die konkrete Verwendungssituation maßgeblich.[519] Dennoch werden in der Regel zumindest die Daten der beteiligten Personen, ggf. des Vertragsgegenstandes zu erfassen sein.

In der Regel geht man bei Schuldverhältnissen von der Erforderlichkeit der Verwendung sog. „Basisdaten" (Name, Anschrift etc.) aus.[520]

Eine Abwägung mit den Interessen des Betroffenen, wie in § 28 Abs. 1 Nr. 2 und 3 BDSG gefordert, ist hier nicht notwendig.[521]

(b) § 28 Abs. 1 Nr. 2 BDSG

Gemäß § 28 Abs. 1 Nr. 2 BDSG müssen berechtigte Interessen zur Tatbestandserfüllung gewahrt bleiben. Das Vorliegen berechtigter Interessen ist BDSG-spezifisch, unabhängig von deren Definition in anderen Gesetzestexten, zu bestimmen.[522] Eine nähere Eingrenzung nimmt der Gesetzestext nicht vor. Es kann sich neben wirtschaftlichen und rechtlichen auch um ideelle Interessen handeln, es müssen jedoch eigene Belange der verarbeitenden Stelle sein.[523] Grundsätzlich kommt damit jedes von der Rechtsordnung gebilligtes Interesse in Frage.[524] Es ist jedoch möglich, dass es im eigenen Interesse ist und zum Aufgabenkreis der

---

517 Hoeren in Roßnagel, Datenschutzrecht, S. 608; Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 48; Taeger in Taeger/Gabel, BDSG, § 28 Rn. 49 ff.

518 Gola/Schomerus in Gola/Schomerus, BDSG, § 28 BDSG, 11. Aufl. 2012 Rn. 15.

519 Im Ergebnis auch Simitis in Simitis, BDSG, § 28 BDSG, Rn. 60.

520 Plath in Plath, BDSG, § 28 BDSG, Rn. 30; Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 18.

521 Taeger in Taeger/Gabel, BDSG, § 28 Rn. 47.

522 Simitis in Simitis, BDSG, § 28 BDSG, Rn. 103 f.

523 Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. § 28 Rn. 48; ähnlich Simitis in Simitis, BDSG, § 28 BDSG, Rn. 104.

524 Schaffland/Wiltfang, BDSG, § 28 Rn. 85.

verarbeitenden Stelle gehört, auch die Interessen Dritter wahrzunehmen.[525] Die Vorbeugung oder Absicherung typischer Geschäftsrisiken kann ebenfalls in den Bereich der berechtigten Interessen fallen.[526] Insbesondere können Aktivitäten, die den Betriebsablauf betreffen, die Kosten verringern oder das Ausfallrisiko minimieren, dazu gezählt werden.[527] In diese Aufzählung gehören auch Sicherheitsaspekte. Ohne die bestimmte Verwendung entstünde der verarbeitenden Stelle ein nicht zumutbarer Nachteil.

Des Weiteren ist eine Interessenabwägung zwischen den berechtigten Interessen der verarbeitenden Stelle und dem schutzwürdigen Interesse des Betroffenen an einem Ausschluss der Verarbeitung – das nicht überwiegen darf – vorzunehmen. Der BGH führt dazu aus: *„Der wertausfüllende Begriff der „schutzwürdigen" Belange verlangt eine Abwägung des Persönlichkeitsrechts des Betroffenen und des Stellenwerts, den die Offenlegung und Verwendung der Daten für ihn hat, gegen die Interessen der speichernden Stelle und der Dritten, für deren Zweck die Speicherung erfolgt. Dabei sind Art, Inhalt und Aussagekraft der beanstandenden Daten an den Angaben und Zwecken zu messen, denen ihre Speicherung dient. Nur wenn diese am Verhältnismäßigkeitsgrundsatz ausgerichtete Abwägung, die die speichernde Stelle vorzunehmen hat, keinen Grund zur Annahme bietet, dass die Speicherung der in Frage stehenden Daten zu dem damit verfolgten Zweck schutzwürdige Belange des Betroffenen beeinträchtigt, ist die Speicherung zulässig."*[528]

Die amtliche Begründung zum BDSG versteht unter schutzwürdigem Interesse den Bereich, *„der in der einschlägigen Literatur und Rechtsprechung mit den Begriffen Privatsphäre, Persönlichkeitsrecht und dgl. versehen wird".*[529]

Der Begriff der schutzwürdigen Interessen wird im Gesetz zunächst nicht näher bestimmt. Damit muss sich die Abwägung an der spezifischen Verarbeitungssituation orientieren und anhand dessen die konkreten Konsequenzen aus der

525 So auch Simitis in Simitis, BDSG, § 28 Rn. 106.

526 Simitis in Simitis, BDSG, § 28 Rn. 116 f.

527 Schaffland/Wiltfang, BDSG, § 28 Rn. 85.

528 BGH Urt. v. 17.12.1985 = NJW 1986, S. 2505 (2506).

529 BT-Drucksache 7/1027, S. 22; Schaffland/Wiltfang, BDSG, § 28 Rn. 86.

Datenverarbeitung für den Betroffenen prognostizieren und daraus die Höhe der Beeinträchtigung ableiten.[530] Mit dem Schutzziel aus § 1 Abs. 1 BDSG ist auf das Persönlichkeitsrecht und damit auf einen Eingriff in die „Privat-, Intim-, und Vertraulichkeitssphäre" und das damit verbundene „informationelle Selbstbestimmungsrecht" des Betroffenen abzustellen.[531] Dabei ist die Perspektive eines objektiven Dritten einzunehmen.[532] Eine summarische Prüfung und Interessenabwägung reicht hierbei aus.[533] Zur Abwägung gehört auch die Untersuchung, ob anonymisierte Daten nicht ausreichend sind.[534]

Eine Einwilligung muss bei Vorliegen eines Erlaubnistatbestandes nicht mehr eingeholt werden.[535] Dies widerspräche auch dem Sinn und Zweck eines Erlaubnistatbestandes. Ein Widerspruch des Betroffenen hingegen ist als Ausdruck des Rechts auf informationelle Selbstbestimmung und als schutzwürdiges Interesse einzustufen.[536]

Das Erforderlichkeitskriterium muss ebenso wie in der ersten Tatbestandsvariante erfüllt sein.

(c) § 28 Abs. 1 Nr. 3 BDSG

§ 28 Abs. 1 Nr. 3 BDSG erlaubt die Verarbeitung von Daten aus allgemein zugänglichen Quellen oder wenn die verantwortliche Stelle diese veröffentlichen durfte. Die Regelung ist Ausfluss der Informationsfreiheit und trägt der Tatsache Rechnung, dass diese Daten ohnehin frei zugänglich sind.[537] Darüber hinaus soll die Regelung trotzdem einen ordnungsgemäßen Umgang auch mit personenbe-

---

530 So auch Simitis in Simitis, BDSG, § 28 Rn. 127.

531 Gola/Schomerus in Gola/Schomerus, BDSG, § 28 Rn. 26; BVerfGE 65, 1 = NJW 984, S. 419.

532 Taeger in Taeger/Gabel, BDSG, § 28 Rn. 63.

533 Simitis in Simitis, BDSG, § 28 Rn. 129; Taeger in Taeger/Gabel, BDSG, § 28 BDSG, Rn. 61 ff.; Schaffland/Wiltfang, BDSG, § 28 Rn. 89.

534 Bergmann/Möhrle/Herb, Datenschutzrecht, § 28 Rn. 239.

535 So auch Taeger in Taeger/Gabel, BDSG, § 28 Rn. 20.

536 Taeger in Taeger/Gabel, BDSG, § 28 Rn. 63.

537 So auch Simitis in Simitis, BDSG, § 28 Rn. 146.

zogenen frei zugänglichen Daten sicherstellen. Im Zuge einer automatisierten Datenverarbeitung, die solche Daten in immer wieder neue sachliche Zusammenhänge stellen kann und aus ihrem bisherigen Kontext herauslöst, ist die Gefahr von Verfälschungen besonders hoch.[538]

Allgemein zugänglich sind Daten, die dazu geeignet sind, einem individuell nicht bestimmbaren Personenkreis Informationen zu vermitteln, und sich dazu von ihrer Publikationsform und Zielsetzung her eignen.[539]

(5) Subsumtion

Fraglich erscheint, ob § 28 BDSG in einer seiner Tatbestandsvarianten als Ermächtigung für die Erhebung personenbezogener Daten zwecks Risikoanalyse in Frage kommt. Eine „eigene" Erhebung kommt für die Risikoanalyse zwecks allgemeiner Gefahrenabwehr nur in Betracht, wenn der CN 23 Datensatz nicht bereits anderweitig erhoben worden ist und vorliegt bzw. der Zweck der Erhebung die Risikoanalyse mit einschließt.

Zunächst müssten die Tatbestandsvoraussetzungen des § 27 BDSG erfüllt sein. Als Aktiengesellschaft ist die DPAG eine juristische Person des Privatrechts und somit eine nicht-öffentliche Stelle. Auch andere Postdienstleister werden je nach ihrer Rechtsform juristische Personen des Privatrechts sein. Sähe man die DPAG nicht bereits als nicht-öffentliche Stelle an, so fällt sie auf jeden Fall unter den Begriff des öffentlich-rechtlichen Wettbewerbsunternehmens des Bundes.[540]

Des Weiteren stellt die Risikoanalyse eine Form der automatisierten Datenverwendung zu nicht familiären oder persönlichen Zwecken dar.

Die Tatbestandsvoraussetzungen von § 27 BDSG sind damit erfüllt.

Weiterhin müsste es sich dabei um die Erfüllung eigener Geschäftszwecke handeln. Die Datenerhebung ist sicherlich kein Selbstzweck, sondern dient der Sicherung der Lieferkette. Die Sicherung der Lieferkette wiederum ist nur Mit-

---

538 Simitis in Simitis, BDSG, § 28 Rn. 148.

539 BVerfG 27, S. 71 (83); 27 104 (108); 33, 52 (65); 103, 44 (60).

540 Bergmann/Möhrle/Herb, Datenschutzrecht, § 27 Rn. 11.

tel zum Zweck, um in Erfüllung vertraglicher Verpflichtungen Postsendungen zustellen zu können. Diese Akzessorietät wird hier besonders deutlich. Dass an der Sicherheit der Lieferkette auch Versender und Empfänger ein Interesse haben und womöglich auch ein öffentliches Interesse an der Sicherung der Lieferkette besteht, verdrängt den eigenen Geschäftszweck hier nicht.

Weiterhin müsste eine der Tatbestandsvarianten erfüllt sein.

(a) Subsumtion der Tatbestandsvariante § 28 Abs. 1 Nr. 1 BDSG

Zunächst kommt § 28 Abs. 1 Nr. 1 BDSG in Frage. Vom Vorliegen eines Schuldverhältnisses zwischen Postdiensteanbieter und Kunden kann grundsätzlich ausgegangen werden. Des Weiteren müsste die Datenerhebung für die Begründung, Durchführung oder Beendigung des Schuldverhältnisses erforderlich sein.

Zum Begründen eines Schuldverhältnisses sind sicherlich Basisdaten wie Name und Anschrift notwendig. Um diese Daten für eine Risikoanalyse zwecks allgemeiner Gefahrenabwehr zu erheben, müsste dieser Zweck zur Begründung, Durchführung oder Beendigung des Rechtsgeschäfts erforderlich sein. Zwar sind die Sicherheitsinteressen des Postdienstleisters die Basis für das Zustandekommen eines Rechtsgeschäfts, jedoch wird man die allgemeine Gefahrenabwehr kaum als primäres Ziel eines Rechtsgeschäfts ansehen. Man kann nicht davon ausgehen, dass beide Seiten dies zum Inhalt ihres Vertrages machen oder machen wollen.

Damit kommt § 28 Abs. 1 Nr. 1 BDSG als Erlaubnistatbestand für die Datenerhebung für eine Risikoanalyse durch Postdiensteanbieter zwecks allgemeiner Gefahrenabwehr nicht in Frage.

(b) Subsumtion der Tatbestandsvariante § 28 Abs. 1 Nr. 2 BDSG

Weiterhin kommt § 28 Abs. 1 Nr. 2 BDSG in Frage. Dafür müssten zunächst berechtigte Interessen der verarbeitenden Stelle, hier des Postdiensteanbieters, durch eine Risikoanalyse zwecks allgemeiner Gefahrenabwehr gewahrt werden. Mit der allgemeinen Gefahrenabwehr werden sicherlich auch individuelle Sicherheitsinteressen von Postdienstleistern bedient. So stellt der Schutz

der Lieferkette und damit unter anderem, der Einrichtungen, Mitarbeiter und des Geschäftsablaufs sicherlich ein wirtschaftliches Interesse dar. Im Falle eines Angriffs auf die postalische Lieferkette hat ein Postdiensteanbieter mit einem wirtschaftlichen Schaden (sei es durch Verzögerungen oder Ausfälle in der Zustellung, technische oder bauliche Schäden etc.) zu rechnen. Weiterhin besteht ein Zustellungsinteresse aus wirtschaftlichen und rechtlichen Gründen beim Postdiensteanbieter und hinzutretend auch grundsätzlich ein Zustellungsinteresse beim Versender und Empfänger. Darüber hinaus ist es auch im Interesse des Postdienstleisters, dieses Interesse beider Parteien wahrzunehmen. Schließlich können durch einen Angriff auf die Lieferkette Gesundheit und Leben von Mitarbeitern und Empfängern bzw. damit in Berührung kommenden Dritten gefährdet werden. Neben möglichen Obhuts- und Sicherungspflichten, die einzuhalten im berechtigten Interesse des Unternehmens liegt, besteht in solchen Fällen darüber hinaus ein mehr als ideelles, unternehmerisches und menschliches Schutzinteresse.

Angesichts der expliziten Regelung der staatlichen und öffentlichen Sicherheit in § 28 Abs. 2 Nr. 2 b BDSG stellt sich die Frage, ob Sicherheitsinteressen nicht grundsätzlich nicht unter die berechtigten Interessen fallen und es aus systematischer Sicht Wille des Gesetzgebers war, die Datenverwendung dafür nur gesondert zuzulassen. Wie dargelegt, handelt es sich bei der Gefahrenabwehr nicht nur um ein öffentliches Interesse, sondern liegt auch im Interesse des Postdienstleisters und der betroffenen Parteien. So besteht zum Beispiel im Bereich der Finanzwirtschaft auch eine Pflicht zum Risikomanagement über

§ 25a KWG.[541] Darüber hinaus kann – soweit § 25a KWG nicht vorgeht – ein berechtigtes Interesse zur Abwehr und Aufdeckung gegen Geldinstitute gerichteter krimineller Handlungen bei Anzeichen oder Vorliegen objektiver Tatbestände oder Verhaltensweisen angenommen werden.[542] Im Kreditkartenbereich geht man von einer Zulässigkeit der Datenverarbeitung auch aus Sicherheitsgründen aus (zur Vorbeugung von Missbrauch und Diebstahl).[543] Auch in anderen Bereichen werden Sicherheitsbelange immer wieder als berechtigte Interessen mitgenannt.[544] Dies lässt den Rückschluss zu, dass Sicherheitsbelange und damit eine Risikoanalyse auch im Interesse eines Postdienstleisters liegen können.

Zur Wahrung dieser Interessen muss die Datenerhebung weiterhin erforderlich sein. Die Daten werden für eine Risikoanalyse benötigt, die das Gefahrenpotenzial von Postsendungen klassifizieren und erkennen helfen soll. Im modernen postalischen Massenverkehr führt jede andere „manuelle" Form der Identifikation des Risikos auf gleichem Niveau, die nicht durch eine automatisierte Auswertung erhobener Daten erfolgt, durch exponentiell höheren Personal- und Zeiteinsatz zu höheren Kosten, die eine Beförderung finanziell nicht darstellbar und konkur-

---

541 „§ 25a Besondere organisatorische Pflichten; Verordnungsermächtigung
(1) Ein Institut muss über eine ordnungsgemäße Geschäftsorganisation verfügen, die die Einhaltung der vom Institut zu beachtenden gesetzlichen Bestimmungen und der betriebswirtschaftlichen Notwendigkeiten gewährleistet. Die Geschäftsleiter sind für die ordnungsgemäße Geschäftsorganisation des Instituts verantwortlich; sie haben die erforderlichen Maßnahmen für die Ausarbeitung der entsprechenden institutsinternen Vorgaben zu ergreifen, sofern nicht das Verwaltungs- oder Aufsichtsorgan entscheidet. Eine ordnungsgemäße Geschäftsorganisation muss insbesondere ein angemessenes und wirksames Risikomanagement umfassen, auf dessen Basis ein Institut die Risikotragfähigkeit laufend sicherzustellen hat; das Risikomanagement umfasst insbesondere 1. die Festlegung von Strategien, insbesondere die Festlegung einer auf die nachhaltige Entwicklung des Instituts gerichteten Geschäftsstrategie und einer damit konsistenten Risikostrategie, sowie die Einrichtung von Prozessen zur Planung, Umsetzung, Beurteilung und Anpassung der Strategien; 2. Verfahren zur Ermittlung und Sicherstellung der Risikotragfähigkeit, wobei eine vorsichtige Ermittlung der Risiken und des zu ihrer Abdeckung verfügbaren Risikodeckungspotenzials zugrunde zu legen ist; 3. die Einrichtung interner Kontrollverfahren mit einem internen Kontrollsystem und einer Internen Revision, wobei das interne Kontrollsystem insbesondere a) aufbau- und ablauforganisatorische Regelungen mit klarer Abgrenzung der Verantwortungsbereiche, [...] ".

542 Taeger in Taeger/Gabel, BDSG, § 28 Rn. 60.

543 Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 55.

544 Übersicht auch mit anderen Tätigkeitsfeldern bei Spindler/Nink in Spindler/Schuster, Recht der elektronischen Medien, § 28 BDSG, Rn. 10.

renzunfähig werden lassen. Damit ist man auf die Erhebung von Daten, falls und soweit sie noch nicht vorliegen, angewiesen.

Dieses berechtigte Interesse der verarbeitenden Stelle muss mit dem schutzwürdigen Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung abgewogen werden. Die Betroffenen, Versender und Empfänger, haben grundsätzlich ein Interesse an einer möglichst restriktiven Datenverarbeitung. Hinzu kommt gleichzeitig aber auch ein Interesse an der Sicherheit der Lieferkette, verbunden mit einem Interesse an einer unversehrten Zustellung der Postsendungen und der Unversehrtheit des Empfängers. Das Interesse an einer restriktiven Datenverarbeitung und dem Schutz der eigenen Daten (Namen, Adresse, womöglich Profil der postalischen Aktivitäten) tritt hinter den eigenen Sicherheitsinteressen zurück und überwiegt folglich auch in einer Gesamtabwägung mit den Sicherheitsinteressen des Postdiensteanbieters nicht.

Demzufolge kann eine Risikoanalyse zur allgemeinen Gefahrenabwehr auch im berechtigten Interesse eines Postdienstleisters liegen.

(c) Subsumtion der Tatbestandsvariante § 28 Abs. 1 Nr. 3 BDSG

§ 28 Abs. 1 Nr. 3 BDSG kommt als Tatbestand für eine Ermächtigung nicht in Frage, da die CN 23 Zollinhaltserklärung keine allgemein zugängliche Quelle darstellt.

(6) Zwischenergebnis

Für die Erhebung personenbezogener Daten aus beispielsweise einer Zollinhaltserklärung CN 23 scheiden die Tatbestandsvarianten § 28 Abs. 1 Nr. 1 und 3 BDSG von vornherein aus. In Frage kommt § 28 Nr. 2 BDSG, soweit die Daten noch nicht erhoben worden sind und für eine Risikoanalyse benötigt werden.

gg) § 29 Abs. 1 BDSG

Gemäß § 29 Abs. 1 BDSG ist *„das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel*

dient" zulässig *„wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat, die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 erfüllt sind; Daten im Sinne von § 28a Abs. 2 Satz 4 dürfen nicht erhoben oder gespeichert werden"*.

Mit § 29 BDSG nimmt der Gesetzgeber zur Kenntnis, dass Informationen einen Marktwert haben können, der wirtschaftlich verwertbar ist.[545] Eine Bewertung oder Ordnung der „Kommerzialisierung des Rechts auf informationelle Selbstbestimmung" ist damit noch nicht verbunden, ebenso wenig die Frage nach den „Eigentumsverhältnissen" an personenbezogenen Daten.[546] Trotzdem erfährt dieser Bereich mit der Norm eine Regulierung, indem festgelegt wird unter welchen Voraussetzungen die verarbeitende Stelle personenbezogene Daten als eigenständige Geschäftsobjekte behandeln und verwenden darf.[547]

(1) Tatbestand

Für die Eröffnung des Anwendungsbereichs müssen zunächst die Tatbestandsvoraussetzungen von § 27 BDSG erfüllt sein.[548]

Eine Abgrenzung zu § 28 BDSG erfolgt über den Zweck der Verwendung.[549] Maßgeblich ist die Funktion der zu verarbeitenden Daten.[550] Bei § 28 BDSG erfolgt die Verwendung personenbezogener Daten zur Erfüllung eigener Daten und hat akzessorischen Charakter. Bei § 29 BDSG steht die Verwendung selbst im Mittelpunkt der Tätigkeit, sie ist der Geschäftsgegenstand und damit

---

545 Ehmann in Simitis, BDSG, § 29 Rn. 2.

546 Ehmann in Simitis, BDSG, § 29 Rn. 3.

547 Ehmann in Simitis, BDSG, § 29 Rn. 4; Taeger in Taeger/Gabel, BDSG, § 29 BDSG, Rn. 12.

548 Siehe 4. Teil. C. II. 2.) a) ff) (2).

549 Bergmann/Möhrle/Herb, Datenschutzrecht, § 29 Rn. 16.

550 Ambs in Erbs/Kohlhaas, Strafrechtliche Nebengesetze, § 29 BDSG, Rn. 2.

Selbstzweck.[551] Die Datenerhebung oder Verarbeitung hat hierbei zum Zwecke der Übermittlung zu erfolgen.[552] Es ist möglich, dass eine Datenverarbeitung für eigene Zwecke als auch zum Zwecke der Übermittlung vollzogen wird.[553]

Die Aufzählung der Tätigkeitsfelder Werbung, Auskunftsdateien und Adresshandel sind beispielhaft und schließen andere Tätigkeiten nicht aus.[554]

Der Begriff der Geschäftsmäßigkeit orientiert sich inzwischen nach überwiegender Meinung an § 157 ZPO (entsprechend auch § 46 Abs. 4 S. 1 AO, § 1 Rechtsberatungsgesetz, oder die Definition in § 3 Nr. 10 TKG) und meint jede auf eine gewisse Dauer angelegte Tätigkeit.[555] Eine Gewinnerzielungsabsicht muss nicht vorliegen, *„geschäftsmäßig meint nicht gewerbsmäßig“.*[556] Bei erstmaliger Verwendung von Daten reicht eine Fortsetzungsabsicht.[557]

Weiterhin muss die Datenverarbeitung zum Zwecke der Übermittlung erfolgen. Dies meint eine Übermittlung an Dritte im Sinne des § 3 Abs. 8 S. 2 BDSG und damit an Personen außerhalb der verarbeitenden Stelle.[558]

(2) Subsumtion

Die Voraussetzungen des § 27 BDSG sind wie für die Erhebung gemäß § 28 BDSG gegeben.[559]

---

551 So auch Taeger in Taeger/Gabel, BDSG, § 29 Rn. 3; Gola/Schomerus in Gola/Schomerus, BDSG, § 29 Rn. 12; Ambs in Erbs/Kohlhaas, Strafrechtliche Nebengesetze § 29 BDSG, Rn. 1.

552 Plath in Plath, BDSG, § 29 BDSG, Rn. 8 f.

553 Gola/Schomerus in Gola/Schomerus, BDSG, § 29 BDSG, 11. Aufl. 2012 Rn. 2.

554 Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 6; dazu ausführlicher Ehrmann in Simitis, BDSG, § 29 Rn. 67 ff.

555 Gola/Schomerus in Gola/Schomerus, BDSG, § 29 Rn. 6; Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 3.; ausführlicher Ehmann in Simitis, BDSG, § 29 Rn. 58 ff.

556 Bergmann/Möhrle/Herb, Datenschutzrecht, § 29 Rn. 19; Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 3.

557 Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 3.

558 Schaffland/Wiltfang, BDSG, § 29 Rn. 1, 37; zum Begriff des Dritten siehe 2. Teil. A. VI, 2.) d).

559 Siehe 4. Teil. C. II. 2.) a) ff) (5).

Die Datenverarbeitung zur Sicherung der postalischen Lieferkette stellt keinen Selbstzweck dar. Die Informationen stellen hier keine eigenständige Ware dar, sondern sind nur Mittel zum Zweck mit eindeutig akzessorischem Charakter.[560] Damit ist die Geschäftsmäßigkeit wie auch der Selbstzweck der Erhebung zu verneinen.

(3) Zwischenergebnis

Damit entfällt § 29 BDSG als Ermächtigungsgrundlage zur Sicherung der Lieferkette durch eine Risikoanalyse zwecks allgemeiner Gefahrenabwehr.

hh) § 30 BDSG

Weiterhin könnte § 30 BDSG als Ermächtigungsgrundlage für die Erhebung personenbezogener Daten durch Postdienstleister in Betracht kommen. Werden gemäß § 30 Abs. 1 BDSG *„personenbezogene Daten geschäftsmäßig erhoben und gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies für die Erfüllung des Zwecks der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist“*.

Jedoch ist auch hier die Geschäftsmäßigkeit zu verneinen.[561]

ii) Art. 46 UZK

Art. 46 UZK könnte eine Ermächtigungsgrundlage für Zollbehörden zur Durchführung einer Risikoanalyse zwecks allgemeiner Gefahrenabwehr darstellen.

Art. 46 Abs. II UZK besagt, dass mit Ausnahme von Stichproben Zollkontrollen in erster Linie auf der Grundlage einer Risikoanalyse mit Mitteln der elektronischen Datenverarbeitung erfolgen, mit dem Ziel, anhand von auf einzel-

---

[560] Im Ergebnis auch Wronka, Datenschutzrechtliche Aspekte beim Postversand in RDV 2011, S. 123.

[561] Vgl. § 29 BDSG, 4. Teil. C. II. 2.) a) gg).

staatlicher Ebene, Unionsebene und – soweit verfügbar – internationaler Ebene entwickelten Kriterien Risiken zu ermitteln und abzuschätzen und die erforderlichen Abwehrmaßnahmen zu entwickeln.

(1) Anforderungen an Art. 46 Abs. 2 UZK als Ermächtigungsgrundlage

Fraglich erscheint, ob die Formulierung eine ausreichende Ermächtigungsgrundlage zur Verarbeitung personenbezogener Daten durch Zollbehörden darstellt. Ausgangspunkt ist dabei § 4 Abs. 1 BDSG.

Das Zollrecht folgt nicht der Systematik des BDSG im Bezug auf das Phasenmodell und regelt die Verwendung von Daten nicht in den Schritten des Erhebens, des Verarbeitens und des Nutzens. Dieser Systematik des BDSG muss der Gesetzgeber jedoch nicht zwingend folgen. Der Tatbestand spricht von der Verwendung elektronischer Datenverarbeitung. Verwendung ist dabei als Oberbegriff zu verstehen. Eine Ermächtigung zur Datenverwendung und damit zum Erheben, Verarbeiten und Nutzen wird damit eindeutig ausgesprochen. Der Verweis auf die Risikokriterien präzisiert den Tatbestand weiter und macht eine Abwägung des Gesetzgebers deutlich.

Art. 46 Abs. 2 UZK ist damit als ausreichende Ermächtigungsgrundlage für die Zollbehörden zur Verwendung von personenbezogenen Daten zwecks Risikoanalyse anzusehen.

(2) Tatbestand

Der Tatbestand von Art. 46 Abs. 2 UZK umfasst die Verwendung von personenbezogenen Daten zur elektronischen Datenverarbeitung zwecks Risikoanalyse und eine Auswertung nach vorher festgelegten Risikokriterien.

(3) Subsumtion

Bei einer Risikoanalyse durch die Zollbehörden zwecks Gefahrenabwehr handelt es sich genau um die vom Tatbestand beschriebene Konstellation. Der Zoll wäre folglich ermächtigt, personenbezogene Daten, soweit für eine Risikoanalyse notwendig, auch gesondert zu erheben.

(4) Zwischenergebnis

Eine Erhebung personenbezogener Daten zwecks allgemeiner Gefahrenabwehr durch die Zollbehörden kann somit auf Art. 46 Abs. 2 UZK gestützt werden.

jj) § 13 Abs. 1 BDSG

Eine Erhebung personenbezogener Daten durch die Zollbehörden könnte aufgrund von § 13 Abs. 1 BDSG zulässig sein.

(1) Anwendungsbereich, § 12 BDSG

Zunächst müsste der Anwendungsbereich des § 12 BDSG eröffnet sein. Demnach gelten die Vorschriften des Abschnitts *„für öffentliche Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen“*. Weiterhin gelten sie für die öffentlichen Stellen der Länder, falls diese den Datenschutz nicht selbst regeln *„soweit sie Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt“*.

Öffentliche Stellen des Bundes sind gemäß § 2 Abs. 1 BDSG *„die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht“*. Weiterhin gelten gemäß § 2 Abs. 3 BDSG *„Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen,* [...] *ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn sie über den Bereich eines Landes hinaus tätig werden oder dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht. Andernfalls gelten sie als öffentliche Stellen der Länder.“*

Davon ausgenommen sind nur öffentlich-rechtliche Unternehmen, die am Wettbewerb teilnehmen. Ausschlaggebend für die Abgrenzung ist eine Leistungserbringung, die auch von Privaten erbracht wird, um eine Verzerrung des Wettbewerbs zu verhindern.[562] Im Einzelfall muss nicht zwingend eine Konkurrenzsituation vorliegen.[563]

Öffentliche Stellen der Länder sind gemäß § 2 Abs. 2 BDSG *„die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform“*.

Umfasst wird jedes Handeln der öffentlichen Stelle, das hoheitliche wie auch das fiskalische.[564]

(2) Tatbestandsvoraussetzungen

Gemäß § 13 Abs. 1 BDSG ist das Erheben personenbezogener Daten zulässig, *„wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist“*. Die Erhebung muss damit die Erfüllung einer Aufgabe bedingen und dafür die Voraussetzung der Erforderlichkeit erfüllen. Die Rechtmäßigkeit der Aufgabenerfüllung ist dabei das entscheidende Kriterium für die Zulässigkeit der Erhebung.[565] Die Zuständigkeit der öffentlichen Stelle ist als Voraussetzung der Erfüllung der Aufgaben immanent.[566]

Fraglich ist, wie weit die Datenerhebung gehen darf. Besondere Arten personenbezogener Daten werden in § 13 Abs. 2 BDSG speziell geregelt. Darüber hinaus wird angenommen, dass die Datenerhebung aufgrund allgemei-

---

562 Gola/Schomerus, BDSG, § 12 BDSG, Rn. 2.

563 Gola/Schomerus, BDSG, § 12 BDSG, Rn. 2.

564 Bergmann, Lutz/Möhrle, Roland/Herb, Armin, Datenschutzrecht, § 12 Rn. 9.

565 Gola/Schomerus, BDSG, § 13 BDSG, Rn. 2.

566 So auch Bergmann, Lutz/Möhrle, Roland/Herb, Armin, Datenschutzrecht, § 13 Rn. 14 ff.; Gola/Schomerus, BDSG, § 14 BDSG, Rn. 5; Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 13 BDSG, Rn. 7; Sokol/Scholz in Simitis, BDSG, § 13 Rn. 15 ff.

ner Erlaubnistatbestände wie in § 13 Abs. 1 BDSG nicht zu schwerwiegenden Grundrechtseingriffen führen dürfen.[567] Bei diesen steigt mit Schwere des Eingriffs die Anforderung an die Bestimmtheit und Normklarheit des Erlaubnistatbestandes.[568]

Das Erforderlichkeitskriterium ist eng auszulegen, es gilt hier der Grundsatz der Minimierung der Datenerhebung.[569] Teilweise wird eine Unmöglichkeit der Aufgabenerfüllung ohne die betreffende Information verlangt.[570] Erforderlich ist eine Erhebung nur zur aktuellen Datenerhebung, eine Erhebung auf Vorrat ist nicht als erforderlich einzustufen.[571]

Ergänzend regelt § 13 Abs. 1a BDSG, dass bei der Erhebung bei nicht-öffentlichen Stellen diese auf die Rechtsgrundlage, die sie zur Auskunft verpflichtet, oder auf die Freiwilligkeit ihrer Angaben hinzuweisen ist. Die Aufforderung stellt einen Verwaltungsakt dar, der eine Begründung und die Rechtsgrundlage enthalten soll.[572]

(3) Subsumtion

Zunächst handelt es sich bei den Zollbehörden unzweifelhaft um öffentliche Stellen. Fraglich erscheint, ob dies auch für die DPAG zutrifft. Dafür müsste ihr ein ausschließliches Recht nach dem Postgesetz zustehen. Durch den Wegfall des Postmonopols liegt kein ausschließliches Recht im Bereich der Zustellung von Päckchen und Paketen vor. Auch der Status des Universaldienstleisters kann eine Einstufung als öffentliche Stelle nicht rechtfertigen. Die DPAG ist folglich nicht als öffentliche Stelle einzustufen.

---

567 Gola/Schomerus, BDSG, § 13 BDSG, Rn. 2; Dammann in Simitis, BDSG, § 14 Rn. 2.

568 Gola/Schomerus, BDSG, § 13 BDSG, Rn. 2.

569 Bergmann/Möhrle/Herb, Armin, Datenschutzrecht, § 13 Rn. 22; BSG Urt. v. 28.11.2002 NJW 2003, 2932.

570 Schaffland/Wiltfang, BDSG, § 13 Rn. 4b; Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 13 BDSG, Rn. 14; Sokol/Scholz in Simitis, BDSG, § 13 Rn. 26.

571 Sokol in Simitis, BDSG, § 13 Rn. 26; Gola/Schomerus, BDSG, § 13 BDSG, Rn. 4.

572 Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 13 BDSG, Rn. 20.

Weiterhin müssten die Daten für die Aufgabenerfüllung des Zolls erforderlich sein. Ohne einen auswertbaren Datenkranz wird eine Risikoanalyse kaum durchführbar sein. Jedoch sind für die Risikoanalyse auch nur die Daten zu erheben, die dafür wirklich erforderlich sind.

(4) Zwischenergebnis

Eine Erhebung von Daten durch die Zollbehörden, die für die Risikoanalyse zur allgemeinen Gefahrenabwehr erforderlich sind, könnte über § 13 Abs. 1 BDSG erlaubt sein.

kk) § 28 Abs. 6 BDSG

Die Verwendung besonderer Arten personenbezogener Daten kommt für eine Risikoanalyse innerhalb der postalischen Lieferkette nicht in Betracht. Daher scheidet auch § 28 Abs. 6 BDSG als Ermächtigungsgrundlage aus.[573]

ll) Zwischenergebnis

Als Ermächtigungsgrundlage für die Erhebung personenbezogener Daten durch die Postdienste kommen die Regelungen des Postrechts nicht in Frage. Sowohl § 41 Abs. 2 PostG als auch die §§ 3 und 5 PDSV decken von ihren Ermächtigungen diesen Sachverhalt nicht mit ab.

---

[573] § 28 Abs. 6 BDSG lautet wie folgt: Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn
1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,
2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,
3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder
4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

Im Bereich des BDSG kommen die Tatbestandsvarianten von § 28 Abs. 1 BDSG in Frage. Hiervon sind die Nummern 1 und 3 nicht als Ermächtigungsgrundlagen geeignet. § 28 Abs. 1 Nr. 2 BDSG könnte hingegen als Ermächtigung für die Risikoanalyse wohl grundsätzlich dienen, soweit es anwendbar ist und nicht verdrängt wird.

Als Ermächtigung für die Erhebung personenbezogener Daten durch die Zollbehörden kommen grundsätzlich Art. 46 Abs. 2 UZK sowie § 13 Abs. 1 BDSG in Frage.

b) Ermächtigungsgrundlagen für eine Datennutzung

Die Ermächtigungsgrundlagen für eine Datennutzung können sich von den Ermächtigungsgrundlagen für eine Datenerhebung unterscheiden und sind deswegen gesondert zu untersuchen.

Für die Nutzung personenbezogener Daten durch Postdienstleister zwecks Risikoanalyse kommen als Ermächtigungsgrundlagen Normen des Postrechts – speziell § 41 Abs. 2 PostG und § 3 Abs. 4 PDSV – sowie die Tatbestandsvarianten des § 28 BDSG in Frage.

Für die Nutzung personenbezogener Daten durch die Zollbehörden kommen § 14 BDSG sowie Art. 46 Abs. 2 UZK in Betracht.

aa) § 41 Abs. 2 PostG

Zunächst kommen die Tatbestandsvarianten des § 41 Abs. 2 PostG als Ermächtigung für die Nutzung personenbezogener Daten durch Postdiensteanbieter in Betracht. Die Bewertung der Tatbestandsvoraussetzungen unterliegt hier der gleichen Wertung wie bei der Datenerhebung.[574] Damit sind „parallel“ die gleichen Schlüsse aus dem Sachverhalt – bezogen auf die Nutzung von personenbezogenen Daten – zu ziehen und die Anwendbarkeit des § 41 Abs. 2 PostG als Ermächtigungsgrundlage ist abzulehnen.

---

[574] Siehe 4. Teil. C. II. 2.) a) aa).

bb) § 3 Abs. 4 PDSV

Gemäß § 3 Abs. 4 PDSV dürfen Diensteanbieter *„im Zusammenhang mit der Erbringung von Postdiensten erhobene Daten für andere Zwecke nur verarbeiten oder nutzen, wenn eine Rechtsvorschrift eine solche Verwendung dieser Daten ausdrücklich vorsieht oder der Beteiligte eine Einwilligung erteilt hat, die den Vorschriften des Bundesdatenschutzgesetzes und dieser Verordnung entspricht“*.

Eine solche Vorschrift müsste sich genau auf die Verarbeitung und Nutzung von personenbezogenen Daten im postalischen Kontext richten. Würde die Vorschrift die Einbeziehung einer allgemeinen Regelung, etwa § 28 BDSG, rechtfertigen, liefen die speziellen Regelungen des PostG und der PDSV ins Leere.

Eine solche Vorschrift für die Nutzung personenbezogener Daten zwecks allgemeiner Gefahrenabwehr durch die Post ist folglich nicht ersichtlich.

cc) § 28 Abs. 1 BDSG

§ 28 Abs. 1 BDSG könnte ebenfalls als Ermächtigungsgrundlage für eine Nutzung personenbezogener Daten zwecks Risikoanalyse durch die Post in Frage kommen, *„das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig wenn* [...] *“.*

(1) Tatbestände § 28 Abs. 1 BDSG

Für die Tatbestandsvoraussetzungen gelten zunächst die gleichen Überlegungen wie für die Datenerhebung.[575] Eine Nutzung der Daten umfasst auch ein Auswerten und das mit ihnen Arbeiten.[576]

Die Tatbestandsvarianten gemäß § 28 Abs. 1 Nr. 1 und 3 BDSG kommen wie schon bei der Erhebung der Daten nicht in Betracht.[577] Auch hier könnte

---

575 Siehe 4. Teil. C. II. 2.) a) ff) (4).

576 Schaffland/Wiltfang, BDSG, § 28 Rn. 2a.

577 Siehe 4. Teil. C. II. 2.) a) ff) (4) (a), (c).

§ 28 Abs. 1 Nr. 2 BDSG in Frage kommen. Die Nutzung personenbezogener Daten unterliegt den gleichen Voraussetzungen wie ihre Erhebung.[578]

(2) Subsumtion

Der Anwendungsbereich des § 27 BDSG ist eröffnet.[579]

Des Weiteren muss die Durchführung einer Risikoanalyse ebenfalls unter dem Tatbestand von § 28 Abs. 1 Nr. 2 BDSG zu subsumieren sein. Dafür muss die beabsichtigte Nutzung bei der Datenerhebung vorgelegen haben und von dessen Zweck mitumfasst sein. Die Nutzung des CN 23 Datensatzes kommt damit nicht in Betracht, da dieser zu einem anderen Zweck erhoben wird. Eine Datennutzung von auf einem anderen Wege erhobenen Daten kommt dagegen grundsätzlich in Betracht (dürfte in der Praxis jedoch kaum vorliegen).[580]

Wie schon bei der Erhebung von Daten ist die Nutzung aus gleichen Gründen als interessenbezogen zu qualifizieren.[581]

Schließlich muss die Nutzung erforderlich sein. Ein äquivalentes „Erkennen" des Risikos bzw. des Gefährdungspotenzials, das sich nicht auf eine automatisierte Auswertung von Daten stützt ist nicht ersichtlich. Ein „manuelles" Untersuchen jeder einzelnen Postsendung wird nicht als gleichwertig einzustufen sein. Ein manuelles Auswerten von Daten ist dagegen – aufgrund komplexer mathematischer Formeln – technisch unmöglich.

Demnach ist die automatisierte Auswertung von Daten als Risikoanalyse als notwendig einzustufen, um ein bestimmtes Schutzniveau zu erreichen, und damit auch erforderlich.

---

578 Siehe 4. Teil. C. II. 2.) a) ff) (4) (b).

579 Vgl. 4. Teil. C. II. 2.) a) ff) (5).

580 Dafür bedürfte es in der Praxis eigens zum Zwecke der Risikoanalyse erhobener Daten. Wenn auch nicht in der Praxis wahrscheinlich, so ist dies jedoch juristisch möglich.

581 Vgl. 4. Teil. C. II. 2.) a) ff) (5) (b).

(3) Zwischenergebnis

Folglich kommt § 28 Abs. 1 Nr. 2 BDSG als Ermächtigung für eine Nutzung personenbezogener Daten zur Risikoanalyse durch Postdiensteanbieter grundsätzlich in Betracht.

dd) § 28 Abs. 2 BDSG

Weiterhin kommt § 28 Abs. 2 BDSG als Ermächtigungsgrundlage für eine Nutzung personenbezogener Daten durch Postdiensteanbirter in Betracht. Gemäß § 28 Abs. 2 BDSG ist *„die Übermittlung oder Nutzung für einen anderen Zweck*" zulässig unter den Voraussetzungen von § 28 Abs. 1 S. 1 Nr. 2 oder Nr. 3 BDSG, *soweit dies „zur Wahrung berechtigter Interessen eines Dritten"* oder *„zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten"* erfolgt *„und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat",* oder *„wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann"*. § 28 Abs. 2 Nr. 3 BDSG ist für die untersuchte Datenverarbeitung nicht relevant.

Die Zweckbindung ist im Datenschutzrecht ein Ausfluss von Art. 6 c) RL 95/46/EG: *„den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen*". Erwägungsgrund Nr. 28 der Richtlinie präzisiert die Zweckbindung weiter: *„Die Verarbeitung personenbezogener Daten muß gegenüber den betroffenen Personen nach Treu und Glauben erfolgen. Sie hat den angestrebten Zweck zu entsprechen, dafür erheblich zu sein und nicht darüber hinauszugehen. Die Zwecke müssen eindeutig und rechtmäßig sein und bei der Datenerhebung festgelegt werden. Die Zweckbestimmungen der Weiterverarbeitung nach der Erhebung dürfen nicht mit den ursprünglich festgelegten Zwecken unvereinbar sein."*

§ 28 Abs. 2 BDSG stellt eine Durchbrechung des Zweckbindungsgrundsatzes dar, indem eine Verwendung von Daten für einen anderen als den eigentlichen Zweck unter bestimmten Voraussetzungen möglich ist.[582] Die Tatbestandsvarianten sind abschließend.[583]

(1) Tatbestandsvoraussetzungen § 28 Abs. 2 BDSG

Der Anwendungsbereich des § 27 BDSG gilt, ebenso wie für die Erhebung von Daten in § 28 Abs. 1 BDSG.[584]

Eine Zweckänderung ist entsprechend dem Wortlaut nur für eine Übermittlung oder Nutzung gestattet. Die Eigenständigkeit von § 28 Abs. 2 BDSG erklärt sich hierbei aus einem separaten Prüfungsschritt.[585] Die Interessenlage kann sich dabei überschneiden, muss dies jedoch nicht notwendigerweise.

Fraglich erscheint, was unter einer Zweckänderung in zeitlicher als auch materieller Hinsicht zu verstehen ist. Grundsätzlich ist der Zweck bei Datenerhebung, spätestens aber bis zum Speichern festzulegen.[586] Der Zweck kann für die Tatbestandsvarianten des § 28 Abs. 2 BDSG später geändert werden.[587] Die weitere Verwendung und damit Zweckänderung des „ursprünglichen Zwecks", für den die Daten eigentlich erhoben worden sind, kann jedoch auch schon bei Erhebung vorliegen. Für diese Sichtweise spricht die Akzessorietät der Datenverarbeitung.

(a) § 28 Abs. 2 Nr. 1 BDSG

§ 28 Abs. 2 Nr. 1 BDSG gestattet eine Zweckänderung bei Wahrung eigener Interessen oder bei allgemein zugänglichen Daten. Die Begriffe sind dabei wie in

---

582 So auch Plath in Plath, BDSG, § 28 BDSG, Rn. 91; Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 69.

583 Plath in Plath, BDSG, § 28 BDSG, Rn. 91; Simitis in Simitis, BDSG, § 28 Rn. 169; Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 69.

584 Siehe 4. Teil. C. II. 2.) a) ff) (2).

585 Polenz, Kilian/Heussen CHB, Materielles allgemeines Datenschutzrecht Rn. 18 f.

586 Bergmann/Möhrle/Herb, Datenschutzrecht, § 28 Rn. 282 ff.; wohl auch Roßnagel, Datenschutz in der künftigen Verkehrstelematik in NVZ 2006, S. 285 (287).

587 Bergmann/Möhrle/Herb, Datenschutzrecht, § 28 Rn. 284.

§ 28 Abs. 1 BDSG zu verstehen.[588] Ebenso darf das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung oder Nutzung seiner personenbezogenen Daten nicht überwiegen.

Dabei muss jedoch der geänderte Zweck mit dem eigenen Geschäftszweck in einem Zusammenhang stehen.[589] Die Existenzberechtigung der Norm neben § 28 Abs. 1 S. 1 Nr. 2 oder 3 BDSG besteht in der grundsätzlichen Zweckbindung der Datenverarbeitung, die hier dadurch besonders zum Ausdruck kommt.[590] Die prinzipiell legitimen Gründe auf die sich hier die Erlaubnistatbestände stützen, sollen bei jeder Zweckänderung oder weitergehenden Datenverarbeitung hinterfragt werden.[591]

(b) § 28 Abs. 2 Nr. 2a BDSG

Ein weiterer möglicher Zweckänderungsgrund ist nach § 28 Abs. 2 Nr. 2a BDSG die Wahrung berechtigter Interessen Dritter. Diese Interessen können, wie bei den eigenen berechtigten Interessen, rechtlicher, materieller oder ideeller Natur sein. Auch sie müssen mit den schutzwürdigen Interessen der Betroffenen abgewogen werden.

(c) § 28 Abs. 2 Nr. 2b BDSG

Nach § 28 Abs. 2 Nr. 2b BDSG wird eine Zweckänderung zur Gefahrenabwehr im Bereich der staatlichen oder öffentlichen Sicherheit sowie zur Verfolgung von Straftaten erlaubt. Für die Behörden der Polizei und Staatsanwaltschaft finden sich in der StPO und den Polizeigesetzen für diese spezialgesetzliche Regelungen, somit sind die Strafverfolgungsbehörden auf diese Ermächtigungsgrundlage nicht angewiesen, um Daten von der verarbeitenden Behörde zu bekommen.[592] Der Tatbestand ist auf die Erfüllung von Art. 13 RL 95/46/EG angelegt.[593]

---

588 Siehe 4. Teil. C. II. 2.) a) ff) (4).

589 Taeger in Taeger/Gabel, BDSG, § 28 Rn. 121.

590 Taeger in Taeger/Gabel, BDSG, § 28 Rn. 122 ff.

591 Taeger in Taeger/Gabel, BDSG, § 28 Rn. 122 ff.

592 Ausführlich bei Simitis in Simitis, BDSG, § 28 Rn. 190 ff.

593 Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 77.

Ordnungswidrigkeiten sind vom Begriff der Verfolgung von Straftaten nicht umfasst.[594]

Weiterhin ist notwendig, dass für eine Zweckänderung bereits konkrete Anhaltspunkte für das Bestehen einer Gefahr oder einer Straftat vorliegen.[595] Eine abstrakte Gefahrenlage reicht hier nicht aus.[596]

Fraglich erscheint, ob es einer Interessenabwägung bedarf oder ob überhaupt das Vorliegen schutzwürdiger Interessen den Tatbestand sperrt. Die Formulierung „überwiegt" wurde aus Abs. 1 nicht übernommen, sondern stattdessen die Konstruktion „und kein Grund zur Annahme besteht" gewählt, was für eine andere Intention des Gesetzgebers spricht. Zudem würden bei einer Abwägung mit der öffentlichen Sicherheit oder einer Verfolgung von Straftaten die Interessen des Betroffenen wohl grundsätzlich unterliegen. So ist davon auszugehen, dass keine Interessenabwägung stattfindet.[597]

Jedoch wird man von einem hohen Argumentationsaufwand ausgehen müssen, um ein schutzwürdiges Interesse des Betroffenen zu bejahen, das einer Datenverarbeitung zur Gefahrenabwehr für die staatliche oder öffentliche Sicherheit oder zur Strafverfolgung entgegensteht.

(2) Subsumtion

Fraglich erscheint, ob eine der Tatbestandsvarianten als Ermächtigung für eine Nutzung personenbezogener Daten in Frage kommt.

Bezüglich der Tatbestandsvarianten § 28 Abs. 2 Nr. 1 BDSG sind die gleichen Wertungen zu ziehen wie für die Datenerhebung.[598] Daraus ergibt sich, dass eine

---

[594] Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 28 Rn. 79; Taeger in Taeger/Gabel, BDSG, § 28 BDSG, Rn. 145.

[595] Plath in Plath, BDSG, § 28 BDSG, Rn. 97.

[596] Taeger in Taeger/Gabel, BDSG, § 28 Rn. 144; Bergmann/Möhrle/Herb, Datenschutzrecht, § 28 Rn. 296.

[597] Im Ergebnis auch Simitis in Simitis, BDSG, § 28 Rn. 195; wohl auch Bergmann/Möhrle/Herb, Datenschutzrecht, § 28 Rn. 288.

[598] Siehe 4. Teil. C. II. 2.) a) ff) (5) (a).

Nutzung personenbezogener Daten zur Wahrung berechtigter Interessen grundsätzlich möglich ist.

Ein berechtigtes Interesse Dritter (§ 28 Abs. 2 Nr. 2a) BDSG) könnte das Interesse anderer Postkunden an der Sicherheit und Funktionsfähigkeit der postalischen Lieferkette sein. Jedoch wird man aus diesem sehr weiten Grundbedürfnis keinen konkreten Eingriff in die informationelle Selbstbestimmung des Betroffenen ableiten können, zumal jeder Postkunde gleichermaßen Betroffener und Dritter wäre.

Weiterhin kommt eine Zulässigkeit der Nutzung personenbezogener Daten aus § 28 Abs. 2 Nr. 2b BDSG in Betracht. Mit der Infrastruktur der postalischen Lieferkette ist sicherlich auch die öffentliche Sicherheit betroffen. Ein generell-abstraktes Strafverfolgungsinteresse, das mittels einer Risikoanalyse durchgesetzt werden könnte, ist jedoch abzulehnen.

Des Weiteren müssten auch konkrete Anhaltspunkte für das Bestehen einer Gefahr vorliegen. Die postalische Risikoanalyse anhand automatisierter Datenverarbeitung arbeitet unabhängig konkreter Anhaltspunkte und ist auf eine präventive Datenverarbeitung auch nicht verdächtiger Daten angewiesen. Folglich scheidet § 28 Abs. 2 Nr. 2 BDSG als Ermächtigungsgrundlage aus.

(3) Zwischenergebnis

Als Ermächtigung für eine Nutzung personenbezogener Daten kommt – soweit sie nicht verdrängt wird und anwendbar ist – die Tatbestandsvariante § 28 Abs. 2 Nr. 1 i. V. m. § 28 Abs. 1 Nr. 2 BDSG in Frage.

ee) Ermächtigungen aus der PDSV als Grundlage für eine Datennutzung

Die in den §§ 3 und 5 PDSV enthaltenen Ermächtigungen für die Nutzung personenbezogener Daten scheiden als Ermächtigung für die Nutzung zwecks Risikoanalyse aus den gleichen Gründen aus, wie für die Erhebung dieser Daten.[599]

[599] Vgl. 4. Teil. C. II. 2.) a) bb–ee).

ff) § 29 BDSG

Für die Zulässigkeit der Nutzung personenbezogener Daten durch Postdienste im Rahmen der Ermächtigungen von § 29 BDSG gelten die gleichen grundsätzlichen Wertungen, wie für das Erheben dieser Daten.[600] Der Selbstzweck der Nutzung ist daher abzulehnen. Damit scheiden auch die Tatbestandsvarianten des § 29 BDSG als Ermächtigung für die Nutzung personenbezogener Daten durch Postdienste im Rahmen der Risikoanalyse aus.

gg) § 14 Abs. 1 BDSG

Weiterhin könnte § 14 BDSG als Ermächtigungsgrundlage für das Nutzen personenbezogener Daten durch die Zollbehörden in Frage kommen.

Gemäß § 14 Abs. 1 BDSG ist das Speichern, Verändern oder Nutzen personenbezogener Daten zulässig, *„wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind“*.

(1) Anwendungsbereich, § 12 BDSG

Der Anwendungsbereich von § 14 Abs. 1 BDSG richtet sich nach § 12 BDSG.[601]

(2) Tatbestandsvoraussetzungen

§ 14 Abs. 1 BDSG legt eine Zweckbindung für die Verwendung personenbezogener Daten fest. Ausgehend davon ist eine Verwendung nur zu dem Zweck erlaubt, zu dem die Daten erhoben worden sind. Wenn keine Erhebung vorausgegangen ist, ist eine Verwendung nur zu dem Zweck erlaubt, für den die Daten gespeichert worden sind. Dies sichert eine Zweckidentität zwischen Erhebung und Verwendung und grenzt darüber hinaus die Verwendung zunächst auf die

---

600 Vgl. 4. Teil. C. II. 2.) a) gg).

601 Siehe 4. Teil. C. II. 2.) a) jj) (1).

bei der Erhebung festgelegten Zwecke ein.[602] Von der Zweckbindung umfasst können neben dem Hauptzweck auch Hilfs- und Nebenzwecke sein, die mit dem Hauptzweck eng verbunden sind und der Erfüllung der Aufgabe dienen.[603]

Anders als in § 13 BDSG ist der Tatbestand in § 14 Abs. 1 BDSG präziser und legt die Zuständigkeit der verantwortlichen Stelle fest. Die verantwortliche Stelle muss dafür örtlich, sachlich und instanziell zuständig sein.[604] Die Rechtmäßigkeit der Datenverwendung ist dem Tatbestand immanent.[605] Schließlich muss die Datenverwendung erforderlich sein. Dies ist eng auszulegen. Sie beinhaltet ebenfalls eine zeitliche Komponente, eine Speicherung auf Vorrat oder Verdacht hin ist ohne weitergehende Ermächtigungsgrundlage in der Regel unzulässig.[606]

(3) Subsumtion

Würden Daten in zulässiger Weise für die Risikoanalyse erhoben, könnten diese anschließend zu diesem Zweck ebenfalls genutzt werden.[607] Weiterhin müsste die Datennutzung auch erforderlich sein. Um aussagekräftige Risikoprofile zu erhalten, kann auch die Auswertung personenbezogener Daten notwendig sein.

(4) Zwischenergebnis

Die Nutzung personenbezogener Daten durch die Zollbehörden zwecks Risikoanalyse zur allgemeinen Gefahrenabwehr ist aus § 14 Abs. 1 BDSG denkbar.

---

602 Bergmann/Möhrle/Herb, Datenschutzrecht, § 14 Rn. 17 ff.; Dammann in Simitis, BDSG, § 14 Rn. 37.

603 Dammann in Simitis, BDSG, § 14 Rn. 47 f.

604 Schaffland/Wiltfang, BDSG, § 14 BDSG, Rn. 10; ausführlicher dazu Dammann in Simitis, BDSG, § 14 Rn. 6 ff.

605 BT-Drucksache 11/4306, S. 44 zitiert aus Schaffland/Wiltfang, BDSG, § 14 BDSG, Rn. 7; Gola/Schomerus, BDSG, § 14 BDSG, Rn. 9; Bergmann/Möhrle/Herb, Datenschutzrecht, § 14 Rn. 11.

606 Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 14 Rn. 8 ff.; Schaffland/Wiltfang, BDSG, § 14 BDSG, Rn. 13 ff.

607 In der Praxis ist eine Erhebung von Daten eigens für die Risikoanalyse unwahrscheinlich, jedoch rechtlich zulässig.

hh) § 14 Abs. 2 BDSG

Weiterhin könnte § 14 Abs. 2 BDSG eine Ermächtigung für die Nutzung personenbezogener Daten durch die Zollbehörden darstellen. Dieser stellt eine Durchbrechung des Zweckbindungsgrundsatzes in § 14 Abs. 1 BDSG dar. Dafür statuiert § 14 Abs. 2 BDSG neun Tatbestandsvarianten, wenn *„1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt, 2. der Betroffene eingewilligt hat, 3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde, 4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen, 5. die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt, 6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist, 7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen erforderlich ist, 8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder 9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann“*. Die Aufzählung ist als Zweckänderungsmöglichkeit abschließend.[608]

Auch für § 14 Abs. 2 BDSG wird der Anwendungsbereich durch § 12 BDSG festgelegt.[609]

---

608 Bergmann/Möhrle/Herb, Datenschutzrecht, § 14 Rn. 22; Wedde in Däubler/Klebe/Wedde/Weichert, BDSG, § 14 Rn. 12.

609 Siehe 4. Teil. C. II. 2.) a) jj) (1).

(1) Tatbestandsvoraussetzungen

§ 14 Abs. 2 Nr. 1 BDSG verweist auf spezialgesetzlich geregelte Ermächtigungsgrundlagen, die im Einklang mit § 14 BDSG eine weitergehende Verwendung erlauben. Dazu können auch Normen zählen, die eine Datenverarbeitung zwingend voraussetzen, diese jedoch im Tatbestand selbst nicht erwähnen.[610]

Eine Zweckänderung durch die Einwilligung des Betroffenen (§ 14 Abs. 2 Nr. 2 BDSG) gehört zu den generellen Zweckänderungsmöglichkeiten. Die Voraussetzungen von § 4a BDSG sind dabei zu beachten. Für ein Handeln ohne Einwilligung des Betroffenen und ohne weiteren Erlaubnistatbestand (§ 14 Abs. 2 Nr. 3 BDSG) muss die Datenverwendung objektiv im Interesse des Betroffenen liegen und offensichtlich ohne Weiteres für einen Bediensteten der verantwortlichen Stelle erkennbar sein.[611]

Gemäß § 14 Abs. 2 Nr. 6 BDSG ist eine Zweckänderung zur Gefahrenabwehr möglich. Die Vorschrift enthält drei unabhängige Tatbestände:[612] die Abwehr von Nachteilen für das Gemeinwohl, die öffentliche Sicherheit und die erheblichen Belange des Gemeinwohls. Die Voraussetzungen sind wie in § 13 Abs. 2 Nr. 5 und 6 BDSG zu werten.[613] Der Tatbestand ist gegenüber Spezialvorschriften subsidiär.[614] Der Tatbestand ist nicht so streng formuliert wie in § 28 BDSG, was angesichts des Handelns öffentlicher Stellen angemessen erscheint. Es bedarf jedoch immer noch eines erheblichen Nachteils für das Gemeinwohl oder der Erforderlichkeit der Zweckänderung und Datenverwendung zur Wahrung erheblicher Belange des Gemeinwohls. Der Schwerpunkt der Regelung liegt im Sicherheitsbereich, in der Abwägung des informationellen Selbstbestimmungsrechts des Einzelnen und in den Rechtsgütern der Allgemeinheit.[615] Der Begriff

---

610 Dammann in Simitis, BDSG, § 14 Rn. 56.

611 Schaffland/Wiltfang, BDSG, § 14 BDSG, Rn. 25; Bergmann, Bergmann/Möhrle/Herb, Datenschutzrecht, § 14 Rn. 26.

612 So auch Dammann in Simitis, BDSG, § 14 Rn. 72.

613 So auch Gola/Schomerus, BDSG, § 14 BDSG, Rn. 20.

614 Heckmann in Taeger/Gabel, BDSG, § 14 BDSG, Rn. 68; Dammann in Simitis, BDSG, § 14 Rn. 76.

615 So auch Wedde in Däubler/Klebe/Wedde/Weichert in BDSG, § 14 BDSG, Rn. 18.

des Gemeinwohls ist weit formuliert und daher aufgrund des Zusatzes „erheblich“ eng auszulegen.[616] Es ist dabei auf eine Beeinträchtigung der Funktionsfähigkeit von Behörden oder Organen abzustellen.[617]

Die Definition der Gefahrenabwehr für die öffentliche Sicherheit richtet sich nach dem Polizeirecht und meint den Schutz der verfassungsmäßigen Ordnung, der Rechtsordnung sowie der Schutzgüter der Bürger.[618]

(2) Subsumtion

Ein Strafverfolgungsinteresse (§ 14 Abs. 2 Nr. 7 BDSG) ist ebenso abzulehnen wie die schwerwiegende Beeinträchtigung der Rechte einer anderen Person (§ 14 Abs. 2 Nr. 8 BDSG).[619]

In Betracht kommen die Tatbestandsvarianten von § 14 Abs. 2 Nr. 6 BDSG. Schutzgut ist dabei die postalische Lieferkette als solche. Dieser beeinhaltet schützenswerte Positionen der DPAG als Private, aber auch die Funktionsfähigkeit des Universaldienstes als Gut der Allgemeinheit.

(3) Zwischenergebnis

In Betracht kommt § 14 Abs. 2 Nr. 6 BDSG als Erlaubnistatbestand für eine Nutzung personenbezogener Daten durch die Zollbehörden zwecks Risikoanalyse. Jedoch ist davon auszugehen, dass dieser gegenüber Art. 46 Abs. 2 UZK subsidiär zurücktritt.

ii) Art. 46 Abs. 2 UZK

Weiterhin kommt Art. 46 Abs. 2 UZK als Ermächtigungsgrundlage für eine Nutzung personenbezogener Daten zum Zwecke einer Risikoanalyse zur allgemeinen Gefahrenabwehr durch die Zollbehörden in Betracht.

---

616 Im Ergebnis auch Dammann in Simitis, BDSG, § 14 Rn. 73.

617 Heckmann in Taeger/Gabel, BDSG, § 14 BDSG, Rn. 69.

618 Heckmann in Taeger/Gabel, BDSG, § 14 BDSG, Rn. 72; Dammann in Simitis, BDSG, § 14 Rn. 72.

619 Siehe 4. Teil. C. II. 2.) b) dd) (2).

(1) Tatbestand

Die Formulierung des Art. 46 Abs. 2 UZK kommt grundsätzlich als Erlaubnistatbestand für eine Nutzung personenbezogener Daten in Frage. Der Begriff der Verwendung automatisierter Datenverarbeitungsmethoden schließt eine Nutzung mit ein.

Wurden Daten nicht für eine Risikoanalyse erhoben, ist zur Zweckänderung von Daten zur Risikoanalyse Art. 46 Abs. 2 UZK in Verbindung mit § 14 Abs. 2 Nr. 1 BDSG zu lesen. Demnach ist eine Zweckänderung zur Nutzung personenbezogener Daten zulässig, wenn *„eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt"*. Die Risikoanalyse ist auf die Nutzung personenbezogener Daten, die dem Zoll durch Anmeldung vorliegen bzw. anderweitig erhoben worden sind, angewiesen. Die Formulierung der Norm setzt die Nutzung vorhandener Daten geradezu voraus, insoweit kann von einer zwingenden Voraussetzung gesprochen werden.

(2) Subsumtion

Wie schon bei der Erhebung personenbezogener Daten, ist der Tatbestand von Art. 46 Abs. 2 UZK auf die Nutzung personenbezogener Daten zwecks Risikoanalyse des Zolls zur allgemeinen Gefahrenabwehr zugeschnitten. Die Auswertung der Informationen zur Erstellung von Risikoprofilen entspricht der Verwendung automatisierter Datenverarbeitungsmethoden.

Die Zweckänderung des Datenkranzes der CN 23 Zollinhaltserklärung zur Gefahrenabwehr kann als zwingende Voraussetzung von Art. 46 Abs. 2 UZK im Sinne von § 14 Abs. 2 Nr. 1 BDSG gewertet werden.

(3) Zwischenergebnis

Eine Nutzung personenbezogener Daten durch die Zollbehörden zwecks Risikoanalyse zur allgemeinen Gefahrenabwehr ist gemäß Art. 46 Abs 2 UZK (i. V. m. § 14 Abs. 2 Nr.1 BDSG) zulässig.

jj) Zwischenergebnis

Als Ermächtigungsgrundlagen für eine Datennutzung personenbezogener Daten der CN 23 Zollinhaltserklärung durch die Postdiensteanbieter kommt § 28 Abs. 2 Nr. 1 BDSG in Frage. Soweit es sich um Datensätze handelt, die identisch sind, aber anders erhoben worden sind und der Zweck entsprechend die Nutzung deckt, kommt weiterhin § 28 Abs. 1 Nr. 2 BDSG in Betracht. § 41 Abs. 2 PostG sowie § 3 PDSV bilden dagegen keine ausreichende Ermächtigungsgrundlage.

Die Datennutzung der Zollbehörden richtet sich nach Art. 46 Abs. 2 UZK, bei einer Zweckänderung personenbezogener Daten in Verbindung mit § 14 Abs. 2 Nr. 1 BDSG. § 14 Abs. 2 Nr. 6 BDSG tritt demgegenüber subsidiär zurück.

c) Ermächtigungsgrundlagen für eine Datenverarbeitung

Die Ermächtigungsgrundlagen für eine Datenverarbeitung müssen ebenfalls getrennt von den Ermächtigungsgrundlagen für eine Datenerhebung und eine Datennutzung untersucht werden.

Der Begriff der Datenverarbeitung umfasst die Übermittlung wie auch das Speichern personenbezogener Daten.

Auf ihre Relevanz sind daher neben Rechtsvorschriften aus dem Datenschutzrecht und Postrecht auch Vorschriften des Zollrechts zu untersuchen, die eine Datenweitergabe an Behörden rechtfertigen könnten.

aa) § 41 Abs. 2 PostG

Zunächst kommen auch für die Datenverarbeitung die Tatbestandsvarianten des § 41 Abs. 2 PostG in Betracht. Die Tatbestandsvoraussetzungen sind wie bei der Datenerhebung zu bewerten.[620] So sind sowohl für das Speichern als auch für die Weitergabe von Daten die gleichen grundsätzlichen Wertungen bezüglich der Risikoanalyse zu ziehen.

---

620 Siehe 4. Teil. C. II. 2.) a) aa).

Damit kommen die Tatbestandsvarianten des § 41 Abs. 2 PostG als Ermächtigungsgrundlagen für das Speichern und das Weitergeben personenbezogener Daten im Rahmen der Risikoanalyse nicht in Betracht.

bb) § 40 PostG

Gemäß § 40 PostG dürfen *„Unternehmen und Personen, die geschäftsmäßig Postdienste erbringen oder an der Erbringung solcher Dienste mitwirken“*, *„Gerichten und Behörden auf deren Verlangen die zustellfähige Anschrift eines am Postverkehr Beteiligten“* mitteilen, *„soweit dies für Zwecke des Postverkehrs der Gerichte oder Behörden erforderlich ist“*. Diese konstellation meint nur den Zugang zu Adressen zu Zwecken des Postverkehrs. Eine Risikoanalyse ist davon nicht umfasst. Als Ermächtigungsgrundlage kommt § 40 PostG daher nicht in Betracht.

cc) § 5 ZollVG

Eine besondere Stellung nimmt § 5 ZollVG als Sondervorschrift für Postsendungen ein. Es gilt zu untersuchen, inwieweit diese zollrechtliche Vorschrift ebenfalls eine Ermächtigung zur Datenweitergabe beinhaltet.

(1) § 5 Abs. 1 ZollVG

§ 5 Abs. 1 ZollVG regelt: *„Soweit Postsendungen nicht bereits nach Maßgabe des Zollkodex und sonstiger gemeinschaftsrechtlicher Vorschriften zu gestellen sind, legt die Deutsche Post AG Sendungen der zuständigen Zollstelle zur Nachprüfung vor, bei denen zureichende tatsächliche Anhaltspunkte dafür bestehen, daß Waren unter Verstoß gegen ein Einfuhr-, Durchfuhr- oder Ausfuhrverbot in den oder aus dem Geltungsbereich dieses Gesetzes verbracht werden. Das Brief- und Postgeheimnis nach Art. 10 des Grundgesetzes wird für die Gestellung sowie für die Vorlegung sonstiger Sendungen eingeschränkt“*.

Dabei handelt es sich zunächst um eine zollrechtliche Vorschrift, die den Vorgang der Gestellung für den postalischen Bereich regelt. Aus ihr folgt eine Gestel-

lungspflicht der DPAG für die betroffenen Sendungen.[621] In welcher Form dieser Vorgang in der Praxis zu geschehen hat, wird vom Gesetz nicht geregelt.

(2) § 5 Abs. 2 ZollVG

Weiter regelt § 5 Abs. 2 ZollVG: *„Die Deutsche Post AG ist befugt, für von ihr beförderte Waren, die nach Maßgabe des Zollkodex zu gestellen sind, Zollanmeldungen in Vetretung des Empfängers abzugeben“.*

Dabei handelt es sich um eine Vertretungsmacht kraft Gesetz für die DPAG, für den Empfänger die Zollanmeldung gegenüber den Zollbehörden abzugeben.[622]

(3) § 5 ZollVG aus datenschutzrechtlicher Perspektive

Fraglich erscheint, welchen Charakter die Norm aus datenschutzrechtlicher Perspektive einnimmt. So ist faktisch mit der Vorlage von Postsendungen ein Informationsaustausch zwischen Postdienstleister und Zollbehörde verbunden.

Bei „zureichenden tatsächlichen Anhaltspunkten“ besteht für den Postdienstleister letztendlich sogar eine Pflicht zur Vorlage und damit zur Informationsverschaffung gegenüber der Zollbehörde.

Der Vorgang der Gestellung stellt einen zwingenden zollrechtlichen Vorgang dar und ist damit auch unzweifelhaft für die Erbringung des Postdienstes erforderlich. Folglich ist neben der gewollten Einschränkung von Art. 10 GG auch die Ausnahme von § 39 PostG einschlägig.

Die Informationsverschaffung der Zollbehörde geschieht damit auf ausdrücklichen Wunsch des Gesetzgebers. Eine Weitergabebefugnis von Informationen von der DPAG an den Zoll ist „kraft Sachzusammenhangs“ der Norm immanent.[623]

---

621 Friedrich in Schwarz/Wockenfoth, Zollrecht, § 5 ZollVG Rn. 2.

622 Friedrich in Schwarz/Wockenfoth, Zollrecht, § 5 ZollVG Rn. 6.

623 Der Begriff „kraft Sachzusammenhangs“ ist der Gesetzgebungsbefugnis des Bundes entliehen (siehe zum Beispiel Rozek in v. Mangoldt/Klein/Starck, GG, Bd. 2 Art. 70 Abs. I GG Rn. 44 ff.) und meint, dass eine Materie nur geregelt werden kann, wenn eine andere mitgeregelt wird. Auf diesen Fall angewendet bedeutet dies, das eine Vorlage nach § 5 ZollVG nur möglich ist, wenn die Norm eine Datenweitergabebefugnis enthält.

(a) § 5 ZollVG als Ermächtigungsgrundlage für eine Datenweitergabe zwecks Risikoanalyse

So ist des Weiteren fraglich, ob § 5 ZollVG auch eine aurseichende Ermächtigungsgrundlage für die DPAG zur Weitergabe von Daten an die Zollbehörden darstellt. Dies richtet sich nach § 4 Abs. 1 BDSG.

Zunächst stellt § 5 ZollVG eine taugliche Ermächtigungsgrundlage für eine Weitergabe – durch die Gestellung – notwendiger Informationen durch die DPAG an die Zollbehörde und damit verbunden Kenntniserlangung durch die Zollbehörde dar. Die Ermächtigung ist jedoch auf den Vorgang der Gestellung vom Wortlaut eindeutig begrenzt und das Postgeheimnis nur für diesen Vorgang eindeutig bewusst eingeschränkt.

Folglich bedarf es für eine anderweitige Nutzung der Daten durch die Zollbehörde einer weitergehenden Ermächtigung, die eindeutig dazu befugt, die Daten zum Zwecke einer Risikoanalyse zu erheben oder zu nutzen bzw. die Zweckbindung zu durchbrechen.

(b) Zwischenergebnis

§ 5 ZollVG stellt damit, isoliert betrachtet, keine ausreichende Ermächtigungsgrundlage für eine Datenweitergabe personenbezogener Daten durch die Post an die Zollbehörden zwecks Risikoanalyse zur allgemeinen Gefahrenabwehr dar.

dd) § 28 Abs. 1 BDSG

Des Weiteren könnten die Tatbestandsvarianten des § 28 Abs. 1 BDSG für eine Datenverarbeitung personenbezogener Daten durch Postdiensteanbieter zwecks Risikoanalyse in Frage kommen.

(1) Tatbestandsvoraussetzungen

Die allgemeinen Voraussetzungen sind wie für die Erhebung von Daten zu bewerten, ebenso der Anwendungsbereich des § 27 BDSG.[624]

[624] Siehe 4. Teil. C. II. 2.) a) ff).

Die Tatbestandsvarianten § 28 Abs. 1 Nr. 1 und Nr. 3 BDSG stellen keine ausreichende Ermächtigung für eine Datenverarbeitung zwecks Risikoanalyse dar.

In Betracht kommt eine Ermächtigung durch § 28 Abs. 1 Nr. 2 BDSG. Die Tatbestandsvoraussetzungen sind parallel zur Datenerhebung einzustufen.

(2) Subsumtion

Der Anwendungsbereich des § 27 BDSG ist eröffnet.[625]

Des Weiteren müssen die Datenverarbeitung, das Speichern wie auch das Weitergeben unter dem Tatbestand von § 28 Abs. 1 Nr. 2 BDSG zu subsumieren sein. Entsprechend der Zweckbindung müssen die Daten bereits mit der Absicht der Sicherung und/oder der Weitergabe erhoben worden sein. Deswegen kommt wohl die Datenverarbeitung des CN 23 Datensatzes nicht in Betracht, da dieser zu einem anderen Zweck erhoben wurde. Eine Datenverarbeitung von auf einem anderen Wege erhobenen Daten kommt dagegen grundsätzlich in Betracht.

Wie schon bei der Erhebung von Daten ist die Datenverarbeitung aus gleichen Gründen als interessensbezogen zu qualifizieren.[626]

Schließlich muss die Datenverarbeitung auch erforderlich sein. Eine Datenweitergabe wäre erforderlich, wenn die empfangende Stelle Teile der Risikoanalyse vornähme und dafür die Datensätze benötigen würde.

Ein zeitlich begrenztes Speichern von Daten kann für die Risikoanalyse für einen Abgleich mit „Altdaten“ – dies meint entsprechend bisher erhobene Daten eines Versenders oder Empfängers – notwendig sein, um Häufigkeiten und Unregelmäßigkeiten im Versand zu erkennen. Die Dauer der Speicherzeit richtet sich dabei nach dem notwendigen Minimum, um valide Ergebnisse im Datenabgleich zu bekommen. Der Mehrwert dieses Datenabgleichs muss dabei in einem angemessenem Verhältnis zur Dauer der Speicherung stehen.

---

625 Vgl. 4. Teil. C. II. 2.) a) ff) (5).

626 Vgl. 4. Teil. C. II. 2.) a) ff) (5).

(3) Zwischenergebnis

Folglich kommt § 28 Abs. 1 Nr. 2 BDSG als Ermächtigungsgrundlage für Postdienstleister zur zeitlich begrenzten Speicherung und Weitergabe von entsprechend zweckgebundenen personenbezogenen Daten in Frage.

ee) § 28 Abs. 2 BDSG

Weiterhin könnten die Tatbestandsvarianten des § 28 Abs. 2 BDSG Ermächtigungen für eine Datenverarbeitung personenbezogener Daten durch Postdienstleister für eine Risikoanalyse enthalten. Geregelt wird dabei die Zulässigkeit der Übermittlung, nicht des Speicherns.

(1) Tatbestandsvoraussetzungen

Die allgemeinen Tatbestandsvoraussetzungen sind zunächst so zu werten wie für die Datenerhebung, ebenso der Anwendungsbereich des § 27 BDSG.[627] Die Tatbestandsvariante § 28 Abs. 2 Nr. 3 BDSG kann von vornherein ausgeschlossen werden.

(2) Subsumtion

Der Anwendungsbereich des § 27 BDSG ist eröffnet.[628]

Bezüglich der Tatbestandsvarianten sind zunächst die gleichen Wertungen vorzunehmen wie für das Nutzen von Daten.[629] So kommt für die Weitergabe von Daten grundsätzlich § 28 Abs. 2 Nr. 1 i. V. m. § 28 Abs. 1 Nr. 2 BDSG in Betracht. Auch hier ist ein berechtigtes Interesse der DPAG an der Sicherheit der postalischen Lieferkette und damit an der Durchführung einer Risikoanalyse gegeben.

---

627 Siehe 4. Teil. C. II. 2.) a) ff).

628 Siehe 4. Teil. C. II. 2.) a) ff) (5).

629 Siehe 4. Teil. C. II. 2.) a) ff) (5) (a)–(c).

(3) Zwischenergebnis

Folglich ist eine Weitergabe personenbezogener Daten durch die Post an die Zollbehörden zum Zwecke der Risikoanalyse gemäß § 28 Abs. 2 Nr. 1 i. V. m. § 28 Abs. 1 Nr. 2 BDSG grundsätzlich zulässig.

ff) § 16 BDSG

Eine Ermächtigungsgrundlage zur Übermittlung personenbezogener Daten von den Zollbehörden an Postdienstleister könnte § 16 BDSG darstellen. Die Norm enthält zwei Tatbestände. Entweder ist die Übermittlung zur Aufgabenerfüllung der übermittelnden Stelle erforderlich oder der Empfänger kann glaubhaft ein Interesse an der Übermittlung geltend machen, ohne dass ein schutzwürdiges Interesse des Betroffenen besteht.

(1) Tatbestandsvoraussetzungen

In der ersten Tatbestandsvariante (§ 16 Abs. 1 Nr. 1 BDSG) sind zunächst die Zulässigkeitsvoraussetzungen nach § 14 BDSG für eine Nutzung personenbezogener Daten zu beachten. Weiterhin müssen die Daten zur Erfüllung der Aufgaben erforderlich sein. Auf die Interessenlage des Empfängers kommt es hierbei nicht an.[630]

In der zweiten Tatbestandsvariante (§ 16 Abs. 1 Nr. 2 BDSG) benötigt der Empfänger zunächst ein berechtigtes Interesse, das er glaubhaft darlegen muss. *„Berechtigt ist jedes ideelle und materielle Interesse, das auf sachlichen Erwägungen beruht und mit der Rechtsordnung im Einklang steht.“*[631] Ein unmittelbares, aber auch ein mittelbares Interesse des Betroffenen ist ausreichend.[632] Für eine glaubhafte Darlegung genügt ein schlüssiges Vorbringen, ein Beweis im eigentlichen Sinne muss nicht erbracht werden.[633] Schließlich darf der Betroffene kein

---

630 Gola/Schomerus, BDSG, § 16 BDSG, Rn. 6.

631 Gola/Schomerus, BDSG, § 16 BDSG, Rn. 10; Dammann in Simitis, BDSG, § 16 BDSG, Rn. 17.

632 Schaffland/Wiltfang, BDSG, § 16 BDSG, Rn. 13 f.

633 Im Ergebnis auch Gola/Schomerus, BDSG, § 16 BDSG, Rn. 10.

schutzwürdiges Interesse am Ausschluss der Übermittlung haben. Dies führt folglich zu einer Abwägung der Interessen des Empfängers und des Betroffenen. Das schutzwürdige Interesse des Betroffenen ist dabei weit zu verstehen.[634]

§ 16 Abs. 4 S. 1 BDSG legt für den Empfänger eine Bindung an den Übermittlungszweck fest.

(2) Subsumtion

Eine Kommunikation zwischen Zollbehörden und Postdienstleistern ist im Rahmen einer Risikoanalyse durchaus denkbar, auch wenn die Kommunikationsrichtung von Zoll zu Postdienstleistern unwahrscheinlich erscheint. Eine Ermächtigung dafür könnte in § 16 Abs. 1 Nr. 1 BDSG i. V. m. § 14 Abs. 2 Nr. 1 BDSG, Art. 46 Abs. 2 UZK liegen. Dafür müsste die Datenvweitergabe für die Risikoanalyse erforderlich sein.

(3) Zwischenergebnis

Eine Weitergabe von Zollbehörden an Postdienstleister für eine Risikoanalyse ist gemäß § 16 Abs. 2 Nr. 1 BDSG i. V. m. § 14 Abs. 2 Nr. 1 BDSG, Art. 46 Abs. 2 UZK nur denkbar, wenn sie für eine Risikoanalyse erforderlich wäre.

gg) Ermächtigungen aus der PDSV als Grundlage für eine Datenverarbeitung

Die in den §§ 3 und 5 PDSV enthaltenen Ermächtigungen für die Verarbeitung personenbezogener Daten scheiden als Ermächtigung für die Verarbeitung zwecks Risikoanalyse aus den gleichen Gründen aus wie für die Erhebung dieser Daten.[635]

Darüber hinaus regelt § 3 Abs. 3 S. 2 PDSV für die Weitergabe von Daten, dass diese unabhängig vom Speicherungsgrund nur mit Einwilligung der Beteiligten an Dritte übermittelt werden dürfen.

---

634 Dammann in Simitis, BDSG, § 16 Rn. 19.

635 Bergmann/Möhrle/Herb, Datenschutzrecht, § 28 Rn. 172 ff. sehen in der PDSV keine Rechtsgrundlage für das Speichern und Übermitteln von Daten; vgl. auch 4. Teil. C. II. 2.) a) bb)–ee).

Laut § 3 Abs. 4 dürfen mit der Erbringung von Postdiensten erhobene Daten nur für andere Zwecke verarbeitet oder genutzt werden, wenn eine Rechtsvorschrift dies für diese Daten ausdrücklich vorsieht oder der Beteiligte eingewilligt hat.

hh) § 29 Abs. 2 BDSG

Weiterhin kommt § 29 Abs. 2 BDSG als Ermächtigungsgrundlage für eine Übermittlung personenbezogener Daten durch Postdienstleister in Betracht. Der Anwendungsbereich des § 27 BDSG ist wie für die Erhebung von Daten gemäß § 28 Abs. 1 BDSG zu bestimmen.[636]

Der Rahmen und die Zweckbestimmung von § 29 Abs. 2 BDSG sind an die von § 29 Abs. 1 BDSG gebunden. Die Formulierung muss hier weit verstanden werden. Des Weiteren müsste in der Datenverwendung der Zweck als solcher vorliegen. Dies ist auch hier abzulehnen, womit § 29 Abs. 2 BDSG als Ermächtigungsgrundlage zur Übermittlung personenbezogener Daten nicht in Betracht kommt.[637]

ii) § 14 Abs. 1 BDSG

Eine Ermächtigungsgrundlage für eine Datenverarbeitung der Zollbehörden könnte weiterhin § 14 Abs. 1 BDSG darstellen. So ist das Speichern von Daten durch die Zollbehörde im Rahmen einer Risikoanalyse (wie auch schon für das Nutzen) über § 14 Abs. 1 BDSG denkbar.

jj) § 14 Abs. 2 BDSG

Des Weiteren kommen auch die Tatbestandsvarianten des § 14 Abs. 2 BDSG als Ermächtigung für die Verarbeitung personenbezogener Daten durch Zollbehörden in Betracht.

---

636 Siehe 4. Teil. C. II. 2.) a) ff) (2).

637 Vgl. 4. Teil. C. II. 2.) a) gg).

§ 14 Abs. 2 Nr. 6 BDSG kommt als Erlaubnistatbestand für ein Speichern personenbezogener Daten durch die Zollbehörden im Rahmen Risikoanalyse in Frage. Jedoch ist davon auszugehen, dass dieser gegenüber Art. 46 Abs. 2 UZK subsidiär zurücktritt.

kk) Art. 47 Abs. 2 UZK

Eine Ermächtigungsgrundlage für die Zusammenarbeit zwischen den Behörden stellt Art. 47 Abs. 2 UZK dar. Dieser besagt, dass im Rahmen der Kontrollen nach die Zollbehörden und andere zuständige Behörden untereinander und mit der Kommission die zur Risikominimierung und Betrugsbekämpfung erforderlichen Daten austauschen können, die sie über Eingang, Ausgang, Versand, Beförderung, Lagerung und Endverwendung – einschließlich des Postverkehrs – von zwischen dem Zollgebiet der Union und Ländern oder Gebieten außerhalb des Zollgebiets der Union beförderten Waren sowie über die im Zollgebiet der Union befindlichen Nicht-Unionswaren und Waren in der Endverwendung und deren Beförderung innerhalb des Zollgebiets und die Ergebnisse von Kontrollen erhalten haben.

ll) § 15 BDSG

Eine weitere Ermächtigungsgrundlage zur Datenweitergabe enthält § 15 BDSG. Dieser regelt die Übermittlung zwischen öffentlichen Stellen. Diese wäre folglich anzuwenden, bestünde die Notwendigkeit für die Zollbehörden, mit anderen öffentlichen Stellen Daten auszutauschen. Aus § 15 BDSG ergibt sich kein Rechtsanspruch auf Übermittlung.[638] Die Frage der Zulässigkeit ist spezialgesetzlich zu beantworten.[639]

(1) Tatbestandsvoraussetzungen

§ 15 Abs. 1 Nr. 2 BDSG verweist zunächst auf die Voraussetzungen für eine Nutzung personenbezogener Daten. Diese werden um die Zuständigkeit der

[638] Bergmann/Möhrle/Herb, Datenschutzrecht, § 15 Rn. 25.

[639] Im Ergebnis auch Bergmann/Möhrle/Herb, Datenschutzrecht, § 15 Rn. 25.

übermittelnden Stelle sowie die Erforderlichkeit für die Aufgabenerfüllung der empfangenden Stelle erweitert. In der ersten Variante ist die Übermittlung zur Aufgabenfüllung der übermittelnden Stelle notwendig.[640] Die Datenübermittlung ist erforderlich, wenn die Aufgabenerfüllung ohne die Daten unmöglich ist.[641]

In der zweiten Variante, wird die Übermittlung zur Aufgabenerfüllung der empfangenden Stelle – zum Beispiel im Wege der Amtshilfe – notwendig.[642] Hier ist jedoch zunächst der Vorrang der Datenerhebung beim Betroffenen gemäß § 4 Abs. 2 S. 1 BDSG zu berücksichtigen.[643] Erst danach sollten Daten von einem Dritten angefordert werden.

§ 15 Abs. 3 S. 1 BDSG legt für den Empfänger eine Bindung an den Übermittlungszweck fest. Der Übermittlungszweck ist weiterhin der Erhebungs- bzw. Speicherzweck.[644] Eine Nutzung zu anderen Zwecken ist gemäß § 15 Abs. 3 S. 2 BDSG nur unter den Bedingungen von § 14 Abs. 2 BDSG möglich.

(2) Subsumtion

Diese Konstellation kommt für den Informationsaustausch von Zollbehörden untereinander und mit weiteren Behörden in Betracht. Dafür müsste die empfangende Zollbehörde für die Risikoanalyse auf die weitergegebenen Daten angewiesen sein. Weiterhin müssten die Voraussetzungen für eine Nutzung personenbezogener Daten aus § 14 BDSG vorliegen. Gemäß § 14 Abs. 2 Nr. 1 BDSG Art. 46 Abs. 3 UZK in Betracht. Diese Normen setzen alle einen Informationsaustausch der Behörden zwingend voraus und benennen diesen auch.

---

640 Gola/Schomerus, BDSG, § 15 BDSG, Rn. 6.

641 Dammann in Simitis, BDSG, § 15 Rn. 11.

642 Gola/Schomerus, BDSG, § 15 BDSG, Rn. 7.

643 So auch Bergmann/Möhrle/Herb, Datenschutzrecht, § 15 Rn. 16.

644 Dammann in Simitis, BDSG, § 15 Rn. 34.

(3) Zwischenergebnis

Art. 15 BDSG kommt in Verbindung mit Art. 46 Abs. 3 UZK als Ermächtigung für den Informationsaustausch von Zollbehörden untereinander und mit anderen Behörden in Frage. Jedoch ist für den Informationsaustausch der Behörden zwecks Risikoanalyse Art. 47 Abs. 2 UZK die speziellere Ermächtigungsgrundlage

mm) Zwischenergebnis

Als Ermächtigungsgrundlage für eine Speicherung personenbezogener Daten durch Postdienstleister kommt zunächst § 28 Abs. 1 Nr. 2 BDSG in Betracht.

Für die Weitergabe personenbezogener Daten durch Postdienstleister kommt ebenfalls § 28 Abs. 1 Nr. 2 BDSG in Betracht. Des Weiteren kann für entsprechend zweckbestimmte Daten § 28 Abs. 2 Nr. 1 i. V. m. § 28 Abs. 1 Nr. 2 BDSG herangezogen werden.

§ 41 Abs. 2 PostG scheidet als Ermächtigungsgrundlage aus.

Als Ermächtigungsgrundlage für die Zollbehörden kommt als lex specialis Art. 47 Abs. 2 UZK in Betracht.

d) Verhältnis der Ermächtigungsgrundlagen zueinander

Das Verhältnis der einschlägigen Ermächtigungsgrundlagen zueinander ist zu untersuchen. Das BDSG regelt dabei sein eigenes Verhältnis zu spezielleren Gesetzen. Treffen bereichsspezifische Gesetze selbst Regelungen zu ihrem Verhältnis zu anderen Gesetzen im Allgemeinen oder zum BDSG im Speziellen, gehen diese Regelungen dem BDSG vor.[645] Im Verhältnis von Landesrecht zu Bundesrecht gilt Art. 31 GG. Hierzu trifft das BDSG keine spezielleren oder weitergehenden Aussagen.[646]

---

[645] Bergmann/Möhrle/Herb, Datenschutzrecht, § 1 Rn. 23 ff.

[646] So auch Schmidt in Taeger/Gabel, BDSG, § 1 BDSG, Rn. 24 ff.; Bergmann/Möhrle/Herb, Datenschutzrecht, § 1 BDSG, Rn. 24 f.; im Ergebnis auch Plath in Plath, BDSG, § 1 Rn. 35, 38; Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, § 1 Rn. 12.

So ist für das Erheben, das Verarbeiten und das Nutzen personenbezogener Daten durch Postdienstleister das Verhältnis von § 41 Abs. 2 PostG zu § 28 BDSG zu bestimmen.

Für das Erheben, das Verarbeiten und das Nutzen personenbezogener Daten durch die Zollbehörden ist das Verhältnis von BDSG und UZK zu bestimmen.

aa) § 1 Abs. 3 BDSG

Das BDSG regelt das Verhältnis zu anderen Rechtsvorschriften in § 1 BDSG. Durch die Zunahme bereichsspezifischer datenschutzrechtlicher Regelungen hat die Norm insgesamt an Bedeutung gewonnen.[647] Gemäß § 1 Abs. 3 BDSG gehen andere Rechtsvorschriften dem BDSG – soweit sie auf personenbezogene Daten anzuwenden sind – vor. Damit wird die Konkurrenz der Rechtsvorschriften auf Bundesebene zugunsten der spezielleren Normen im Sinne der Priorität gelöst.[648] Über die Reichweite der datenschutzrechtlichen Regelungen ist damit noch keine Aussage getroffen. Die vorrangigen Regelungen können den Datenschutz ausweiten wie auch verkürzen.[649]

Bei nebeneinander stehenden Ermächtigungsgrundlagen – also solchen, die in keinem Spezialitätsverhältnis zueinander stehen –, können mehrere Ermächtigungsgrundlagen parallel zur Anwendung kommen und die Datenverarbeitung legitimieren. Sofern nicht anderweitige Sicherheitsgründe, wie unterschiedliche Sicherheitsstufen, Zugänge etc. entgegenstehen, müssen Daten auch zu mehreren Zwecken parallel verarbeitet werden können. So können Ermächtigungen nach § 28 und § 29 BDSG gleichzeitig greifen.[650]

---

647 Dix in Simitis, BDSG, § 1 Rn. 159.

648 Dix in Simitis, BDSG, § 1 Rn. 158.

649 Schaffland/Wiltfang, BDSG, § 1 Rn. 37.

650 Taeger in Taeger/Gabel, BDSG, § 28 Rn. 34.

(1) Anwendbarkeit der Subsidiaritätsklausel

Für eine Anwendbarkeit von § 1 Abs. 3 BDSG muss zunächst generell das BDSG einschlägig sein.[651] Unter den Begriff der Rechtsvorschriften des Bundes fallen alle formellen Gesetze.[652] Dazu zählen alle Bundesgesetze, Rechtsverordnungen, Satzungen bundesunmittelbarer Körperschaften, Anstalten und Stiftungen, durch ein Zustimmungsgesetz inkorporierte Staatsverträge sowie alle aufgrund von EG-Richtlinien verabschiedeten Gesetze.[653] Zu beachten ist jedoch die Wesentlichkeitstheorie des Bundesverfassungsgerichts.[654] Damit muss der Gesetzgeber bei jeder Regelung, die er trifft, die personenbezogene Daten tangiert, die Notwendigkeit der Regelung in diesem Gesetz mitbedenken.[655] Hierfür reicht jedoch zumindest ein mittelbar datenschützender Charakter der verdrängenden Norm aus.[656]

(2) Kollision nach § 1 Abs. 3 BDSG

Mit der Formulierung „soweit" in § 1 Abs. 3 BDSG wird der Umfang der Subsidiarität festgelegt.[657] Damit eine Kollision vorliegt, müssen die kollidierenden Vorschriften exakt den gleichen Sachverhalt regeln und damit deckungsgleich sein.[658] Bei nicht vollständiger Tatbestandskongruenz sind zwei Konstellationen denkbar. Ist der Regelungsgehalt der betreffenden Norm des BDSG in der spezielleren Norm enthalten, tritt die Norm des BDSG zurück.[659] Regelt die betreffen-

---

651 Dix in Simitis, BDSG, § 1 Rn. 162.

652 Dix in Simitis, BDSG, § 1 Rn. 164.

653 Weichert in Däubler/Klebe/Wedde/Weichert, BDSG, § 1 BDSG, Rn. 12; Dix in Simitis, BDSG, § 1 Rn. 164 f.

654 Zur Wesentlichkeitstheorie siehe auch Epping in Epping/Hillgruber, GG, Art. 87a Rn. 24.

655 Dix in Simitis, BDSG, § 1 Rn. 165; vgl. Rogall, Der Informationsbegriff und Gesetzesvorbehalt im Strafprozessrecht, S. 53 ff.

656 Schaffland/Wiltfang, BDSG, § 1 Rn. 42.

657 Gola/Schomerus, BDSG, § 1 Rn. 24; Dix in Simitis, BDSG, § 1 BDSG, Rn. 170.

658 So auch Schmidt in Taeger/Gabel, BDSG, § 1 Rn. 33 f.; für eine breitere Verdrängung Schaffland/Wiltfang, BDSG, § 1 Rn. 42; Gola/Schomerus in Gola/Schomerus, BDSG, § 1 Rn. 24.

659 Schmidt in Taeger/Gabel, BDSG, § 1 Rn. 33.

de Norm des BDSG Sachverhalte, die im spezielleren Gesetz nicht geregelt sind, oder trifft es weitergehende Regelungen, bleibt das BDSG für diese Konstellation anwendbar.[660] So sah z. B. der BGH das NRWDSG gegenüber Notaren nicht zurücktreten und den § 18 I BNotO nicht den gesamten datenschutzrechtlichen Bereich verdrängen.[661]

Dafür muss das das BDSG verdrängende Gesetz zunächst selbst verfassungskonform sein.[662] Rechtsvorschriften, die allgemein den Vorrang eines bestimmten Gesetzes statuieren, genügen daher nicht.[663]

(3) Subsumtion

Fraglich erscheint daher, in welchem Verhältnis die Regelungen des PostG, des UZK und des BDSG zueinander stehen.

(a) Verhältnis von Postrecht und BDSG

So sind für die einzelnen Verarbeitungsschritte und Phasen die einschlägigen Normen des BDSG und des Postrechts zueinander in Beziehung zu setzen und zu bestimmen, ob und wie weit die Regelungen des PostG und der PDSV vorangehen und das BDSG sperren.

Zunächst ist dahingehend die Phase der Erhebung zu untersuchen. Dafür ist zunächst der Tatbestand der beiden Normen vergleichend zu hinterfragen. § 41 Abs. 2 PostG wie auch § 28 Abs. 1 BDSG regeln beide die Erhebung personenbezogener Daten. § 41 Abs. 2 PostG regelt die Verwendung von Daten für die betriebliche Abwicklung im Rahmen der geschäftsmäßigen Erbringung von Postdienstleistungen. § 28 Abs. 1 BDSG regelt die Verwendung personenbezogener Daten zur Erfüllung eigener Geschäftszwecke. Hier müsste zunächst

---

660 Bergmann/Möhrle/Herb, Datenschutzrecht, § 1 BDSG, Rn. 24; Schmidt in Taeger/Gabel, BDSG, § 1 Rn. 33; Gola/Schomerus, BDSG, § 1 Rn. 24; im Ergebnis wohl auch Schaffland/Wiltfang, BDSG, § 1 Rn. 42.

661 NJW 1991, S. 568 f. BGH Beschluss v. 30.07.1990 – NotZ.

662 Zu den Konsequenzen und dem Umgang mit verfassungswidrigen Normen siehe Dix in Simitis, BDSG, § 1 Rn. 171.

663 Simitis in Simitis, BDSG, § 28 Rn.15.

Tatbestandskongruenz vorliegen. Wortgleiche Formulierungen liegen nicht vor. Diese können jedoch nicht gefordert sein, sonst liefe die Subsidiaritätsregelung letztendlich immer ins Leere. Abzustellen ist vielmehr auf den materiellen Regelungsgehalt der Norm. Beide Tatbestände stellen auf die Erhebung von Daten im Rahmen und zur Erfüllung eigener Geschäftszwecke ab. Während das BDSG dies allgemein formuliert, gilt die Regelung im PostG für den postalischen Bereich. Beide Normen regeln damit den gleichen Vorgang mit derselben Intention. Hinzu kommt, dass der Gesetzgeber die Datenverwendungsmöglichkeiten mit § 41 PostG abschließend regeln wollte.

Folglich ist davon auszugehen, dass § 41 Abs. 2 PostG § 28 Abs. 1 BDSG als Ermächtigungsgrundlage für die Erhebung personenbezogener Daten im postalischen Bereich sperrt.[664]

Weiterhin ist ebenfalls das Verhältnis von § 41 Abs. 2 PostG zu § 28 Abs. 1 BDSG sowie § 28 Abs. 2 BDSG vergleichend bezüglich der Nutzung personenbezogener Daten zu untersuchen.

Für die Nutzung ist im Verhältnis von § 41 Abs. 2 PostG zu § 28 Abs. 1 BDSG die gleiche Wertung zu ziehen wie für die Erhebung. § 28 Abs. 2 BDSG stellt hingegen eine bewusste Durchbrechung der Zweckbindung dar und weicht von den Tatbestandsvoraussetzungen und der Zielsetzung von § 28 Abs. 1 BDSG ab. Es liegt folglich keine Tatbestandskongruenz zu § 41 Abs. 2 PostG vor.

Fraglich erscheint jedoch, ob im Bezug auf § 28 Abs. 1 BDSG auch § 28 Abs. 2 von dessen Subsidiarität mitumfasst sein könnte. Die spezielleren Regelungen des PostG – die die Datenverarbeitungstatbestände für den postalischen Bereich abschließend regeln wollen – liefen leer, würde man die Zweckänderungstatbestände von § 28 Abs. 2 BDSG auf § 41 PostG anwenden.

Folglich ist davon auszugehen, dass auch für die Nutzung personenbezogener Daten § 41 PostG den § 28 BDSG sperrt.

664 Im Ergebnis, wohl auch im Allgemeinen Wronka, Datenschutzrechtliche Aspekte beim Postversand in RDV 2011, S. 122.

Weiterhin ist das Verhältnis von § 41 Abs. 2 PostG zu § 28 Abs. 1 BDSG und § 28 Abs. 2 BDSG bezüglich der Verarbeitung personenbezogener Daten vergleichend zu bestimmen.

Für das Verhältnis von § 41 Abs. 2 PostG zu § 28 Abs. 1 BDSG sind bezüglich des Speicherns und der Weitergabe personenbezogener Daten die gleichen Wertungen zu treffen, wie bezüglich der Erhebung personenbezogener Daten. Im Verhältnis von § 41 Abs. 2 PostG zu § 28 Abs. 2 BDSG wird man auch hier eine Zweckänderung gegenüber § 41 Abs. 2 PostG ablehnen müssen.

(b) Verhältnis von Zollrecht und BDSG

Für die Datenverarbeitung durch die Zollbehörden ist das Verhältnis von Zollrecht und BDSG zueinander zu bestimmen.

Art. 46 Abs. 2 UZK als Ermächtigungsgrundlage für die Verwendung von Daten zwecks Risikoanalyse unterscheidet nicht nach dem Phasenmodell des BDSG. Allein dadurch unterscheiden sich schon die Tatbestandsformulierungen der §§ 13–15 BDSG von Art. 46 Abs. 2 UZK.

Jedoch sollen die Regelungen ebenfalls gegenüber spezialgesetzlichen Regelungen subsidiär zurücktreten. § 15 Abs. 1 BDSG entfaltet insoweit eine eigene Wirkung, als es zusammen mit Art. 46 Abs. 2 UZK gelesen wird und den datenschützenden Charakter ergänzt.

bb) Zwischenergebnis

Als Ermächtigungsgrundlage für die Erhebung, die Verarbeitung und die Nutzung personenbezogener Daten durch Postdienstleister zwecks Risikoanalyse wird § 28 Abs. 1 BDSG durch § 41 Abs. 2 PostG gesperrt.

Eine Verwendung personenbezogener Daten durch die Zollbehörden zwecks Risikonanalyse richtet sich hingegen nach Art. 46 Abs. 2 UZK. Die Erlaubnistatbestände des BDSG werden insoweit verdrängt.

Eine Verwendung personenbezogener Daten durch die DPAG zwecks Risikoanalyse ist durch keinen Erlaubnistatbestand gedeckt.

III. Möglichkeiten für eine weitergehende Ermächtigung

Weiterhin ist zu untersuchen, wie weitergehende bzw. präzisere Erlaubnistatbestände im Bezug auf eine Risikoanalyse zwecks allgemeiner Gefahrenabwehr durch die DPAG aussehen könnten. In Betracht kommen Formen der Beleihung oder eines „allgemeinen" Erlaubnistatbestandes.

1. Ausgangslage

Wenn auch die Ermächtigungsgrundlagen besonders des BDSG zwar auch die automatisierte Datenverarbeitung regeln, so ist der Gesetzgeber grundsätzlich an vielen Stellen noch von einer „manuellen" Datenverarbeitung im Sinne eines einzelnen Abrufens und Beantragens von Daten ausgegangen. Der „intelligente" Datenaustausch im Sinne eines selbständigen Informationsaustausches von miteinander vernetzten Systemen und Programmen lag den Vorstellungen des Gesetzgebers nicht zugrunde. Dies führt zu Anpassungsschwierigkeiten der gesetzlichen Normen an die „EDV-Realität" und die Möglichkeiten moderner Massendatenverarbeitung.

Die Ausgestaltung der gesetzlichen Ermächtigungsgrundlagen durch den Gesetzgeber machen deutlich, dass, auch wenn sie möglicherweise im Einzelnen die Datenverarbeitung zulassen, die Datenverarbeitung zwecks Risikoanalyse nicht im Fokus der Regelungen stand. Die Gefahren, denen Postdiensteanbieter ausgesetzt sind und denen sie begegnen müssen, und die Möglichkeiten, die ihnen dafür zur Verfügung stehen, wurden letztendlich gesetzlich nicht geregelt bzw. nicht mitbedacht. Das Ergebnis ist eine Gesetzeslage, die den Gefahren und Herausforderungen des modernen Postverkehrs wie auch dem Schutz von personenbezogenen Daten und Unternehmensdaten nicht mehr gerecht wird.

Die Sicherung der Lieferkette unter Berücksichtigung der Erfordernisse eines modernen Datenschutzes erfordert deswegen eindeutige Regelungen.

2. Beleihung

Zu untersuchen ist weiterhin, ob und inwieweit die DPAG mit einer Risikoanalyse zwecks allgemeiner Gefahrenabwehr beliehen werden könnte.

a) Grundlagen

Die Beleihung ist zunächst ein Institut, bei dem hoheitliche Befugnisse Personen des Privatrechts übertragen werden.[665] In der Folge können Private im eigenen Namen gegenüber Dritten in öffentlich-rechtlichen Formen handeln.[666] Bis heute ist das Institut nicht eindeutig bestimmt. In der Lehre stehen sich die Aufgabentheorie und die Befugnis- oder Rechtsstellungstheorie gegenüber. Die Aufgabentheorie stellt auf die Erfüllung öffentlicher Aufgaben ab.[667] Die Befugnistheorie hingegen richtet sich nach der Verleihung typisch staatlicher Machtbefugnisse.[668] Die Beleihung der DPAG erfüllt beide Theorien. Eine Risikoanalyse zwecks allgemeiner Gefahrenabwehr stellt die Erfüllung einer öffentlichen Aufgabe wie auch eine typisch staatliches Machtbefugnis dar.

---

665 Ähnlich Battis, Beleihung anlässlich der Privatisierung der Postunternehmen in FS Peter Raisch zum 70. Geburtstag 1995, S. 355 (356).

666 Battis, Beleihung anlässlich der Privatisierung der Postunternehmen in FS Peter Raisch zum 70. Geburtstag 1995, S. 355 (356); Krebs in Isensee/Kirchhof, Handbuch des Staatsrechts, Bd. III, § 69 Rn. 39.

667 Battis, Beleihung anlässlich der Privatisierung der Postunternehmen in FS Peter Raisch zum 70. Geburtstag 1995, S. 355 (357); Benz, Die verfassungsrechtliche Zulässigkeit der Beleihung einer Aktiengesellschaft mit Dienstherrenbefugnissen, Dissertation, Tübingen 1995, S. 28 f.; Steiner, Der beliehene Unternehmer in JuS 1969, S. 69 (70).

668 Battis, Beleihung anlässlich der Privatisierung der Postunternehmen in FS Peter Raisch zum 70. Geburtstag 1995, S. 355 (357); Benz, Die verfassungsrechtliche Zulässigkeit der Beleihung einer Aktiengesellschaft mit Dienstherrenbefugnissen, Dissertation, Tübingen 1995, S. 29 f.; Kirchhof, Verwalten durch „mittelbares“ Einwirken, 1977, S. 11.

b) Voraussetzungen einer Beleihung

Zunächst bedarf es für eine Beleihung – als Ausfluss des Demokratieprinzips – einer gesetzlichen Ermächtigung.[669] Der Kreis der übertragbaren Aufgaben ist grundsätzlich nicht eingeschränkt.[670] Jedoch darf der Gesetzgeber sich nicht unbegrenzt des Instruments der Privatisierung der Bundesverwaltung bedienen. Es muss sich vielmehr um abgrenzbare Teilbereiche handeln; der Kernbereich der Verwaltungsmaterie muss bei den Behörden bleiben und eine Anbindung an den Staat muss gewährleistet sein.[671] Der Adressatenkreis einer Beleihung ist nicht begrenzt, sodass jede juristische Person des Privatrechts in Betracht kommt.[672] Schließlich bedarf der beliehene Vorgang einer staatlichen Aufsicht.[673]

c) Anwendung auf die DPAG

Eine Beleihung der DPAG mit der Kompetenz, Risikoanalysen zwecks allgemeiner Gefahrenabwehr durchzuführen, bedürfte zunächst eines Gesetzes. Dieses müsste Anforderungen an die formelle und materielle Verfassungsmäßigkeit genügen. Für die formelle Verfassungsmäßigkeit müssten die Zuständigkeit, das Verfahren und die Form eingehalten werden. Die Zuständigkeit des Bundes richtet sich nach Art. 70, 73 Abs. 1 Nr. 5, 7 GG sowie Art. 83, 86 GG.

Weiterhin stellt sich die Frage, inwieweit die Gefahrenabwehr als staatliche Hoheitsaufgabe einen Kernbereich staatlichen Handelns darstellt und privatisierbar ist. Als Kern der Gefahrenabwehr wird *„das Einschreiten mit Befehl und Zwang zum Schutz*

669 Battis, Beleihung anlässlich der Privatisierung der Postunternehmen in FS Peter Raisch zum 70. Geburtstag 1995, S. 355 (362); Benz, Die verfassungsrechtliche Zulässigkeit der Beleihung einer Aktiengesellschaft mit Dienstherrenbefugnissen, Dissertation Tübingen 1995, S. 39 f.; BVerwG, DÖV 1984, 1025; DVBL 1970, S. 735 (736).

670 Battis, Beleihung anlässlich der Privatisierung der Postunternehmen in FS Peter Raisch zum 70. Geburtstag 1995, S. 355 (359).

671 Pieroth in Jarass/Pieroth, GG, Art. 87 Rn. 16.

672 Battis, Beleihung anlässlich der Privatisierung der Postunternehmen in FS Peter Raisch zum 70. Geburtstag 1995, S. 355 (361); Steiner, Der beliehene Unternehmer in, JuS 1969, S. 69 (71).

673 Battis, Beleihung anlässlich der Privatisierung der Postunternehmen in FS Peter Raisch zum 70. Geburtstag 1995, S. 355 (362).

von Bürgern oder staatlichen Einrichtungen angesehen.“[674] Das Recht kennt grundsätzlich die Beleihung Privater mit Aufgaben der Gefahrenabwehr.[675] Zum „Kernbereich der Staatsgewalt“ wird jedoch jenes Verwaltungshandeln gezählt, das unmittelbarer Bestandteil des staatlichen Gewaltmonopols ist.[676] Die Risikoanalyse ist diesem Vorgehen grundsätzlich vorgelagert und dient der Identifizierung des Risikos. Es ist daher wohl präziser, von Gefahrenvorsorge als Unterfall der Gefahrenabwehr zu sprechen.[677] Es handelt sich damit um einen klar eingrenzbaren Vorgang innerhalb der staatlichen Gefahrenabwehr. Begrenzt man den Vorgang auf die reine Datenverarbeitung, müssen keine hoheitlichen Handlungsbefugnisse verliehen werden.

Die DPAG ist als Aktiengesellschaft potenziell beleihungsfähig.[678] Staatliche Kontrollmechanismen wären weiterhin entsprechend zu schaffen.

d) Verhältnis der Beleihung zu Art. 46 Abs. 2 UZK

Fraglich erscheint, in welchem Verhältnis eine Beleihung zu Art. 46 Abs. 2 UZK stünde. Die Norm spricht von Zollbehörden im Zusammenhang mit Zollkontrollen, die wiederum auf eine Risikoanalyse gestützt werden. Eine eindeutige Zuweisung, die Risikoanalyse müsse von den Zollbehörden vollzogen werden, enthält die Norm nicht. Weitere Regulierungen zur Verwaltungsstruktur werden nicht getroffen. Der Aufbau der Zollverwaltung wird national im ZollVG geregelt und ist nationale Zuständigkeit.[679]

Art. 46 Abs. 2 UZK steht einer Beleihung somit nicht im Wege.

---

674 Bracher, Gefahrenabwehr durch Private, Berlin 1987, S. 26; Drews/Wacke/Martens, Gefahrenabwehr Bd. 2, S. 34; Friauf in v. Münch, Besonderes Verwaltungsrecht, S. 186.

675 Etwa beim Schiffskapitän nach § 106 SeemG, dem Flugzeugführer nach § 29 Abs. 3 LuftVG, sowie Jagsaufsehern etc.; ausführlich bei Bracher, Gefahrenabwehr durch Private, Berlin 1987, S. 27 ff.

676 Bracher, Gefahrenabwehr durch Private, Berlin 1987, S. 79; Ossenbühl, Eigensicherung und hoheitliche Gefahrenabwehr, S. 42.

677 So auch Bracher, Gefahrenabwehr durch Private, Berlin 1987, S. 44 f.; vgl auch Ossenbühl, Vorsorge als Rechtsprinzip im Gesundheits-, Arbeits- und Umweltschutz, NVwZ 1986, S. 161 ff.

678 So auch Benz, Die verfassungsrechtliche Zulässigkeit der Beleihung einer Aktiengesellschaft mit Dienstherrenbefugnissen, Dissertation Tübingen 1995, S. 81.

679 Witte, Zollkodex, Art. 4 Nr. 3.

e) Zwischenergebnis

Der Bundesgesetzgeber wäre ermächtigt, die DPAG mit der Risikoanalyse zwecks allgemeiner Gefahrenabwehr zu beleihen.

3. Ermächtigungsgrundlage für eine Risikoanalyse zwecks allgemeiner Gefahrenabwehr durch die DPAG

Ausgehend von der Annahme, dass für Postdiensteanbieter keine Ermächtigungsgrundlagen zur Verarbeitung von Daten zwecks Risikoanalyse vorliegen, sollen im Weiteren Möglichkeiten einer solchen gesetzlichen Ermächtigung aufgezeigt werden.

Die Regelung von Tatbeständen, die die öffentliche Sicherheit und Ordnung, die Gefahrenabwehr oder den Schutz oder die Verfolgung von Straftaten betreffen, wird in Gesetzen grundsätzlich speziell realisiert. Auch die Postgesetze oder Gesetzesentwürfe enthielten im Bezug auf diese Tatbestände teilweise Regelungen, die in die verabschiedeten Fassungen der Gesetze nicht übernommen oder bei Gesetzesnovellierungen im Laufe der Neuorganisation und Reform der gesamten Wirtschafts- und Rechtsgebiete nicht in die neuen Fassungen übernommen wurden.

Ihre grundsätzliche Existenz deutet jedoch darauf hin, dass der Gesetzgeber von einer gesonderten Notwendigkeit der Regulierung dieser Tatbestände ausgeht und diese deswegen von den allgemeinen Datenverwendungstatbeständen nicht umfasst werden.

Da es sich hierbei um eine Regelung im Bereich des Postwesens handelt, bedürfte es einer spezialgesetzlichen Regelung im Postgesetz. Um Postdiensteanbietern eine Risikoanalyse zur allgemeinen Gefahrenabwehr zu ermöglichen, wären Änderungen bzw. Ergänzungen der §§ 39 und 41 PostG notwendig oder das Einfügen einer gesonderten Norm, die speziell diesen Sachverhalt regelt.

a) Änderung des § 39 PostG

§ 39 PostG schützt im Zusammenhang mit dem Postverkehr stehende Daten und erlaubt ihre Verwendung nur in einem sehr engen Rahmen. Eine Ausnahme zur Zweckänderung gilt lediglich gemäß § 39 Abs. 4 Nr. 4 PostG für die Abwendung körperlicher Gefahren. Dieser Ausnahmetatbestand ist auf die allgemeine Gefahrenabwehr nicht anwendbar.[680] Folglich müsste der Ausnahmenkatalog um die allgemeine Gefahrenabwehr ergänzt werden. § 39 Abs. 4 Nr. 5 könnte wie folgt aussehen: („Die Verbote des Absatzes 3 gelten nicht, soweit die dort bezeichneten Handlungen erforderlich sind, um") „erhebliche Gefahren für die öffentliche Sicherheit abzuwenden".

Eine Risikoanalyse dient der Gefahrenabwehr und ist auch dazu geeignet, „risikoreiche" Postsendungen innerhalb des allgemeinen Sendungsstroms zu erkennen.

Damit wäre eine Verwendung von Sachdaten durch Postdiensteanbieter zwecks allgemeiner Gefahrenabwehr möglich.

b) Änderung des § 41 PostG

Eine Verwendung personenbezogener Daten bedürfte weiterhin einer Ergänzung von § 41 PostG. Anders als § 14 BDSG enthält dieser keine Ermächtigungsgrundlage zur Abwehr von Gefahren für die öffentliche Sicherheit. § 41 Abs. 2 Nr. 5 PostG könnte gemäß dem Gefahrenabwehrtatbestand des BDSG wie folgt lauten: („Nach Maßgabe der in Abs. 1 genannten Rechtsverordnung dürfen Unternehmen und Personen, die geschäftsmäßig Postdienste erbringen oder an der Erbringung solcher Dienste mitwirken, die Daten natürlicher und juristischer Personen erheben, verarbeiten und nutzen, soweit dies zur betrieblichen Abwicklung von geschäftsmäßigen Postdiensten erforderlich ist, nämlich für") „das Abwehren erheblicher Nachteile oder Gefahren für das Gemeinwohl oder die öffentliche Sicherheit".

680 Siehe 2. Teil. B. IV. 1.) a).

c) „Eigener" Erlaubnistatbestand § 41a PostG

Schließlich könnte eine eigene Regelung ausschließlich die Risikoanalyse durch Postdiensteanbieter regeln. Ein § 41a PostG, könnte wie folgt aussehen:

„Das Erheben, Verarbeiten und Nutzen von Daten natürlicher oder juristischer Personen sowie des Inhaltes von Postsendungen durch Unternehmen, die geschäftsmäßig Postdienste erbringen, ist zulässig zur Durchführung einer Risikoanalyse, um erhebliche Gefahren für das Gemeinwohl, die öffentliche Sicherheit oder die postalische Lieferkette abzuwehren, sofern das Interesse der Betroffenen nicht überwiegt und der Zweck nicht auf andere Weise oder nur mit unverhältnismäßigen Aufwand erreicht werden kann.

Das Erheben, Verarbeiten und Nutzen von Daten zu diesem Zweck hat unter Beachtung der allgemeinen Grundsätze, insbesondere der Datensparsamkeit und Datenvermeidung, zu erfolgen.

Das Brief- und Postgeheimnis nach Art. 10 des Grundgesetzes wird zu diesem Zweck eingeschränkt. Eine Informationspflicht gegenüber dem Betroffenen besteht nicht. Eine unabhängige Kontrolle findet statt".[681]

Eine solche Formulierung hat den Vorteil, dass sie Forderungen nach Normenklarheit und Normenbestimmtheit nachkommt.[682] Das Zitiergebot von Art. 10 GG wird eingehalten. Weiterhin wird der Anwendungsbereich der Regelung zur Gefahrenabwehr klar auf eine Risikoanalyse begrenzt und mit Anforderungen an die Datenverarbeitungsgrundsätze und allgemeine Rechtsgrundsätze, wie das Verhältnismäßigkeitsprinzip und eine Abwägung mit den Schutzgütern der Betroffenen, verknüpft.[683] Damit ginge eine solche Regelung über die Formulierungen polizeilicher Generalklauseln hinaus, bei denen von einer Rechtskonformität ausgegangen wird („*In jahrzehntelanger Entwicklung durch die Rechtsprechung und Lehre nach Inhalt, Zweck und Ausmaß hinreichend präzisiert, in ihrer*

---

[681] Weitere Regelungen zu einer Kontrollinstanz müssten entsprechend folgen, stehen jedoch nicht im Fokus dieser Arbeit.

[682] BVerfG Beschluss v. 03.03.2004 – 1 BvF 3/92 in NJW 2004, S. 2216.

[683] BVerfG Beschluss v. 03.03.2004 – 1 BvF 3/92 in NJW 2004, S. 2220.

Bedeutung geklärt und im juristischen Sprachgebrauch verfestigt“).[684] So kann man bei „polizeilichen Generalklauseln“ davon ausgehen, dass diese den Anforderungen an die Zweckbindung genügen.[685]

§ 41a PostG müsste weiterhin formell verfassungsgemäß sein. Dafür müssten die Zuständigkeit, das Verfahren und die Form eingehalten werden. Zuständig für den Erlass einer solchen Norm ist der Bundesgesetzgeber gemäß Art. 70, 73 Abs. 1 Nr. 7 GG.

4. Zwischenergebnis

Es gibt verschiedene Ansätze, einen Erlaubnistatbestand für die Gefahrenabwehr durch die Post zu formulieren und dadurch die Risikoanalyse durch die Post zu ermöglichen. Gemeinsam haben alle, dass sie einen Aspekt der allgemeinen Gefahrenabwehr innerhalb der postalischen Lieferkette an einen Privaten (hier die DPAG) übertragen und damit die Verwendung von Daten auf diesem Gebiet zulassen.[686]

---

[684] BVerfG –Vorprüfungsausschuss-, Beschluss, v. 23.05.1980, BVerfGE 54, S. 143, 144 f.

[685] Schaffland/Wiltfang, BDSG, § 14 Rn. 20.

[686] Aufgrund der Ähnlichkeit des materiellen Gehalts wird, um Überschneidungen und Wiederholungen zu vermeiden, § 41a PostG stellvertretend für die verschiedenen möglichen Erlaubnistatbestände und die Beleihung untersucht.

D. Vereinbarkeit mit höherrangigem Recht

Die erarbeiteten Ergebnisse müssen mit höherrangigem Recht vereinbar sein. So ist zu untersuchen, ob eine Regelung zur Verwendung von Daten zwecks Risikoanalyse durch Postdiensteanbieter nicht gegen höherrangiges Recht verstieße. Dafür ist entscheidend, dass sie im Einklang mit den Grundrechten auf nationaler und europäischer Ebene stehen muss.

Zu diesem Zweck sind die verschiedenen Grundrechtssysteme in Europa herauszuarbeiten und ihr Verhältnis zueinander zu bestimmen. An diesem erarbeiteten Grundrechtsrahmen und dem daraus resultierendem Gewährleistungsumfang, sind die Maßnahmen zu messen.

I. Der Grundrechtsschutz in Europa

Neben der Ausübung hoheitlicher Gewalt durch die Nationalstaaten und dem hier angesiedelten Grundrechtsschutz hat die Ausübung autonomer hoheitlicher Gewalt durch die Institutionen der Europäischen Union auch auf dieser Ebene einen Schutz der Bürger vor diesen Akten notwendig gemacht.[687] Voraussetzung dafür ist eine Verbriefung von Grundrechten, ohne die auch eine Übertragung von Hoheitsgewalt auf Organe der Union nach deutschem nationalen Recht nicht möglich gewesen wäre.[688]

Der Grundrechtsschutz in Europa besteht grundsätzlich in einer Trias aus der Europäischen Menschenrechtskonvention, der Charta der Grundrechte der Europäischen Union sowie dem nationalen Grundrechtsschutz, in Deutschland durch das Grundgesetz garantiert. Hinzu kommen auf Ebene der EU die in den allgemeinen Grundsätzen herausgearbeiteten gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten.

---

687 Nicolaysen, Die gemeinschaftsrechtliche Begründung von Grundrechten in EuR 2003, S. 719 f.

688 Dazu siehe Ausführungen zu Art. 23 GG; in 4. Teil. D. II. 1.) a).

Es gilt herauszuarbeiten, in welchem Verhältnis die Grundrechtsschutzregime zueinander stehen und wie weit ihr Schutz jeweils reicht.

1. Historische Einordnung

Die Anfangsphase nach dem Zweiten Weltkrieg war geprägt von der Entstehung und Entwicklung des nationalen Grundrechtssystems.[689] Auch wenn die Bundesrepublik bereits 1952 die EMRK ratifiziert und sich damit dem Grundrechtsregime der EMRK unterworfen hatte, wurde der EGMR noch selten angerufen, und der Grundrechtschutz durch die EMRK war durch die Rechtsprechung noch nicht in dem Maße entwickelt und stand deswegen noch nicht so im Fokus der Betrachtungen.[690] Die entstehenden Europäischen Gemeinschaften hatten noch keinen Grundrechtskatalog, zumal die Kompetenzen auf Gemeinschaftsebene noch nicht stark ausgeprägt waren. Bewegung kam in das Gemeinschaftsrecht mit den Entscheidungen des EuGH die Verträge dynamisch zu interpretieren, und der Statuierung des Vorrangs des Gemeinschaftsrechts vor den nationalen Rechtsebenen, den Grundrechten eingeschlossen.[691]

Mit der Errichtung des gemeinsamen Binnenmarktes bekam die EG mehr Kompetenzen und der EuGH arbeitete auf der Basis der gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten einen gemeinsamen Grundrechtsschutz heraus. Das Bundesverfassungsgericht hat mit seiner „Solange“ Rechtsprechung diese Entwicklung mitausgelöst und eine Position zum Verhältnis der Grundrechtsregime entwickelt.

---

689 Schmahl, Grundrechtsschutz im Dreieck von EU, EMRK und nationalem Verfassungsrecht in EuR 2008 Heft Beiheft 1, S. 7, 8.

690 Schmahl, Grundrechtsschutz im Dreieck von EU, EMRK und nationalem Verfassungsrecht in EuR 2008 Heft Beiheft 1, S. 7, 9.

691 Schmahl, Grundrechtsschutz im Dreieck von EU, EMRK und nationalem Verfassungsrecht in EuR 2008 Heft Beiheft 1, S. 7, 9.

2. Die Europäische Menschenrechtskonvention

Die Konvention zum Schutze der Menschenrechte und Grundfreiheiten wurde im Rahmen des Europarates ausgearbeitet, am 04.11.1950 in Rom unterzeichnet und trat am 03.09.1953 in Kraft. Sie stellt die erste Konvention dieser Art weltweit dar.[692]

Der Europäische Gerichtshof für Menschenrechte sieht in der Konvention ein „lebendes Instrument", das sich im Sinne einer dynamischen Auslegung den Lebensbedingungen anpassen muss.[693]

Über den eigentlichen Konventionstext hinaus gehören zum Gewährleistungsumfang Zusatzprotokolle, die jedoch nur für die Staaten verbindlich sind, die diese ratifiziert haben.[694]

3. Die Grundrechtecharta der Europäischen Union

Die Charta der Grundrechte der Europäischen Union wurde am 07.12.2000 vom Rat und der Kommission proklamiert. Vorangegangen waren 2 Jahre Arbeit des sogenannten Konvents, der aus Vertretern der Regierungen und Parlamente der Mitgliedstaaten und Vertretern der Kommission und des Europäischen Parlaments zusammengesetzt – diesen Text erarbeitet hatte.[695] Überarbeitet und zum zweiten Mal in neuer Fassung proklamiert wurde die Charta am 12.12.2007. Über Art. 6 Abs. 1, UAbs. 1 EUV wurde die Charta darüber hinaus, mit Inkrafttreten des Vertrages von Lissabon am 01.12.2009 für verbindlich erklärt und im Amtsblatt der Union veröffentlicht. Sie gehört damit zum Primärrecht der Union. Die Charta markiert eine neue Etappe in der europäischen Grundrechtsentwicklung. Bis dato wurden die Grundrechte für die Union über die allgemeinen Rechtsgrundsätze aus den gemeinsamen Verfassungsüberlieferungen

692 Peters, EMRK, § 1 I 2; Grabenwarter, EMRK, 1 Rn. 1.

693 Grabenwärter, EMRK, § 5 Rn. 15 f.

694 Grabenwarter, EMRK, § 2 Rn. 4.

695 Meyer in Meyer, EU-GrCh, Präambel Rn. 8 ff.

der Mitgliedstaaten vom EuGH herausgearbeitet und bildeten so einen nicht kodifizierten Grundrechtsschutz. Einen großen Einfluss hatte dabei die EMRK als verbindlicher Grundrechtstext aller Mitgliedstaaten der Union.[696]

Zunächst stellte sich die Frage nach dem Inhalt der Charta. Eine Strömung wollte eine Sichtbarmachung bestehender Rechte, wie sie vom EuGH – an die EMRK angelehnt – entwickelt wurden, eine andere wollte die Grundrechte an neue Entwicklungen anpassen, eine dritte schließlich auch soziale Rechte in die Charta aufnehmen.[697]

Im Ergebnis sind viele Grundrechte an die EMRK angelehnt, teilweise ist es gelungen Lücken – gerade im Datenschutz – zu schließen, eine Reihe von sozialen Rechten wurde aufgenommen, teilweise auch als Grundsatz, deren gerichtliche Geltendmachung deutlich eingeschränkt ist.[698]

Die Grundrechtecharta verdeutlicht so, dass die Europäische Union nicht nur eine Rechts-, sondern auch eine Grundrechts- und eine Wertegemeinschaft ist.[699]

4. Das Grundgesetz

Das Grundgesetz für die Bundesrepublik Deutschland trat am 23.05.1949 in Kraft. Vorangegangen waren Beratungen des sogenannten Herrenchiemseer Verfassungskonvents sowie des Parlamentarischen Rates. Der Herrenchiemseer Verfassungskonvent erarbeitete vom 10.08.1948 bis 23.08.1948 einen Grundgesetzentwurf mit Anmerkungen und einer Übersicht über die Meinungsstände.[700] Diesem schloss sich vom 08.09.1948 bis 08.05.1949 die Arbeit des Parlamentarischen

696 Jarass, Charta EU-Grundrechte, Einl. Rn. 40 ff.

697 Jarass, Charta EU-Grundrechte, Einl. Rn. 5, zu den Sozialen Grundrechten siehe: Bernsdorff, Soziale Grundrechte in der Charta der Grundrechte der Europäischen Union, in VSSR 2001, S. 1.

698 Vgl. auch Jarass, Charta EU-Grundrechte, Einl. Rn. 5 ff.

699 Pache/Rösch, Die neue Grundrechtsordnung der EU nach dem Vertrag von Lissabon in EuR 2009, S. 769, 773 f.; 786 ff.

700 Sachs in Sachs, GG, Einführung Rn. 16.

Rates an.[701] Beeinflusst wurden die Arbeiten am Grundgesetz von den Vorgaben der Alliierten, etwa im Aide Mémoire vom 22.11.1948 das Mindesterfordernisse für ein künftiges Regelwerk aufstellte.[702] Bis heute hat das Grundgesetz 59 Änderungen erfahren.[703]

II. Das Verhältnis von Grundrechten nach dem Grundgesetz, der Grundrechtecharta der EU und der EMRK zueinander

Es gilt nun das Verhältnis der drei Grundrechtsregime – der EMRK, der Charta der Grundrechte, sowie des nationalen Grundrechtsschutzes – jeweils zueinander zu bestimmen. Damit sind die Funktion und das Verhältnis der EMRK auf Ebene der Europäischen Union wie auch auf nationalstaatlicher Ebene zu benennen und weiterhin den Einfluss der Grundrechtecharta auf die Unionsorgane wie auch auf die Mitgliedstaaten herauszuarbeiten.

Letztendlich ist für den Kollisionsfall eine Rangordnung der Grundrechtsebenen und ein Prüfungsmaßstab zu bestimmen, um im konkreten Anwendungsfall – bei nicht deckungsgleichem Gewährleistungsumfang aller Ebenen und Grundrechtsregime – einen eindeutigen Schutzumfang bestimmen zu können.

Eine Kollision liegt vor, *„wenn mindestens zwei Normen bei gleichzeitiger Anwendung zu miteinander nicht zu vereinbarenden oder vom Normgeber nicht intendierten Ergebnissen oder zur Nichtrealisierbarkeit eines vom Gesetzgeber intendierten Regelungszwecks führen“*, insbesondere wenn dadurch unterschiedliche Rechtsfolgen aufgezeigt werden.[704]

---

701 Sachs in Sachs, GG, Einführung Rn. 16.

702 Sachs in Sachs, GG, Einführung Rn. 19.

703 Die letzte Änderung ist vom 11.07.2012, BGBl., S. 1478.

704 Lindner, Grundrechtsschutz in Europa – System einer Kollisionsdogmatik in EuR 2007 Heft 2, S. 160, 163.

Grundsätzlich gelten die Grundsätze, „lex superior derogat legi inferiori" sowie „lex specialis derogat legi generali".[705] Innerhalb der deutschen Rechtsordnung sind diese Probleme durch – Art. 31 GG *„Bundesrecht bricht Landesrecht"* sowie Art. 142 GG – *„ungeachtet der Vorschrift des Art.s 31 bleiben Bestimmungen der Landesverfassungen auch insoweit in Kraft, als sie in Übereinstimmung mit den Art. 1 bis 18 dieses Grundgesetzes Grundrechte gewährleisten"* – geregelt.

Für das europäische Mehrebenensystem fehlen teilweise solche Regelungen, und allgemeine Rechtsgrundsätze versagen angesichts von Grundrechten, die Allgemeingültigkeit beanspruchen, ineinandergreifen, einander überlagern und überlappen.

Weiterhin ist jedoch ein Prüfungsmaßstab für solche Kollisionsfälle festzulegen. Im Grundsatz ist zunächst herauszuarbeiten, ob und wie weit der jeweilige Hoheitsträger an die Grundrechtsordnung gebunden ist.[706] Ist ein Hoheitsträger jeweils an nur ein Grundrechtssystem gebunden, ergeben sich daraus keine Probleme der Kollision, weil die anderen Grundrechtsregime den Hoheitsträger nicht binden. Im europäischen Mehrebenensystem ist jedoch davon auszugehen, dass ein Hoheitsträger von mindestens zwei Grundrechtssystemen gebunden wird: der Nationalstaat durch seine nationalen Grundrechte, die EMRK und gegebenenfalls die GrCh, die Union und Ihre Organe hingegen von der GrCh und der EMRK. Ausnahmen von diesem Grundsatz bilden die „Solange" Rechtsprechung des Bundesverfassungsgerichts und die Zurückhaltung bei der Überprüfung unionaler Rechtsakte durch den EGMR.[707]

---

705 Vgl. Vranes, Lex Superior, Lex Specialis, Lex Posterior – Zur Rechtsnatur der „Konfliktlösungsregeln" in ZaöRV 2005, S. 391.

706 Lindner, Grundrechtsschutz in Europa – System einer Kollisionsdogmatik in EuR 2007 Heft 2, S. 160, 189.

707 Lindner, Grundrechtsschutz in Europa – System einer Kollisionsdogmatik in EuR 2007 Heft 2, S. 160, 190.

1. Nationalstaatliche Ebene

Ausgangspunkt für die Betrachtung des Verhältnisses der verschiedenen Rechtsebenen und ihrer wechselseitigen Wirkungen ist der Nationalstaat als Hoheitsgewalt abtretende Ebene, von dem die Hoheitsgewalt ausgeht. Die Bundesrepublik wie auch die übrigen Mitgliedstaaten der Union haben sich dabei an die EMRK und auch in einem gewissen Umfang die GrCh gebunden. Auch auf der nationalstaatlichen Ebene ist neben einer Kollision der deutschen Grundrechte mit den beiden Grundrechtsregimen eine Kollision zwischen EMRK und GrCh denkbar.

Das deutsche Grundgesetz hat sein Verhältnis zur Europäischen Union und zur Übertragung von Hoheitsrechten ausführlich in Art. 23 GG geregelt. So wird unter bestimmten Bedingungen die Abtretung von Souveränität zugelassen und im Gegenzug werden Mitwirkungsrechte im Verflechtungsbereich vereinbart.[708] Das Bundesverfassungsgericht hat in seinen Urteilen dieses Verhältnis weiter präzisiert.

Die EMRK gilt in der Bundesrepublik über Art. 59 Abs. 2 GG im Rang eines Bundesgesetzes. Ihre Bedeutung und Funktion gehen dabei über die reine Position, die sich aus der Ratifikation eines völkerrechtlichen Vertrages ergibt, weit hinaus.

a) Art. 23 Abs. 1 GG

Art. 23 Abs. 1 S. 1 GG artikuliert mit der Formulierung *„und einen diesem Grundgesetz im wesentlichen vergleichbaren Grundrechtsschutz gewährleistet“* die Erwartung an einen Grundrechtsschutz in der EU und spiegelt dabei die Bindung des Art. 6 EUV.[709] Dabei handelt es sich um keine Kollisionsnorm. Es wird ein Grundrechtsschutz gegenüber Akten der Union gefordert, der dem Kern

[708] Schmahl, Grundrechtsschutz im Dreieck von EU, EMRK und nationalem Verfassungsrecht in EuR 2008 Heft Beiheft 1, S. 7, 32; Grawert, Der Deutschen supranationaler Nationalstaat in ders. u.a. (Hrsg.), Festschrift für E.-W. Böckenförde, 1995, S. 125 (142).

[709] Für Art. 6 EUV so im Ergebnis Schorkopf in Grabitz/Hilf/Nettesheim, EUV Art. 6 Rn. 16.

des nationalen Grundrechtschutzes entspricht.[710] Damit handelt es sich letztendlich um eine Festschreibung der „Solange II" Entscheidung des BVerfG.[711] Ein gleichwertiges Schutzniveau gilt unstreitig mit den vom EuGH entwickelten EU-Grundrechten und der GrCh als generell gegeben.[712]

b) Die Rechtsprechung der Bundesverfassungsgerichts

Das Bundesverfassungsgericht als „Hüter der Verfassung" ist maßgeblicher Akteur im deutschen und europäischen Grundrechtsschutz und hat in seiner Rechtsprechung deutlich zum Rangverhältnis zwischen deutschen und europäischen Grundrechten Stellung genommen und damit die deutsche Perspektive stark beeinflusst.

Ausgangspunkt dafür ist die „Solange Rechtsprechung" des BVerfG. *„Solange der Integrationsprozess der Gemeinschaft nicht so weit fortgeschritten ist, dass das Gemeinschaftsrecht auch einen von einem Parlament beschlossenen und in Geltung stehenden formulierten Grundrechtskatalog enthält, der dem Grundrechtskatalog des Grundgesetzes adäquat ist, ist nach Einholung der in Art. 234 EG geforderten Entscheidung des EuGH die Vorlage eines Gerichtes der Bundesrepublik Deutschland an das BVerfG im Normenkontrollverfahren zulässig und geboten, wenn das Gericht die für es entscheidungserhebliche Vorschrift des Gemeinschaftsrechts in der vom EuGH gegebenen Auslegung für unanwendbar hält, weil und soweit sie mit einem der Grundrechte des Grundgesetzes kollidiert".*[713] Diese Rechtsprechung wurde mit dem „Solange II" Beschluss weitgehend gelockert. *„Solange die Europäischen Gemeinschaften, insbesondere die Rechtsprechung des Gerichtshofs der*

---

710 Jarass in Jarass/Pieroth, GG, Art. 23 Rn. 20; Uerpmann/Wittzack in v. Münch/Kunig, Grundgesetz, 6. Aufl. 2012, Art. 23 GG Rn. 25; Classen in v. Mangoldt/Klein/Starck, GG, Bd. 2, Art. 23 Rn. 42 ff.; BVerfGE 102, 147/164; 73, 339/387.

711 So auch Hillgruber in Schmidt-Bleibtreu/Klein, GG, Art. 23 GG Rn. 23; Classen in. v. Mangoldt/Klein/Starck, GG, Bd. 2 Art. 23 Rn. 42.

712 Jarass in Jarass/Pieroth, GG, Art. 23 Rn. 20; Hillgruber in Schmidt-Bleibtreu/Klein, GG, Art. 23 GG Rn. 23; Uerpmann/Wittzack in v. Münch/Kunig, Art. 23 GG Rn. 29; Classen in v. Mangoldt/Klein/Starck, GG, Bd. 2, Art. 23 Rn. 45; BVerfGE 73, 339/378.

713 BVerfGE 37, S. 271.

Gemeinschaften einen wirksamen Schutz der Grundrechte gegenüber der Hoheitsgewalt der Gemeinschaften generell gewährleisten, der dem vom Grundgesetz als unabdingbar gebotenen Grundrechtsschutz im wesentlichen gleichzuachten ist, zumal den Wesensgehalt der Grundrechte generell verbürgt, wird das Bundesverfassungsgericht seine Gerichtsbarkeit über die Anwendbarkeit von abgeleitetem Gemeinschaftsrecht, das als Rechtsgrundlage für ein Verhalten deutscher Gerichte und Behörden im Hoheitsbereich der Bundesrepublik Deutschland in Anspruch genommen wird, nicht mehr ausüben und dieses Recht mithin nicht mehr am Maßstab der Grundrechte des Grundgesetzes überprüfen; entsprechende Vorlagen nach Art. 100 Abs. 1 GG sind somit unzulässig."[714]

So behält sich das BVerfG grundsätzlich ein Prüfungsrecht vor, verzichtet jedoch auf eine Kontrolle im konkreten Einzelfal, solange nicht ein generelles Absinken des unionalen Grundrechtsschutzes festgestellt wird.[715] Im „Maastricht Urteil" geht das BVerfG in Abweichung zu seiner bisherigen Rechtsprechung davon aus, dass auch Akte der Organe der Union an den Grundrechten gemessen werden können.[716] Jedoch geschieht dies in einem „Kooperationsverhältnis" zum EuGH.[717]

c) Zwischenergebnis

Art. 23 Abs. 1 S. 1 GG gibt lediglich die Grundlagen für das Verhältnis zwischen nationalen und unionalen Grundrechten vor. Es legt weniger ein Rangverhältnis und mehr ein Nebeneinander der Grundrechtsebenen fest. Konkreter wird das Bundesverfassungsgericht, Akte der Union müssen weiterhin mit dem Wesensgehalt der Grundrechte vereinbar sein. Dadurch dass der unionale Grundrechtsschutz jedoch im Kern das gleiche Schutzniveau bietet, werden Akte der Union grundsätzlich an den EU-Grundrechten und der GrCh gemessen.

---

714 BVerfGE 73, S. 339/340.

715 BVerfGE 102, 147/164; Uerpmann/Wittzack in v. Münch/Kunig, Art. 23 GG Rn. 30 f.

716 BVerfGE 89, S. 155/175.

717 BVerfGE, S. 155/156, 175.

2. Ebene der Europäischen Union

Auf Ebene der Europäischen Union wurde der Grundrechtsschutz zunächst durch die Rechtsprechung des EuGH aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten entwickelt.

Im Vertrag von Lissabon findet sich mit Art. 6 EUV eine Rechtsnorm, die aus Sicht der EU ihr Verhältnis zu den verschiedenen Grundrechtssystemen strukturiert. Schließlich gehört die Europäische Grundrechtecharta zum primären Unionsrecht.

Art. 51, 52, 53 GrCh befassen sich hingegen mit der Anwendbarkeit, der Tragweite und dem Schutzniveau der in der Charta garantierten Rechte.

a) Art. 6 EUV

Ausgangspunkt für die Betrachtung auf Ebene des Rechts der Europäischen Union ist Art. 6 EUV. Die Vorschrift ist mit dem Vertrag von Lissabon weitgehend neugefasst worden und nimmt Stellung zur Bindung der EU an die Grundrechte-Charta sowie an die EMRK.[718] Gemeinsam mit den allgemeinen Grundsätzen werden so die Rechtsquellen der Union benannt.[719] Indem mit Art. 6 die EU im europäischen Grundrechtsraum verankert wird, soll diese als Rechts- und Wertegemeinschaft positioniert werden.[720] Der Beitritt zur EMRK soll die Bindung an den völkerrechtlichen Menschenrechtsschutz unterstreichen.[721] Die Grundrechtsbindung der Institution EU ist etwas Singuläres, da bisher nur Staaten an Grundrechte gebunden waren, und hebt die EU damit von anderen internationalen Organisationen ab.[722]

Abs. 1 bezieht sich auf das Verhältnis zur Grundrechtecharta, während sich die Absätze 2 und 3 mit dem Beitritt und dem Verhältnis zur EMRK befassen.

---

[718] Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 1 f.

[719] Jarass, Charta EU-Grundrechte, Art. 6 EUV Rn. 1.

[720] Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 11.

[721] Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 10.

[722] Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 15.

aa) Art. 6 Abs. 1 EUV

Mit der Formulierung des Art. 6 Abs. 1, UAbs. 1 Hs. 1 EUV *„Die Union erkennt die Rechte, Freiheiten und Grundsätze an, die in der Charta der Grundrechte der Europäischen Union vom 07.12.2000 in der am 12.12.2007 in Straßburg angepassten Fassung niedergelegt sind"* wird die Grundrechtecharta anerkannt und mittelbar zu einem Rechtsakt.[723]

Die sich daraus ergebende Rechtsfolge ist der Formulierung nicht zu entnehmen. Der Hinweis auf die Rechtsverbindlichkeit war auf der Regierungskonferenz 2007 mit dem Hinweis auf die Gleichrangigkeit gestrichen worden.[724] Jedoch wird die Rechtsverbindlichkeit in den Erklärungen zu den Bestimmungen der Verträge erklärt und ist damit als unzweifelhaft gegeben anzusehen.[725]

Die Formulierung nennt die Trias von Rechten, Freiheiten und Grundsätzen und geht damit über die reine Geltung von Grundrechten hinaus. Alle in der Grundrechtecharta enthaltenen Zielsetzungen sollen damit Rechtsverbindlichkeit erlangen. *„Die Charta der Grundrechte und die Verträge sind rechtlich gleichrangig"* (Art. 6 Abs. 1 UAbs. 1, Hs. 2 EUV). Damit gehört sie neben den Verträgen und den allgemeinen Grundsätzen zum Primärrecht der Union.[726]

Eine Ausnahme von der Anwendbarkeit der Grundrechtecharta besteht über das gleichrangig gültige Protokoll Nr. 30 für Polen und für Großbritannien. Als weiteres Land hat Tschechien ebenfalls eine solche Ausnahmeregelung ausgehandelt, die in das Protokoll Nr. 30 aufgenommen und mit dem Beitrittsvertrag Kroatiens rechtsverbindlich geworden ist.

Demnach greift die Jurisdiktion der EU bei der Kollision mit der Grundrechtecharta mit nationalem Recht nicht. Ferner wird festgestellt, dass keine neuen Rechte oder Grundsätze begründet werden, die die nationalen Rechtsordnungen nicht vorsehen. Die derzeitigen Folgen der Ausnahmeregelung sind begrenzt,

---

723 Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 19 ff.

724 Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 20.

725 ABl. der Europäischen Union C 115/337, Nr. 1.

726 Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 28 f.

da die Charta ohnehin keine neuen Rechte vorsieht, denn *„durch die Bestimmungen der Charta werden die in den Verträgen festgelegten Zuständigkeiten der Union in keiner Weise erweitert"*, sondern lediglich den bestehenden aquis bündelt und bekräftigt, der über die allgemeinen Grundsätze oder die EMRK auch weiterhin anwendbar bleibt.[727] Relevanz könnte die Ausnahme bekommen, falls in Zukunft – im Wege einer dynamischen Auslegung der Charta wie auch bei den Verträgen schon geschehen – neue Rechte oder Pflichten begründet würden.[728]

Eine weitere Präzisierung findet sich im Bezug auf Irland, das sich vor dem zweiten Referendum zum Vertrag von Lissabon hat zusichern lassen, dass die irischen Verfassungsbestimmungen bezüglich des Rechts auf Leben sowie zu den Bereichen Bildung und Familie vom neuen Primärrechtsstatus der GrCh nicht berührt werden.[729]

Art. 6 Abs. 1 UAbs. 3 EUV legt fest, dass *„die in der Charta niedergelegten Rechte, Freiheiten und Grundsätze"*, *„gemäß den allgemeinen Bestimmungen des Titels VII der Charta, der ihre Auslegung und Anwendung regelt, und unter gebührender Berücksichtigung der in der Charta angeführten Erläuterungen, in denen die Quellen dieser Bestimmungen angegeben sind, ausgelegt"* werden. Damit werden die Grundsätze und Grundrechte der Charta direkt an das übrige Unionsrecht angebunden und gerade der Interpretationsspielraum der Judikative eingeschränkt und an die Verfassungstradition der Mitgliedstaaten und an den Willen des Gesetzgebers gebunden. Die bisherige Praxis der Rechtsprechung einer dynamischen Auslegung des Primärrechts wird dadurch erschwert.

bb) Art. 6 Abs. 2 EUV

Ursprünglich sollte der Beitritt der Europäischen Union zur Europäischen Menschenrechtskonvention eine Antwort auf einen fehlenden geschriebenen Grund-

---

727 Art. 6 Abs. 1 UAbs. 2 EUV; Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 24.

728 Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 24.

729 Tagung des Europäischen Rates vom 11./12.12.2008 in Brüssel, Schlussfolgerungen des Vorsitzes, 12.12.2008, CONCL 5/17271/08, S. 2, zitiert nach: Pache/Rösch, Die neue Grundrechtsordnung der EU nach dem Vertrag von Lissabon in EuR 2009, S. 769, 770.

rechtskatalog auf unionaler Ebene sein.[730] Dieses Problem wurde mit der Grundrechtecharta der Europäischen Union behoben, gleichzeitig jedoch ein weiterer Grundrechtskatalog im europäischen Rechtsraum geschaffen, der zwar nicht deckungsgleich, jedoch für die Länder der EU neben der EMRK steht. Der Beitritt dient deswegen der Verzahnung der beiden Schutzsysteme, um eine Kohärenz der Rechtsprechung von EuGH und EGMR und damit des Grundrechtsschutzes in Europa sicherzustellen.[731] Bestätigt wird damit auch die bisherige Rechtsprechung des EuGH, die auf die EMRK Bezug genommen hat.[732] Die EMRK wird zu einer verbindlichen Rechtserkenntnisquelle des Unionsrechts und bindet mit dem Beitritt die Organe der Union.[733]

Art. 6 Abs. 2 S. 1 EUV – *„die Union tritt der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten bei"* – formuliert zunächst einen Beitrittsimperativ, der durch das Protokoll Nr. 8 ergänzt wird, da man der EMRK nicht durch Erklärung, sondern nur durch einen völkerrechtlichen Vertrag beitreten kann.[734]

Auf Seiten der EMRK erfordert ein Beitritt der Europäischen Union eine Änderung der Konvention, da bisher gemäß Art. 59 Abs. 1 EMRK nur Mitglieder des Europarats der Konvention beitreten können. Diesem beitreten können wiederrum nach Art. 4 der Satzung nur Staaten. Die nötigen Änderungen sind im 14. Zusatzprotokoll zur EMRK vorbereitet, das von 46 der 47 Staaten ratifiziert

730 Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 36.

731 Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 36.

732 So z. B. das Urteil des Gerichtshofes, Stauder, 29/69, Slg. 1969, 419 vom 12.11.1969.

733 Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 36; eine Übersicht der Urteile des EuGH die sich auf die EMRK beziehen, ist zu finden bei Schorkopf in der Fn. 79.

734 ABL der Europäischen Union, C 83/273 Protokoll (Nr. 8) zu Art. 6 Abs. 2 des Vertrags über die Europäische Union über den Beitritt der Union zur Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten; Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EU Rn. 37.

wurde, bislang fehlt eine Ratifikation durch Russland.[735] Solange diese ausbleibt, ist ein Beitritt der EU zur EMRK juristisch nicht möglich.[736]

Auf Seiten der Union fordern die Erklärungen zu den Bestimmungen der Verträge, dass der Beitritt die Besonderheiten der Rechtsordnung der Union wahrt.[737] Art. 1 Protokoll Nr. 8 präzisiert Art. 6 Abs. 2 EUV dahingehend, dass die besonderen Merkmale der EU erhalten bleiben und in die Funktionsweise der EMRK integriert werden. Art. 2 Protokoll Nr. 8 sichert den Status quo der Mitgliedstaaten im Verhältnis zur EMRK sowie der Zuständigkeiten der Union und ihrer Organe. Die Festlegung auf die Zuständigkeit der Union wird in Art. 6 Abs. 2 S. 2 EUV ebenfalls festgehalten. Zu den weiteren besonderen Merkmalen der Union gehört insbesondere deren Gerichtssystem.[738] So muss der ausgeprägte Subsidiaritätsgrundsatz, der für den Rechtsweg in der Union gilt und in den Mitgliedstaaten anfängt, sowie die Tatsache, dass zum Wesen der Rechtsordnung die Umsetzung oder Durchführung der Rechtsakte oft im mitgliedsstaatlichen Bereich liegt, Beachtung finden.[739]

Der bereits bestehende Dialog zwischen EuGH und EGMR soll zur Sicherung dieses Gefüges intensiviert werden.[740]

cc) Art. 6 Abs. 3 EUV

Art. 6 Abs. 3 EUV stellt fest, dass *„die Grundrechte, wie sie in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten gewährleistet sind*

---

735 Pache/Rösch, Die neue Grundrechtsordnung der EU nach dem Vertrag von Lissabon in EuR 2009, S. 769, 780.

736 Pache/Rösch, Die neue Grundrechtsordnung der EU nach dem Vertrag von Lissabon in EuR 2009, S. 769, 781. Zur Weigerung Russlands: EUGRZ 2007, 241.

737 ABL der EU C 115/337, A. Erklärungen zu Bestimmungen der Verträge Nr. 2.

738 Reflexionspapier des Gerichtshofes der Europäischen Union zu bestimmten Aspekten des Beitritts der Europäischen Union zur Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten, Luxemburg, den 5. Mai 2010, Nr. 4 f.

739 Reflexionspapier des Gerichtshofes der Europäischen Union zu bestimmten Aspekten des Beitritts der Europäischen Union zur Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten, Luxemburg, den 5. Mai 2010, Nr. 4 f.

740 ABL der EU C 115/337, A. Erklärungen zu Bestimmungen der Verträge Nr. 2.

und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten ergeben", *„als allgemeine Grundsätze Teil des Unionsrechts"* sind. Damit wird eine Brücke von der EMRK und den nationalen Grundrechten hin zum Europarecht geschlagen, indem deren Grundrechtsgewährleistungen als Teil der allgemeinen Grundsätze angesehen werden.

Diese Einbeziehung der Grundrechte in die allgemeinen Grundsätze durch Art. 6 EUV wird durchaus kritisch gesehen. So wird sie durch den direkten Schutz, den die Grundrechtecharta entfaltet, als überflüssig angesehen.[741] Hier muss man zumindest von einer vorrangigen Anwendung der Grundrechtecharta ausgehen, da sie den verschriftlichten und verrechtlichten Willen des Gesetzgebers widerspiegelt und sonst ins Leere liefe.[742] Weiterhin kann diese Konstruktion als Einfallstor dazu genutzt werden, die dynamische Auslegung der Verträge an dieser Stelle im Grundrechtsschutz fortzusetzen und „neue" Gewährleistungen aus der gemeinsamen Verfassungsüberlieferung der Mitgliedstaaten zu entwickeln. Nicht zuletzt ist die Regelung zum Aushebeln der Anwendungsausnahmen der GrCh für Polen und Großbritannien geeignet.[743]

Gleichzeitig wird damit eine Dopplung des Grundrechtsschutzes durch die EMRK vollzogen, da der durch die EMRK gewährleistete Grundrechtsumfang direkt durch den Beitritt zur EMRK wirkt und gleichzeitig indirekt über die allgemeinen Grundsätze Resonanz findet. Jedoch ist diese Dopplung so in der Lage, eine Kohärenz des Grundrechtsschutzes in Europa dadurch herzustellen, dass über die allgemeinen Grundsätze auf Ebene der Europäischen Union – gerade auch bei der Rechtsprechung durch den EuGH – die EMRK wie auch die gemeinsamen nationalen Verfassungsüberlieferungen Beachtung finden müssen.

---

741 Schmitz, Die Grundrechtecharta als Teil der Verfassung der Europäischen Union in EuR 2004, 691 (698).

742 Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 56.

743 Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 53.

dd) Zwischenergebnis

Die Union wird durch drei Grundrechtssäulen gebunden: erstens die Grundrechte, die in der Charta der Grundrechte der Europäischen Union verbrieft sind, zweitens mit dem Beitritt der EU zur EMRK den Grundrechtskatalog der Konvention sowie drittens die in den allgemeinen Grundsätzen enthaltenen Grundrechte, die sich aus den Verfassungsüberlieferungen der Mitgliedstaaten speisen.

Mit Art. 6 Abs. 1 EUV werden die Grundrechte, Freiheiten und Grundsätze der Charta der Grundrechte der Europäischen Union Bestandteil des Primärrechts und binden damit die Europäische Union und ihre Organe bei der Ausübung ihrer Rechte und Pflichten. Insbesondere der EuGH wird nun bei seiner dynamischen Auslegung der Verträge an geschriebene Grundrechte gebunden.

Die Grundrechte aus den allgemeinen Grundsätzen bilden eine weitere Grundrechtssäule ab, die sich aus den Verfassungstraditionen der Mitgliedstaaten speist und vom EuGH herausgearbeitet wurde und die neben der Grundrechtecharta und der EMRK gleichberechtigt steht. Grundsätzlich sind alle Grundrechtssäulen harmonisierend auszulegen. Durch die geschriebene Verfasstheit der Grundrechtecharta dürfte auf die Grundrechte aus allgemeinen Grundsätzen nur dort zurückzugreifen sein, wo sie weitergehende Rechte als die Grundrechtecharta gewähren, insbesondere da die gemeinsame Grundrechtstradition der Mitgliedstaaten in der EMRK einen gemeinsamen Ausdruck gefunden hat, auf den der EuGH zurückgreifen konnte und der diese beeinflusst hat und wiederum auch in der Grundrechtecharta seinen Niederschlag gefunden hat.

Bezogen auf den Beitritt zur EMRK werden die in ihr enthaltenen Grundrechte für die Europäische Union verbindlich. Die Union und ihre Organe unterliegen damit dem Grundrechtsregime letztendlich wie ein Mitgliedsstaat. Die Rechtsakte der Union unterliegen demnach der Überprüfbarkeit durch den EGMR.[744] Der EuGH verliert weiterhin das von ihm beanspruchte Auslegungsmonopol über das Unionsrecht, soweit die EMRK tangiert wird, zugunsten des EGMR.[745]

---

[744] Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 45.

[745] Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 45.

Dass die Grundrechtsbindung zu keiner Erweiterung der Zuständigkeit der EU führen darf, ist durch mehrere Wiederholungen manifestierter Wille des Gesetzgebers.

b) Art. 51 GrCh, Anwendungsbereich

Art. 51 Abs. 1 S. 1 GrCh regelt den Anwendungsbereich der Charta, sie *„gilt für die Organe und Einrichtungen der Union unter Einhaltung des Subsidiaritätsprinzips und für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union"*. Damit wird zunächst die Bindung der Union und ihrer Organe und aller nachgeordneten Stellen an die Charta festgelegt.[746] Die Regelung präzisiert Art. 6 EUV sowie die Erläuterungen und Protokolle dahingehend, dass die Mitgliedstaaten nur bei der Durchführung des Unionsrechts an die Charta gebunden sind.[747] Die gesamte Hoheitsgewalt der Union soll so – an die Unionsgrundrechte, unabhängig von der Organisationsform – gebunden werden.[748] Die Bindung der Mitgliedstaaten,umfasst alle Teilgliederungen eines Mitgliedsstaates je nach Organisation. Verpflichtet werden neben zentralen Behörden auch regionale und lokale Stellen sowie öffentliche Einrichtungen, wenn sie Unionsrecht anwenden.[749] Davon umfasst sind sowohl die legislative Umsetzung als auch der administrative Vollzug.[750]

Was unter der Durchführung des Rechts der Union zu verstehen ist, ist umstritten. Die Rechtsprechung versteht den Begriff wohl weit als „Handeln im Rahmen des Unionsrechts".[751] Beachtet man hingegen den Wortlaut und die Entstehungsgeschichte der Norm, die Kompetenzen der Union nicht zu erwei-

---

746 Callies/Ruffert, EUV-AEUV, Art. 51 EUV Rn. 4 ff.

747 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

748 Borowsky in Meyer, EU-GrCh Art. 51 Rn. 16; Jarass, Charta EU-Grundrechte, Art. 51 Rn. 1 ff.

749 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

750 Kingreen in Callies/Ruffert, EUV-AEUV, Art. 51 EUV Rn. 8; Jarass, Charta EU-Grundrechte, Art. 51 GrCh Rn. 16 f.

751 Koen/Lenaerts, Die EU-Grundrechtecharta: Anwendbarkeit und Auslegung in EuR 2012, S. 3 (5).

tern, ist unter der Durchführung des Rechts der Union die Situation zu verstehen, wenn die Mitgliedstaaten als Vertreter der Union handeln.[752]

Art. 51 Abs. 2 betont wie schon in Art. 6 EUV sowie den Erläuterungen, dass *„weder neue Zuständigkeiten noch neue Aufgaben für die Gemeinschaft und für die Union"* begründet noch *„die in den Verträgen festgelegten Zuständigkeiten und Aufgaben"* geändert werden.[753] Mit dieser Regelung wird dem Subsidiaritätsprinzip folgend sichergestellt, dass durch die Charta keine Erweiterung der Zuständigkeiten und Aufgaben des Unionsrechts bewirkt wird.[754] Auch den Verpflichtungen und Garantien aus der Charta darf die Union nur im Rahmen ihrer Befugnisse nachkommen.[755]

c) Art. 52 GrCh, Tragweite der garantierten Rechte

Art. 52 GrCh regelt die Tragweite der garantierten Rechte. Die Einschränkungsregelung von Abs. 1 lehnt sich an die Rechtsprechung des EuGH an.[756] So muss *„jede Einschränkung der Ausübung der in dieser Charta anerkannten Rechte und Freiheiten" „gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten. Unter Wahrung des Grundsatzes der Verhältnismäßigkeit dürfen Einschränkungen nur vorgenommen werden, wenn sie notwendig sind und den von der Union anerkannten dem Gemeinwohl dienenden Zielsetzungen oder den Erfordernissen des Schutzes der Rechte und Freiheiten anderer tatsächlich entsprechen"*. Diese Schrankenregelung gilt für Grundrechte unabhängig davon, ob diese noch eigene

---

752 Koen/Lenaerts, Die EU-Grundrechtecharta: Anwendbarkeit und Auslegung in EuR 2012, S. 3 (4 ff.); im Ergebnis wohl auch Jarass, Charta EU-Grundrechte, Art. 51 GrCh Rn. 11 ff.

753 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

754 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.; so Jarass, Charta EU-Grundrechte, Art. 51 GrCh Rn. 8 f.

755 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff. so auch Jarass, Charta EU-Grundrechte, Art. 51 GrCh Rn. 8 f.

756 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

spezielle Schranken aufweisen.[757] Ausgenommen von den Schranken sind lediglich die Grundrechte die, uneinschränkbar sind.[758]

Zunächst wird mit Satz 1 ein einfacher Gesetzesvorbehalt formuliert, der als Gesetzgebungsvorbehalt zu verstehen ist und alle Rechtsakte umfasst, die im Rahmen eines unionalen Gesetzgebungsverfahrens erlassen worden sind.[759] Soweit die Mitgliedstaaten gebunden werden, muss ein nationaler Rechtssatz ausreichen.[760] Weiterhin wird eine Wesensgehaltsgarantie festgelegt.

Schließlich wird der Grundsatz der Verhältnismäßigkeit verankert. Der Begriff des Gemeinwohls bezieht sich nicht nur auf die in Art. 6 EUV formulierten Ziele, sondern ebenfalls auf weitere Interessen, wie z. B. in Art. 4 EUV, Art. 35 AEUV, Art. 36 AEUV sowie Art. 346 AEUV festgelegt.[761]

Art. 52 Abs. 2 GrCh regelt *„die Ausübung der durch diese Charta anerkannten Rechte, die in den Gemeinschaftsverträgen oder im Vertrag* über *die Europäische Union begründet sind“*, diese, *„erfolgt im Rahmen der darin festgelegten Bedingungen und Grenzen“*. Hierdurch soll der Umfang der Rechte aus den Verträgen – insbesondere der Unionsbürgerschaft – garantiert, aber auch auf den bestehenden Umfang begrenzt werden.[762] Damit stellt der Abs. eine Kollisionsregelung im Verhältnis zu Rechten aus dem EUV und AEUV dar.[763] Die Vorgaben in den weiteren Absätzen von Art. 52 GrCh treten damit in Sinne der Spezialität hinter die Regelungen im EUV und AEUV zurück.[764] Zu den Rechten zählen neben

---

757 Kingreen in Callies/Ruffert, EUV-AEUV, Art. 52 EUV Rn. 59.

758 Dies trifft wohl auf Art. 1 oder Art. 5 Abs. 3 GrCh zu. Dazu siehe Callies/Ruffert, EUV-AEUV, Art. 52 EUV Rn. 60.

759 Kingreen in Callies/Ruffert, EUV-AEUV, Art. 52 EUV Rn. 61 f.; Jarass, Charta EU-Grundrechte, Art. 52 Rn. 23 ff.

760 Jarass, Charta EU-Grundrechte, Art. 52 Rn. 26.

761 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

762 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

763 Kingreen in Callies/Ruffert, EUV-AEUV, Art. 52 EUV Rn. 3; Becker in Schwarze, EU, Art. 52 GrCh Rn. 13.

764 Kingreen in Callies/Ruffert, EUV-AEUV, Art. 52 EUV Rn. 3.

subjektiven Rechten wohl auch Kompetenzbestimmungen.[765] Damit eine Spezialität vorliegt, muss eine funktionale Äquivalenz vorliegen, das bedeutet, dass eine sinngemäße Übereinstimmung zwischen einem Unionsgrundrecht und einem Recht in den Verträgen vorliegen muss.[766]

Art. 52 Abs. 3 GrCh regelt das Verhältnis der Charta zur EMRK. So sollen die Rechte aus der Charta, *„die den durch die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten garantierten Rechten entsprechen*", *„die gleiche Bedeutung und Tragweite, wie sie ihnen in der genannten Konvention verliehen wird"*, haben. *„Diese Bestimmung steht dem nicht entgegen, dass das Recht der Union einen weiter gehenden Schutz gewährt".*

So soll eine Kohärenz zwischen GrCh und EMRK hergestellt werden, die sich auch auf die Schranken der Rechte bezieht und vom Gesetzgeber beachtet werden muss.[767] Von dieser Geltung umfasst wird auch der EGMR.[768] Fraglich erscheint, wie weit die Formulierung der gleichen Bedeutung und Tragweite zu verstehen ist. Eine direkte Bindung an die EMRK als Rechtsquelle wird über diese Formulierung überwiegend abgelehnt.[769] Einigkeit besteht weitgehend über den Charakter der EMRK als Rechtserkenntnisquelle.[770] Art. 52 Abs. 3 S. 2 GrCh stellt sicher, dass die Union einen weitergehenden Schutz gewährleisten kann.[771]

---

765 Kingreen in Callies/Ruffert, EUV-AEUV, Art. 52 EUV Rn. 5. Für Kompetenzbestimmungen als Rechte im Sinne des Art. 52 Abs. 2 GrCh hat sich das Präsidium des Europäischen Konvents ausgesprochen (GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.).

766 Kingreen in Callies/Ruffert, EUV-AEUV, Art. 52 EUV Rn. 8.

767 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

768 Naumann, Kolja, Art. 52 Abs. 3 GrCh zwischen Kohärenz des europäischen Grundrechtsschutzes und Autonomie des Unionsrechts in EuR 2008, S. 424 (425); Jarass, Charta EU-Grundrechte, Art. 52 Rn. 65.

769 Kingreen in Callies/Ruffert, EUV-AEUV, Art. 52 EUV Rn. 32 ff., 34, 37.

770 Kingreen in Callies/Ruffert, EUV-AEUV, Art. 52 EUV Rn. 32 ff., 34, 37; Ehlers in Ehlers, GuG § 14 Rn. 29; Jarass, Charta EU-Grundrechte, Art. 52 Rn. 64; anders Borowsky in Meyer, EU-GrCh, Art. 52 Rn. 34; ausführlicher dazu Naumann, Kolja, Art. 52 Abs. 3 GrCh zwischen Kohärenz des europäischen Grundrechtsschutzes und Autonomie des Unionsrechts in EuR 2008, S. 424 (429 ff).

771 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

Art. 52 Abs. 4 GrCh bezieht die Verfassungs- und Grundrechtstradition der Mitgliedstaaten als Rechtserkenntnisquelle ein.[772] Diese müssen weder in allen Mitgliedstaaten identisch sein noch seit langem bestehen.[773] Als Verfassungstradition scheidet jedoch eine Vorstellung aus, die nur in wenigen Mitgliedstaaten anzutreffen ist und auf deren Inhalt bezogen die meisten Mitgliedstaaten andere Vorstellungen entwickelt haben.[774]

d) Art. 53 GrCh, Schutzniveau

Gemäß Art. 53 GrCh soll keine Bestimmung der Charta, „als eine Einschränkung oder Verletzung der Menschenrechte und Grundfreiheiten" ausgelegt werden, *„die in dem jeweiligen Anwendungsbereich durch das Recht der Union und das Völkerrecht sowie durch die internationalen Übereinkommen, bei denen die Union, die Gemeinschaft oder alle Mitgliedstaaten Vertragsparteien sind, darunter insbesondere die Europäische Konvention zum Schutze der Menschenrechte und Grundfreiheiten, sowie durch die Verfassungen der Mitgliedstaaten anerkannt werden"*. Die Norm regelt das Verhältnis der Grundrechtecharta zu nationalen und supranationalen Grundrechtskatalogen. So soll sichergestellt werden, dass das gegenwärtige Schutzniveau in der Union aufrechterhalten wird.[775]

e) Die Rechtsprechung des EuGH

Bei der Gründung und Entwicklung der Gemeinschaften wurde auf einen Grundrechtskatalog in den Verträgen verzichtet. Eine Absicherung des unionalen Handelns durch Grundrechte lag nicht im Fokus und wurde zunächst nicht

772 Kingreen in Callies/Ruffert, EUV-AEUV, Art. 52 EUV Rn. 39 ff.; EuGH, Gutachten 2/94, Slg. 1996, I-1759, (I-1789) Rn. 33.

773 Jarass, Charta EU-Grundrechte, Art. 52 Rn. 66.

774 Jarass, Charta EU-Grundrechte, Art. 52 Rn. 66.

775 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

als notwendig erachtet; eine Freistellung von Grundrechten war jedoch ebenfalls nicht beabsichtigt.[776]

Das weitgehende Fehlen eines geschriebene Grundrechtskataloges – mit einigen Ausnahmen in den Verträgen – führte zu einer Entwicklung von Grundrechtsstandards aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten sowie der Rechtsprechung des EGMR durch den Europäischen Gerichtshof.[777]

Ausgangspunkt des Rechtsprechung des EuGH zum Verhältnis des nationalen Rechts zum Gemeinschaftsrecht war das Urteil des EuGH vom 05.02.1963 (van Gend & Loos gegen die Niederländische Finanzverwaltung), in dem festgestellt wurde das Gemeinschaftsrecht sei eine neue Rechtsordnung, deren Rechtssubjekt neben den Mitgliedstaaten auch der Einzelne sei, dem aus dieser Rechtsordnung Rechte zustehen.[778] Weiterentwickelt wurde diese Rechtsprechung im Urteil „Costa/ENEL“ vom 15.07.1964, in dem der Vorrang des Gemeinschaftsrechts vor nationalem Recht betont wurde, der durch die Abtretung von Hoheitsrechten an die Gemeinschaft zustande gekommen sei.[779] Die Existenz von (damals noch) Gemeinschaftsgrundrechten wurde erstmals im EuGH Urteil vom 12.11.1969 („Stauder“) bejaht.[780] Im Urteil vom 17.12.1970 (Internationale Handelsgesellschaft/Einfuhr- und Vorratsstelle für Getreide und Futtermittel) wird schließlich ein Vorrang des Gemeinschaftsrechts vor nationalen Grundrechten mit der Begründung herausgearbeitet, Akte der Gemeinschaft seien an Gemeinschaftsgrundrechten zu messen.[781]

Im Urteil vom 13.06.1996 (Maurin) wird Stellung zur Geltung der Gemeinschaftsgrundrechte gegenüber der Hoheitsgewalt der Mitgliedstaaten genommen,

---

776 Bahlmann, Der Grundrechtsschutz in der EG, EuR 1982, S. 1, 3; Nicolaysen, Die gemeinschaftsrechtliche Begründung von Grundrechten in EuR 2003, 722.

777 So auch Mehde, Gespaltener Grundrechtsschutz in der EU? in EuGRZ 2008, S. 269 (270).

778 van Gend & Loos, EuGH Urteil vom 05.02.1963 – Slg 1963 Rs. 26/62 S. 1 (25).

779 Costa/ENEL, EuGH Urteil vom 15.07.1964, Slg. 1964, S. 1251, 1269 f.

780 Pechstein, Entscheidungen des EuGH, 7. Aufl. 2012 Tübingen, S. 63 Rn. 23.

781 Internationale Handelsgesellschaft/Einfuhr- und Vorratsstelle für Getreide und Futtermittel, EuGH Urteil vom 17.12.1970 – Slg. 1979, S. 1125.

die gegenüber diesen grundsätzlich keine Wirkung entfalten.[782] Die Funktion der Grundrechte geht jedoch über die reine Abwehrfunktion hinaus. Diese sichern auch den unionalen Freiheitsraum gegenüber den Mitgliedstaaten, insoweit gelten die Grundrechte auch bei Durchführung von Unionsrecht durch die Mitgliedstaaten diesen gegenüber.[783]

f) Zwischenergebnis

Nachdem zunächst der EuGH einen Vorrang des Unionsrechts vor dem nationalen Recht und dessen Prüfung einzig an Unionsgrundrechten herausgearbeitet hat, wurde mit der Grundrechtecharta diese Rechtsprechung in die Art. 6 EUV, Art. 51 bis Art. 53 GrCh übernommen. Es besteht nun eine dreifache Bindung aus allgemeinen Rechtsgrundsätzen, GrCh und EMRK gegenüber Akten und Einrichtungen der Union.

3. Ebene der Europäischen Menschenrechtskonvention

Neben der Rechtsprechung des EGMR regelt Art. 53 EMRK das Verhältnis dieser zu Grundrechten der Vertragsparteien.

a) Art. 53 EMRK

Gemäß Art. 53 EMRK ist die Konvention *„nicht so auszulegen, als beschränke oder beeinträchtige sie Menschenrechte und Grundfreiheiten, die in den Gesetzen einer Hohen Vertragspartei oder in einer anderen Übereinkunft, deren Vertragspartei sie ist, anerkannt werden“*.

Damit wird das Verhältnis von nationalem Recht und der EMRK nach dem Günstigkeitsprinzip entschieden.[784] Diese Regelung trägt der Tatsache Rechnung,

---

[782] Maurin, Slg. 1996, I-2909 Rn. 12.

[783] Nicolaysen, Die gemeinschaftsrechtliche Begründung von Grundrechten in EuR 2003, S. 719, 720 f.; vgl. auch Maurin, Slg. 1996, I-2909 Rn. 12; sowie 4. Teil. D. II. 2.) b).

[784] Krüger/Polakiewicz, Vorschläge für ein kohärentes System des Menschenrechtsschutzes in Europa in EUGRZ 2001, S. 92(99); Grabenwarter, EMRK, § 2 Rn. 14.

dass die nationalen Grundrechtskataloge einen weitergehenden Schutzumfang aufweisen können als die EMRK selbst.[785] Diese stellt demzufolge einen Mindeststandard dar.[786]

b) Übernahme der EMRK in nationales Recht

Die EMRK regelt nicht die Übernahme der Gewährleistungen der EMRK ins nationale Recht. Ein genereller Vorrang der EMRK vor nationalstaatlichem Recht konnte sich bisher ebenfalls nicht durchsetzen.[787] Die Mitgliedstaaten regeln die Durchsetzung der EMRK unterschiedlich. Es gibt dabei drei Gruppen von Ländern.[788] In einer Gruppe von Staaten genießt die EMRK Verfassungsrang.[789] In einer weiteren Gruppe steht die EMRK zwischen der Verfassung und den einfachen Gesetzen in einer Sonderrolle.[790] Schließlich gibt es Vertragsstaaten, in denen die EMRK im Rang eines einfachen Gesetzes steht.[791] In Deutschland steht die EMRK im Rang eines einfachen Gesetzes.[792]

c) Die EMRK im Unionsrecht

Die Europäische Union ist der EMRK gegenwärtig noch nicht beigetreten. Jedoch ist die EMRK Rechtserkenntnisquelle des Unionsrechts gemäß Art. 6 Abs. 3 EUV. Darüber hinaus stützen sich viele Grundrechte der Europäischen Grundrechtecharta unmittelbar auf die EMRK. Weiterhin sind alle Mitgliedstaaten der

---

785 Grabenwarter, EMRK, § 2 Rn. 14.

786 Grabenwarter, EMRK, § 2 Rn. 14.

787 Grabenwarter, EMRK, § 3 Rn. 1.

788 Eine Übersicht mit der Zuteilung der Vertragsstaaten in die jeweilige Kategorie findet sich bei Grabenwarter, EMRK, 4. Aufl., München 2009, § 3 Rn. 3 ff. ebenso bei Peters/Altwicker, Europäische Menschenrechtskonvention, § 1 Rn. 6.

789 Grabenwarter, EMRK, § 3 Rn. 1.

790 Grabenwarter, EMRK, § 3 Rn. 1.

791 Grabenwarter, EMRK, § 3 Rn. 1.

792 BVerfG NJW 2004, S. 3407 (3408); BVerfGE 74, S. 358, 370.

EU auch Vertragsparteien der EMRK. Darüber hinaus regelt Art. 52 GrCh das Verhältnis der Union zur EMRK.[793]

d) Die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte

Zum Verhältnis der EMRK zum Grundrechtsschutz der Union hat der EGMR im „Bosphorus" Urteil vom 30.06.2005 Stellung genommen. Demnach wird ein „äquivalenter" Grundrechtsschutz in der EG vermutet.[794]

e) Zwischenergebnis

Die EMRK als verpflichtendes Grundrechtsregime für die Mitgliedstaaten wie auch zumindest indirekt und mit einem Beitritt der Union zur EMRK direkt bindendes Grundrechtsregime für die EU stellt so einen Mindeststandard für den Grundrechtsschutz im gesamten europäischen Rechtsraum dar.[795]

4. Der Grundrechtsrahmen im europäischen Mehrebenensystem

Grundsätzlich ist jede Ebene an ihr eigenes und an höherrangiges Recht gebunden.[796] Jedoch kann im europäischen Mehrebenensystem nicht von einem absoluten Vorrang einer Ebene ausgegangen werden.[797] Kollisionen der Grundrechtssysteme sind grundsätzlich im Wege der praktischen Konkordanz aufzulösen.[798] Ist dies nicht möglich, sind zunächst im Falle einer Kollision der EMRK

---

793 Siehe 4. Teil. D. II. 2.) c).

794 EGMR „Bosporus" Urteil vom 30.06.2005 Nr. 45036/98 = EuGRZ 2007, S. 662 (667).

795 Schmahl, Grundrechtsschutz im Dreieck von EU, EMRK und nationalem Verfassungsrecht in EuR 2008 Heft Beiheft 1, S. 7, 25.

796 So auch Mehde, Gespaltener Grundrechtsschutz in der EU? in EuGRZ 2008, S. 269.

797 Uerpmann/Wittzack in v. Münch/Kunig, Grundgesetz, Art. 23 GG Rn. 36.

798 Vgl. von Danwitz in Tettinger/Stern, Europäische Grundrechtecharta, Art. 52 Rn. 20; Borowsky in Meyer, EU-GrCh, Art. 52 Rn. 20.

mit den deutschen Grundechten diese EMRK-freundlich auszulegen. Im Falle der Kollision der Grundrechte aus der Grundrechtecharta mit den deutschen Grundrechten wird die Verletzung von Grundrechten nach dem Grundgesetz so lange nicht vom Bundesverfassungsgericht überprüft, wie die Union einen gleichwertigen Schutz bietet.[799]

Kollidieret auf unionaler Ebene die Grundrechtecharta mit der EMRK, so ist auch hier zunächst die Grundrechtecharta EMRK-freundlich auszulegen. Der EGMR vermutet einen gleichwertigen Schutz der EU-Grundrechte. Das Verhältnis zwischen Grundrechtecharta und EMRK ist jedoch grundsätzlich als unproblematisch anzusehen, da sich die GrCh an vielen Stellen auf die EMRK stützt.[800]

III. Zwischenergebnis

Das vielschichtige Geflecht von Europäischer Menschenrechtskonvention, Grundrechtecharta sowie allgemeinen Grundsätzen, die jeweils sowohl die nationale als auch die europäische Ebene binden, und das Hinzutreten von nationalen im Grundgesetz verankerten Grundrechten verdeutlichen den Rechtsquellenpluralismus in der Union.[801] Gleichzeitig bilden sie den Versuch ab, einen flächendeckenden möglichst aufeinander aufbauenden und abgestimmten einheitlichen Grundrechtsschutz auf allen Ebenen zu gewährleisten.

Die legislativen Organe auf allen Ebenen sind aufgerufen, bei der Ausgestaltung von Legislativakten die Grundrechtetrias möglichst optimal zu beachten. Dies gilt ebenfalls für die Exekutive bei der Durchführung und Durchsetzung des Rechts. Die Rechtsprechung ist aufgerufen, die Gewährleistungsumfänge der verschiedenen Grundrechtssysteme möglichst aufeinander abzustimmen und zu harmonisieren. Im Konfliktfall bildet die EMRK einen Minimalstandard, in dessen Licht die übrigen Grundrechtsregime ausgelegt werden sollten. Solange

---

799 Vgl. 4. Teil. CD. II. 1.) b).

800 So auch Grabenwarter, EMRK § 3 Rn. 11 ff.

801 So auch Schorkopf in Grabitz/Hilf/Nettesheim, EUV, Art. 6 EUV Rn. 13.

die Grundrechtsgewährleistung auf unionaler Ebene dem Niveau der deutschen Grundrechte entspricht, werden diese durch das Bundesverfassungsgericht nicht an den deutschen Grundrechten gemessen. Der EuGH geht sogar von einem grundsätzlichen Vorrang der Unionsgrundrechte gegenüber nationalen Grundrechten gegenüber dem „Recht der Union“ aus.

So ist in Europa auf allen Ebenen ein flächendeckender Grundrechtschutz gegeben. Anhand des aufgezeigten Prüfungsmaßstabs können Grundrechtskollisionen weitestgehend aufgelöst werden.

E. Grundrechtsprüfung

Aufgrund des aufgezeigten Prüfungsmaßstabs ist es sinnvoll, mit der Prüfung des Mindeststandards der EMRK zu beginnen, im Anschluss mit der Prüfung der Grundrechtecharta fortzufahren und mit der Prüfung der Grundrechte nach dem Grundgesetz abzuschließen.

Des Weiteren ist nun der Prüfungsmaßstab für § 41a PostG festzulegen. In dieser Konstellation würde es sich um ein nationales Gesetz handeln. Es würde sich bei einer solchen Regelung zunächst um keine exakte Umsetzung eines Rechtsaktes der Union handeln. Folglich hätte hier der nationale Gesetzgeber mit eigenem Handlungsspielraum eine solche Norm erlassen. Im Verhältnis zwischen nationalen Grundrechten und der unionalen Ebene ergibt sich daraus, dass der nationale Gesetzgeber kein „Recht der Union" durchsetzte und die Grundrechte der Grundrechtecharta keine Anwendung fänden.[802] § 41a PostG wäre folglich an den nationalen Grundrechten zu messen. Daneben anwendbar bliebe die EMRK als europäischer Mindeststandard.

I. Grundrechte nach der EMRK

Nach der EMRK käme eine Verletzung des Rechts auf Achtung des Privat- und Familienlebens sowie der Achtung des Briefverkehrs und weiterer Kommunikationsformen aus Art. 8 EMRK durch § 41a PostG in Betracht.

1. Art. 8 EMRK, Recht auf Achtung des Privat- und Familienlebens

Gemäß Art. 8 EMRK hat jede Person *„das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz. (2) Eine Behörde darf in*

[802] Um auch die Konstellation einer exakten Umsetzung einer unionalen Regelung abzubilden und einen umfassenden Grundrechtsüberblick zu geben, werden im Folgenden auch die Grundrechte nach der Grundrechtecharta geprüft.

die Ausübung dieses Rechts nur eingreifen, soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer".

Art. 8 EMRK enthält eine Vielzahl voneinander unabhängiger, sich teilweise überschneidender Gewährleistungen, die Achtung des Privatlebens, die Achtung des Familienlebens, die Achtung der Wohnung sowie die Achtung des Briefverkehrs und weiterer Kommunikationsformen.[803] Für diese Arbeit sind die Gewährleistungen des Privatlebens sowie des Briefverkehrs und weiterer Kommunikationsformen relevant.

a) Die Achtung des Privatlebens

Art. 8 Abs. 1 EMRK statuiert die Achtung des Privatlebens. Bevor diese Sprachregelung gefunden wurde, war eine Formulierung im Gespräch, die der Allgemeinen Erklärung der Menschenrechte nachgebildet war, derzufolge niemand willkürlichen Eingriffen in sein Privatleben ausgesetzt sein darf.[804] Hiernach wurde eine deutliche Schutzpflicht des Staates deutlich, der Begriff der Achtung ist hingegen für eine Grundrechtsgewährleistung atypisch.[805]

aa) Schutzbereich

Zunächst müsste durch die Regelung des § 41a PostG der allgemeine Schutzbereich der Achtung des Privatlebens eröffnet sein.

---

803 Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 1.

804 Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 2.

805 So auch Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 1 f.

(1) Persönlicher Schutzbereich

Auf Beschränkungen im persönlichen Schutzbereich der EMRK wurde grundsätzlich verzichtet.[806] Entsprechend dem Wortlaut der Norm ist damit jede Person geschützt. Davon umfasst werden alle natürlichen Personen. Juristische Personen sind so weit berechtigt wie die Grundrechtsgewährleistungen auf sie anwendbar sind.[807] Aus dem Bereich des Privatlebens ist insbesondere der Datenschutz auf juristische Personen anwendbar.[808]

Von einem § 41a PostG oder einer vergleichbaren Regelung wären natürliche als auch juristische Personen betroffen, da ihre personenbezogenen Daten zwecks einer Risikoanalyse zur allgemeinen Gefahrenabwehr verarbeitet würden.

Der persönliche Schutzbereich von Art. 8 EMRK wäre damit eröffnet.

(2) Sachlicher Schutzbereich

Trotz der Formulierung „Achtung des Privatlebens“ handelt es sich zunächst um ein Abwehrrecht gegenüber staatlicher Gewalt.[809]

Grundsätzlich entzieht sich das Privatleben einer exakten allgemeingültigen Definition.[810] Unter Privatleben wird daher eine Sphäre verstanden, in der das Individuum sich frei entfalten und Kontakte jeglicher Art zu anderen Menschen aufnehmen kann, um so seine Persönlichkeit zu entwickeln und zu erfüllen.[811] Die Rechtsprechung hat das Recht auf Achtung des Privatlebens weiter präzisiert und drei Schutzbereiche formuliert: das Selbstbestimmungsrecht über den Körper, die freie Gestaltung der Lebensführung und den Schutz der Privatsphäre.[812]

---

806 So auch wohl Grabenwarter, EMRK, § 17 Rn. 1.

807 Grabenwarter, EMRK, § 17 Rn. 5.

808 Breitenmoser, Privatsphäre, S. 239 zitiert nach Grabenwarter, EMRK, § 22 Rn. 4.

809 Grabenwarter, EMRK, § 22 Rn. 1.

810 Bernsdorff in Meyer, EU-GrCh Art. 7 Rn. 19.

811 So auch Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 3.

812 Grabenwarter, EMRK, § 22 Rn. 6.

Auch berufliche Aktivitäten sollen zum Privatleben zählen.[813] Insbesondere gehört auch das Sammeln und Speichern von Daten über eine Person in den Schutzbereich des Privatlebens als Ausformung des Schutzes der Privatsphäre.[814] Weiterhin wird auch die individuelle Kommunikation von der Achtung des Privatlebens mitumfasst.[815] Die Kenntniserlangung und Verarbeitung von Informationen, die die Privatsphäre betreffen, werden von Art. 8 EMRK mit geschützt.[816]

Dem Staat kommt eine Schutzpflicht zu, entsprechende Rahmenbedingungen zu schaffen, dass das Privatleben – auch von Dritten – nicht beeinträchtigt wird.[817] Der Begriff der Achtung ist wohl schwächer zu interpretieren als die Einräumung eines konkreten Rechtes.[818]

Auch wenn es sich bei Art. 8 EMRK um kein Auffanggrundrecht im Sinne von Art. 2 Abs. 1 GG handelt und es deswegen keinen lückenlosen Schutz gewährleistet, wird über die Rückbindung an das Privatleben ein dynamischer Schutz entwickelt, der neuen Gefährdungslagen begegnet.[819]

Grundrechtsverpflichteter ist zunächst der Staat und nicht Private. Damit wäre die DPAG als Aktiengesellschaft nicht direkt Grundrechtsverpflichtete. Jedoch trifft den Staat eine Schutzpflicht, dass Dritte – hier die DPAG – das Privatleben der Grundrechtsträger nicht beeinträchtigen. Da Private wie auch berufliche Aktivitäten und damit auch private wie auch geschäftliche Kommunikation zum Privatleben gezählt werden, umfasst der Schutzbereich alle Postsendungen. Insbesondere werden in diesem Zusammenhang personenbezogene Daten vor

---

813 Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 3; so auch Grabenwarter, EMRK, § 22 Rn. 6.

814 Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 5; ähnlich EGMR, Leander/Schweden Urteil v. 26.03.1987 Rn. 48.

815 Klass ./. D, GH 28 = EUGRZ 1979, 278 ff. Rn. 41; Tettinger in Tettinger/Stern, Europäische Grundrechtecharta, 2006, Art. 7 Rn. 14.

816 Grabenwarter, EMRK, § 22 Rn. 10; ähnlich EGMR, Leander /Schweden Urteil v. 26.03.1987 Rn. 48.

817 Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 9.

818 Knecht in Schwarze (Hrsg.), EU-Kommentar, 3. Aufl., 2012, Art. 7 GrCh Rn. 6.

819 Grote/Marauhn, EMRK/GG Konkordanzkommentar, 2006, Kap. 16 Rn. 19.

Speicherung und Sammlung geschützt. Dies sind auch Vorgänge, die eine Risikoanalyse mitumfasst.

Folglich fiele eine Regelung wie § 41a PostG in den sachlichen Schutzbereich von Art. 8 EMRK.

Der Schutzbereich von Art. 8 EMRK wäre folglich eröffnet.

bb) Eingriffe in die Achtung des Privatlebens

Fraglich erscheint, ab welcher Intensität, ein Eingriff in die Achtung des Privatleben vorliegt.

Dies ist vor allem der Fall, wenn der Staat Regelungen für den Bereich des Privatlebens trifft.[820] Bringt die Person ihr Privatleben freiwillig in Kontakt mit dem öffentlichen Leben, wird in diesem Bereich ein Eingriff regelmäßig zu verneinen sein.[821] Als Eingriffe zu qualifizieren sind insbesondere Überwachungsmaßnahmen, auch in der Öffentlichkeit, das Mithören von Telefongesprächen sowie alle Abhörmaßnahmen im häuslichen Bereich.[822] Grundsätzlich sind Beeinträchtigungen der körperlichen Integrität auch unter der Schwelle von Art. 3 EGMR als Eingriffe zu werten.[823]

Im Bereich des Datenschutzes ist das Erheben, das Nutzen und das Verarbeiten personenbezogener Daten als Eingriff zu werten.[824]

Systematisch wohl eher ein Bestandteil der Rechtfertigung, wird ein Eingriff teilweise bei kollidierenden Interessen Anderer ausgeschlossen.[825]

---

820 Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 3.

821 Noch stärker von einen Nichtvorhandensein eines Eingriffs überzeigt ist Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 3 ff.

822 Malone ./. GB, GH 82, 30 = EUGRZ 1985 17, 20; Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 6.

823 Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 7.

824 Grabenwarter, EMRK, § 22 Rn. 26.

825 So wurde von der KOM ein Eingriff in die Achtung des Privatlebens durch Abtreibungsgesetze verneint, weil das ungeborene Leben als „Anderer" anzusehen sei. Zu der Problematik genauer siehe Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 4.

§ 41a PostG stellte eine Norm dar, die innerhalb eines Tatbestandes die Erhebung, Nutzung und Verarbeitung personenbezogener Daten erlaubte und so einen Bereich des Privatlebens regelte. Ein Eingriff läge damit durch eine Schutzpflichtverletzung des Gesetzgebers durch § 41a PostG unstrittig vor.

cc) Rechtfertigung von Eingriffen in die Achtung des Privatlebens

Ein Eingriff in die Achtung der Privatsphäre bedarf einer Rechtfertigung, die ihrerseits verhältnismäßig ist.

(1) Qualifizierter Gesetzesvorbehalt

Die Achtung des Privatlebens gemäß Art. 8 Abs. 1 EMRK unterliegt einem qualifizierten Gesetzesvorbehalt in Art. 8 Abs. 2 EMRK. Demnach dürfen Behörden nur aufgrund einer gesetzlichen Ermächtigung eingreifen, wenn die Maßnahme eine der in Art. 8 Abs. 2 EMRK genannten Voraussetzungen erfüllt.[826] Insbesondere zum Schutz der nationalen Sicherheit kann die Verarbeitung personenbezogener Daten geboten sein, auch ohne die betroffene Person davon in Kenntnis zu setzen.[827] Die öffentliche Sicherheit, die Aufrechterhaltung der Ordnung, Maßnahmen zur Verhütung von Straftaten sowie Schutz der Rechte und Freiheiten anderer können dabei ineinandergreifen.[828]

Im datenschutzrechtlichen Bereich sind besonders hohe Anforderungen an eine Ermächtigungsgrundlage für eine Datenerhebung, Verarbeitung und Nutzung, die im Geheimen stattfinden, zu stellen.[829]

Fraglich erscheint, in welchem Verhältnis § 41a PostG zu Art. 8 Abs. 2 EMRK stünde. Dieser stellt einen qualifizierten Gesetzesvorbehalt für das Handeln von Behörden auf. § 41a PostG gälte jedoch nur für das Verhältnis von Privaten untereinander. Diese Konstellation der Verletzung positiver Pflichten löst der EGMR

826 Alle Voraussetzungen sind in der Einleitung aufgeführt, 4. Teil. E. I. 1.).

827 Klass ./. D, GH 28, = EUGRZ 1979, 278 Rn. 48.

828 Siehe Klass ./. D, GH 28, 22 = EUGRZ 1979, 278 Rn. 48.

829 Grabenwarter, EMRK, § 22 Rn. 39.

durch eine Verhältnismäßigkeitsprüfung, in deren Rahmen der Qualifikationstatbestand auch von Bedeutung ist.[830] Jedoch handelt es sich um einen Bereich der Gefahrenabwehr, der grundsätzlich in den staatlichen Handlungsbereich fällt. Dem Gesetzgeber würde eine solche Ermächtigung die Möglichkeit geben, aus den strengeren Vorgaben des qualifizierten Gesetzesvorbehalts zu flüchten.

Eine Entscheidung der Problematik dürfte unnötig sein, erfüllte § 41a PostG die Vorgaben von Art. 8 Abs. 2 EMRK.

Die Verfassungsmäßigkeit des Gesetzgebungsverfahrens wäre zu unterstellen. Des Weiteren müsste § 41a PostG in einer demokratischen Gesellschaft notwendig sein für die *„nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer“*.

Die Risikoanalyse in § 41a PostG diente dem Wortlaut nach der Abwehr erheblicher Gefahren für das Gemeinwohl, die öffentliche Sicherheit oder die postalische Lieferkette. Damit wäre bereits im Ermächtigungstatbestand die öffentliche Sicherheit als Motiv und Voraussetzung zitiert. Eine solche Gefahrenabwehr überschneidet sich dabei auch mit der Verhütung von Straftaten und schützt mit der Kommunikation auch das wirtschaftliche Wohl des Landes und die Rechte und Freiheiten der Benutzer des Universaldienstes.

(2) Schranken-Schranken

Die Anforderungen an die Verhältnismäßigkeit steigen mit der Intensität des Eingriffes. Bei staatlichen Maßnahmen müssen insbesondere Maßnahmen ergriffen werden, die vor Missbrauch schützen.[831] Weiterhin muss für eine Rechtfertigung das Kriterium der *„Notwendigkeit in einer demokratischen Gesellschaft“* erfüllt sein. Hierbei handelt es sich um einen besonderen Maßstab, der bei der Prüfung

---

[830] Pätzold in Karpenstein/Mayer EMRK Art. 8 EMRK, 2012 München Rn. 100; EGMR Urt. v. 16.12.2010-25579/05 = NJW 2011, S. 2107(2108); EGMR, Urt. v. 08.07.2003 – 36022/97 = NVwZ 2004, S. 1465 (1467).

[831] Klass ./. D, GH 28, 22 = EUGRZ 1979, S. 278, 283.

der Verhältnismäßigkeit anzulegen ist.[832] Über die Anforderungen an eine reine Zweckmäßigkeit hinaus soll es hier zu einer fairen Abwägung der betroffenen individuellen Rechtsgüter und der Interessen der Allgemeinheit kommen.[833]

Bei der Heranziehung der in Art. 8 Abs. 2 EMRK genannten Voraussetzungen ist ebenfalls die Qualität der Beeinträchtigung ins Verhältnis zu setzen. Dabei können mehrere Rechtfertigungsgründe betroffen sein.

Der Schutz der nationalen Sicherheit kann rechtfertigen, dass eine Datenverarbeitung personenbezogener Daten ohne Einsichtsmöglichkeit des Betroffenen geboten erscheint.[834]

Das Recht auf Achtung des Privatlebens ist in einer Verhältnismäßigkeitsprüfung mit den Sicherheitsinteressen der Allgemeinheit abzuwägen.[835]

Mit dem Schutz vor erheblichen Gefahren für das Gemeinwohl, die öffentliche Sicherheit sowie die postalische Lieferkette werden legitime Ziele der Allgemeinheit verfolgt, die weitgehend mit dem qualifizierten Gesetzesvorbehalt in Art. 8 Abs. 2 EMRK übereinstimmen.

Die Maßnahme müsste weiterhin geeignet sein, die verfolgten Ziele zu erfüllen. Dafür müsste § 41a PostG die Zwecke zumindest fördern.

Die Datenverarbeitung zwecks Risikoanalyse ist geeignet potenzielle Gefahren für die postalische Lieferkette zu identifizieren, und schafft damit erst die Grundlage, diesen Gefahren zu begegnen. Damit wäre § 41a PostG geeignet, die verfolgten Ziele zu fördern.

Weiterhin müsste die Datenverarbeitung in § 41a PostG erforderlich sein. Dafür müsste es sich um die mildeste gleichgeeignete Maßnahme handeln. Der

---

832 Tettinger in Tettinger/Stern, Europäische Grundrechtecharta, 2006, Art. 7 Rn. 51 f.

833 Vgl. auch Grabenwarter, EMRK, § 22 Rn. 42; Tettinger in Tettinger/Stern, Europäische Grundrechtecharta, 2006, Art. 7 Rn. 51 f.

834 Grabenwarter, EMRK, § 22 Rn. 41; ähnlich Klass ./. D, GH 28, 22 = EUGRZ 1979, 278 Rn. 48.

835 Aufgrund der weitgehenden Überschneidung der Rechtfertigungsanforderungen, besonders von Art. 8 EMRK und Art. 7 und 8 GrCh wird an dieser Stelle die Verhältnismäßigkeitsprüfung exemplarisch durchgeführt, um bei den weiteren Grundrechten hierauf zu verweisen und ggf. Abweichungen zu untersuchen.

Status quo, ohne Datenverarbeitung auskommend, bietet ein niedrigeres Schutzniveau, potenzielle Risiken zu erkennen, da er sich ausschließlich auf die Identifizierung von Risiken durch Personal stützt, das eine umfassende Untersuchung jedes Paketes nicht leisten kann. Wie ohne eine Datenverarbeitung potenzielle Risiken persönlichkeitsrechtsschonender identifiziert werden könnten, ist nicht ersichtlich. Die Notwendigkeit heimlicher Überwachungen, um Bedrohungen der öffentlichen Sicherheit zu begegnen, hat der EMRK bereits 1979 festgestellt: *„Der Gerichtshof muss daher einräumen, dass das Bestehen von gesetzlichen Bestimmungen, die zur geheimen Überwachung des Briefverkehrs, der Postsendungen und des Telefonverkehrs ermächtigen, in einer demokratischen Gesellschaft bei einer außergewöhnlichen Situation zum Schutze der nationalen Sicherheit und oder/zur Sicherung der Ordnung sowie zur Verhütung von strafbaren Handlungen notwendig ist.“*[836]

Eine physische Inspektion jeder Sendung – unter wirtschaftlichen Gesichtspunkten kaum zu leisten – würde zu einem viel intensiveren Eingriff in die Rechte des Einzelnen führen. Damit wäre die Datenverarbeitung gemäß § 41a PostG auch die mildeste gleichgeeignete Maßnahme.

Schließlich müsste § 41a PostG angemessen bzw. verhältnismäßig im engeren Sinne sein. Dafür dürfte die Achtung des Privatlebens die Sicherheitsinteressen der Allgemeinheit nicht überwiegen. Die Intensität des Erlaubnistatbestandes ist dabei mit dem potenziellen Sicherheitsgewinn abzuwägen. Hinsichtlich der Ausgestaltung von Überwachungsmaßnahmen, ist dem Gesetzgeber ein gewisser Ermessensspielraum zugestanden.[837] Dabei sind insbesondere die verankerte Verhältnismäßigkeitsprüfung der Maßnahme selbst sowie die verankerten Grundsätze der Datensparsamkeit und Datenvermeidung zu berücksichtigen („[…] *sofern das Interesse der Betroffenen nicht überwiegt und der Zweck nicht auf andere Weise oder nur mit unverhältnismäßigen Aufwand erreicht werden kann. Das Erheben, Verarbeiten und Nutzen von Daten zu diesem Zweck hat unter Beachtung der allgemeinen Grundsätze, insbesondere der Datensparsamkeit und Datenvermei-*

836 Klass ./. D, GH 28, 21 = EUGRZ 1979, S. 278 ff. Rn. 48.

837 Klass ./. D, GH 28, 21 = EUGRZ 1979, S. 278 ff. Rn. 49.

dung, zu erfolgen"). Die Datenverarbeitung zwecks Risikoanalyse wird so nicht pauschal erlaubt, sondern ist nur in engen Grenzen zulässig. Die persönlichen Daten sollen so wenig wie möglich verwendet werden und der Eingriff in das Privatleben damit so gering wie möglich ausfallen. Die Identifikation von Gefahren soll so sichergestellt werden, wobei die Datenverarbeitung in einem ausgewogenen Verhältnis zum Sicherheitsgewinn und damit zu einer erhöhten Identifikation von Gefahrenquellen stehen muss.

Folglich ist die Intensität der Datenverarbeitung, unter Berücksichtigung der Verhältnismäßigkeit und der Datenschutzgrundsätze, als verhältnismäßig zum Eingriff in die Achtung des Privatlebens einzuschätzen.

Der Erlaubnistatbestand von § 41a PostG wäre damit verhältnismäßig.

dd) Zwischenergebnis

Der Eingriff durch § 41a PostG in den Schutzbereich der Achtung des Privatlebens wäre gerechtfertigt und Art. 8 EMRK nicht verletzt.

b) Die Achtung des Briefverkehrs und weiterer Kommunikationsformen

Weiterhin umfasst Art. 8 Abs. 1 EMRK die Achtung des Briefverkehrs wie auch weiterer Kommunikationsformen.

aa) Schutzbereich

Zunächst müsste auch hier der Schutzbereich eröffnet sein.

(1) Persönlicher Schutzbereich

Der persönliche Schutzbereich schützt alle natürlichen Personen. Der Schutz juristischer Personen ist ebenfalls umfasst und kommt besonders in den Bereichen des Briefverkehrs und der Kommunikation zum Tragen.[838]

[838] Grabenwarter, EMRK, § 22 Rn. 4.

Der persönliche Schutzbereich der Achtung der Kommunikation umfasst den Schutz natürlicher und juristischer Personen, die von § 41a PostG betroffen wären.

(2) Sachlicher Schutzbereich

Der Schutzbereich des Briefverkehrs umfasst zunächst die schriftliche Mitteilung.[839] Diese genießt Schutz, wenn ein anerkannter und geordneter Beförderungsweg gewählt wird.[840] Der Schutzbereich wurde mit Blick auf die ehemals staatlichen Postunternehmen formuliert, heute werden jedoch auch äquivalente Kommunikationssysteme – unabhängig davon, ob diese staatlich oder privat betrieben werden – anerkannt und vom Schutzbereich umfasst.[841]

Auch Telefongespräche sind vom Schutzbereich umfasst.[842] Deswegen wird man den Begriff der anderen Kommunikationsformen weit und offen für Innovationen auslegen müssen.[843] Ein effektiver Schutz setzt voraus, dass bei der rasanten technischen Entwicklung auch E-Mails, E-Postbriefe und weitere neue Kommunikationswege ebenfalls vom Schutzbereich umfasst werden.[844]

Gerade durch die Privatisierungen im postalischen Bereich wandelt sich der Schwerpunkt des Schutzbereichs in besonderer Weise in einen Schutzauftrag, die gesetzlichen Rahmenbedingungen so zu gestalten, dass die Kommunikation des Einzelnen geschützt wird.

Der Kommunikationsweg des Universaldienstes wird vom Schutzbereich mitumfasst; es ist unerheblich, ob der Kommunikationsweg von staatlicher oder privater Stelle betrieben wird. Dabei werden neben schriftlichen Mitteilungen auch neue Kommunikationsformen mitgeschützt. Fraglich erscheint, ob vom Schutzbereich auch Postsendungen geschützt werden, die Waren zu kommer-

---

839 Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 34.

840 Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 34.

841 Frowein in Frowein/Peukert, EMRK-Kommentar, Art. 8 EMRK Rn. 34.

842 Klass ./. D, GH 28, 21 = EUGRZ 1979, 278 Rn. 41; Malone ./. GB, GH 82, 30 = EUGRZ 1985 17, 20.; Lüdi ./. Ch, GH 238, 19 = EuGRZ 1992, S. 300 (301).

843 Im Ergebnis auch Grabenwarter, EMRK, § 22 Rn. 35 f.

844 So auch Grabenwarter, EMRK, § 22 Rn. 35.

ziellen Zwecken enthalten. Geschützt werden soll die Kommunikation, also ein Informationsaustausch zwischen Personen. Ein Schutz von Transport und Handel ist davon wohl nicht umfasst. Jedoch enthalten wohl auch Warensendungen Informationen (z. B. eine Rechnung, Warenbeschreibung etc.) und stellen damit auch eine Form von Kommunikation dar. Eine Abgrenzung erscheint kaum möglich. Damit sind alle Arten von Postsendungen in den Schutzbereich einzubeziehen. Geschützt wird damit auch der gesamte Rahmen der Kommunikation und folglich auch die personenbezogenen Daten, die mit einer Postsendung verbunden sind.

bb) Eingriffe in die Achtung des Briefverkehrs und weiterer Kommunikationsformen

Als einen Eingriff wird man jede Beeinträchtigung des Kommunikationsweges ansehen müssen. Insbesondere die Kenntnisnahme von Informationen, – sei es über den Inhalt der Kommunikation oder über den Kommunikationsvorgang selbst – muss als Eingriff zu werten sein.

Besonders als Eingriff zu qualifizieren sind Maßnahmen wie die Zensur von Briefen sowie deren Kontrolle, Anhalten oder verzögerte Weitergabe.[845] *„Hierunter fallen das Öffnen, das Lesen, und Kopieren von Briefen, das Löschen bestimmter Stellen in Briefen, Genehmigungsvorbehalte, Beschränkungen der Zahl oder Länge von Briefen oder Verzögerungen bei der Übermittlung.“*[846]

§ 41a PostG würde eine Kenntnisnahme und Verarbeitung von Daten erlauben, die unmittelbar mit der Sendung wie auch dem Kommunikationsvorgang selbst in Verbindung stehen und für diesen benötigt werden. Damit könnte eine Schutzpflichtverletzung des Gesetzgebers durch § 41a PostG vorliegen.

[845] Grabenwarter, EMRK, § 22 Rn. 31.

[846] Grabenwarter, EMRK, § 22 Rn. 35.

cc) Rechtfertigung von Eingriffen in die Achtung des Briefverkehrs und weiterer Kommunikationsformen

Ein Eingriff in die Achtung des Briefverkehrs und weiterer Kommunikationsformen bedarf einer Rechtfertigung, die ihrerseits verhältnismäßig ist.

(1) Qualifizierter Gesetzesvorbehalt

Die Achtung des Briefverkehrs und anderer Kommunikationsformen unterliegt ebenfalls einem qualifizierten Gesetzesvorbehalt.[847] Für die Achtung des Briefverkehrs hat der EGMR besondere Vorgaben für die Regelungsdichte und Regelungsqualität entwickelt.[848] Auch wenn die Rechtsgrundlage nicht zwingend ein Gesetz sein muss, so ist im Hinblick auf das Erfordernis der Vorhersehbarkeit *„jedoch erforderlich, dass Vorschriften, die den Behörden einen Ermessenspielraum zubilligen, nicht nur benennen, wer in seiner Kommunikation kontrolliert werden kann und welche Stellen über diese Kommunikation entscheiden, sondern darüber hinaus regeln, in welcher Art und Weise, für welche Dauer und aus welchen Gründen die Kontrolle, die im Einzelfall zu begründen ist, durchgeführt werden kann".*[849]

Zunächst gilt auch für die Achtung des Briefverkehrs für die Verletzung positiver Pflichten die Einhaltung des Qualifikationstatbestandes.[850] Die besondere Regelungsdichte bezieht sich auf die Kontrolle von Sendungen, jedoch wäre bereits für die Datenverarbeitung ein Erlaubnistatbestand durch ein Gesetz geschaffen, welcher den Zweck der Erlaubnis bennent und eine Verhältnismäßigkeitsprüfung für den Einzelfall vorsieht.

---

847 Siehe 4. Teil. D. I. 1.) a) cc) (1).

848 EGMR, Urteil vom 25.03.1983, „Silver". Grabenwarter, EMRK, § 22 Rn. 37.

849 Grabenwarter, EMRK, § 22 Rn. 37; in der Fn. dazu gibt es ausführliche Hinweise auf die Rechtsprechung.

850 Vgl. 4. Teil. D. I. 1.) a) cc) (1).

(2) Schranken-Schranken

Die Verhältnismäßigkeitsprüfung richtet sich grundsätzlich nach dem Maßstab wie für die Achtung des Familienlebens.[851] Dabei ist das Sicherheitsinteresse der Allgemeinheit mit der Achtung des Briefverkehrs abzuwägen.

Bezüglich der Prüfung des legitimen Zweckes, der Geeignetheit und der Erforderlichkeit ist auf die Prüfung der Achtung des Privatlebens zu verweisen, da diesen Überlegungen der gleiche Maßstab und die gleichen Wertungen zugrunde liegen. Weiterhin wäre § 41a PostG angemessen, wenn das Sicherheitsinteresse der Allgemeinheit den Schutz der Achtung des Briefverkehrs übersteigt.

Für den Umgang mit dem Einzelfall hat sich bereits durch Rechtsprechung und Lehre ein recht detaillierter Beurteilungsmaßstab herausgebildet. So muss im Einzelfall eine hinreichend konkrete Gefährdung bestehen.[852] Für eine Überwachung der Kommunikation müssen so hinreichend gewichtige Anhaltspunkte für eine Straftat vorliegen.[853] Drohende Terroranschläge rechtfertigen durch einen pauschalen Verweis auf die Verteidigung der Demokratie dabei nicht jede Maßnahme.[854] Es gilt dabei: Je stärker die Bedrohung ist, desto geringere Anhaltspunkte genügen.[855] Im Umkehrschluss muss dann gelten: Je geringer die Belastung ist, desto höher sind der Rechtfertigungsdruck und die Auflagen. Ein solcher „Einzelfallmaßstab" lässt sich nur bedingt auf eine generalisierte Überwachung übertragen. Der Maßstab für eine generalisierte Überwachung muss der Tatsache Rechnung tragen, dass der gesamte Sendungsstrom überwacht werden muss und deswegen die Daten aller Postsendungen verarbeitet werden. Bezüglich der Datenverarbeitung führt der Anknüpfungspunkt an tatsächliche hinreichende Anhaltspunkte daher nicht weiter.[856] Frenz führt richtig aus; *„Die an Überwa-*

---

851 Vgl. 4. Teil. D. I. 1.) a) cc) (2).

852 Frenz, Handbuch Europarecht, Bd. 4, § 4 Rn. 1340.

853 Frenz, Handbuch Europarecht, Bd. 4, § 4 Rn. 1340.

854 NJW 1979, S. 1755 (Klaas); Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1340.

855 Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1349; NJW 2007, 1433 (1439) Webner u. Saravia/Deutschland.

856 Dazu ausfürlicher unter Art. 10; 4. Teil. D. III. 3.) c) bb).

chungsmaßnahmen der Kommunikation zu stellenden Anforderungen dürfen deshalb nicht derart starr gehandhabt werden, dass solche Gefahren [Terror] praktisch kaum aufgedeckt und damit abgewehrt werden können.“[857]

Die Nutzung des Briefverkehrs hängt in hohem Maße von dessen Vertraulichkeit ab. Der Eindruck der Überwachung und der Nachvollziehbarkeit von Kommunikation kann sich hemmend auf die Kommunikation des Einzelnen auswirken. Die Überwachung des Briefverkehrs muss daher so ausgestaltet sein, dass der Einzelne in seinem Kommunikationsverhalten nicht beeinflusst wird. Es muss sichergestellt sein, dass die Datenverarbeitung ausschließlich – und nur soweit notwendig – zu den benannten Zwecken vorgenommen wird und nicht anderweitig genutzt werden kann. Mit der Erfordernis der Verhältnismäßigkeit der Maßnahmen und der verankerten Grundsätze der Datenvermeidung und Datensparsamkeit trüge § 41 a PostG diesen Anforderungen Rechnung und wäre folglich angemessen.

§ 41a PostG wäre damit verhältnismäßig.[858]

dd) Zwischenergebnis

Der Eingriff durch § 41a PostG in den Schutzbereich der Achtung des Briefverkehrs wäre gerechtfertigt und Art. 8 EMRK nicht verletzt.

2. Zwischenergebnis

§ 41a PostG würde Art. 8 EMRK weder in der Achtung des Privatlebens noch in der Achtung des Briefverkehrs verletzen. Grundrechte nach der Europäischen Konvention für Menschenrechte wären demnach nicht verletzt.

---

857 Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1351.

858 Für weitere Argumente wird ebenfalls auf die Verhältnismäßigkeitsprüfung der Achtung des Privatlebens verwiesen, 4. Teil. D. I. 1.) a) cc) (2).

II. Grundrechte nach der Europäischen Grundrechtecharta

Nach der Europäischen Grundrechtecharta käme eine Verletzung der Achtung des Privat- und Familienlebens aus Art. 7 GrCh sowie des Schutzes personenbezogener Daten aus Art. 8 GrCh durch Art 41a PostG in Betracht.

1. Art. 7 GrCh, Achtung des Privat- und Familienlebens

Gemäß Art. 7 GrCh hat jede Person *„das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation"*.

Art.7 GrCh ist im Wesentlichen Art. 8 EMRK nachgebildet und soll dessen Gewährleistungsumfang entsprechen.[859] Die informationelle Selbstbestimmung hat bereits durch richterliche Rechtsfortbildung Grundrechtsqualität erlangt.[860] Art. 7 GrCh umfasst ebenso wie Art. 8 EMRK die vier Teilbereiche der Achtung des Privatlebens, des Familienlebens, der Wohnung sowie der Kommunikation. Gemeinsam bilden diese *„eine umfassende Garantie eines Freiraums des Individuums, der für die freie Entfaltung jeder Persönlichkeit unabdingbar ist"*.[861] Für diese Bearbeitung ist die Achtung des Familienlebens sowie der Kommunikation von Relevanz.

a) Achtung des Familienlebens

Die Achtung des Familienlebens ist Art. 8 EMRK nachgebildet. Damit entspricht sie zwar dessen Wortlaut, weicht jedoch mit der Formulierung „Achtung" von

---

859 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.; Bernsdorff in Meyer, EU-GrCh, Art. 7 Rn. 1.

860 Bernsdorff in Meyer, EU-GrCh, Art. 8 Rn. 14; Zur Rechtsprechung dazu siehe Bernsdorff in Meyer, EU-GrCh, Art. 8 Rn. 14, Fn. 87.

861 Tettinger in Tettinger/Stern, Europäische Grundrechtecharta, 2006, Art. 7 Rn. 8; Grabenwarter, EMRK, § 22 Rn. 1; vgl. auch Stern, Der allgemeine Privatsphärenschutz durch das Grundgesetz und seine Parallelen im internationalen und europäischen Recht in Festschrift für Georg Ress, 2005, S. 1259 (1272 ff.).

der Struktur der anderen Grundrechte der Grundrechtecharta ab.[862] Es handelt sich dabei um kein Auffanggrundrecht der allgemeinen Handlungsfreiheit wie in Art. 2 Abs. 1 GG.[863]

aa) Schutzbereich

Zunächst müsste durch die Regelung des § 41a PostG der allgemeine Schutzbereich der Achtung des Familienlebens eröffnet sein.

(1) Persönlicher Schutzbereich

Gemäß Art. 7 GrCh hat jede Person die gewährten Rechte. Davon unbestritten umfasst sind alle natürlichen Personen.[864]

Der Schutz juristischer Personen ist umstritten. Einen Schutz wird man wohl so weit annehmen können wie er funktional denkbar ist.[865] Logisch ausgeschlossen ist er zum Beispiel bei der Achtung des Familienlebens.[866]

Die Verwendung personenbezogener Daten natürlicher Personen zwecks Risikoanalyse fällt unstrittig in den Schutzbereich von Art. 7 GrCh.[867] Bezüglich des Schutzes juristischer Personen ist eine parallele Gefährdungslage durch Datenverarbeitung wie bei natürlichen Personen gegeben. Das Kontrollpotenzial und die Auswirkungen auf das Kommunikationsverhalten einer juristischen Person sind potenziell ähnlich. Zudem ist der Schutzbereich Art. 8 EMRK nachgebildet, der ebenfalls den Schutz juristischer Personen annimmt.

---

862 So auch Bernsdorff in Meyer, EU-GrCh, Art. 7 Rn. 16.

863 Grabenwarter, EMRK, § 22 Rn. 1.

864 Kingreen in Callies/Ruffert, EUV-AEUV, Art. 7 GrCh Rn. 11.

865 Knecht in Schwarze, EU, Art. 7 GrCh Rn. 4; Bernsdorff in Meyer, EU-GrCh, Art. 7 Rn. 25; ebenfalls für einen Schutz Tettinger in Tettinger/Stern, Europäische Grundrechtecharta, Art. 7 Rn. 9.

866 Knecht in Schwarze, EU, 2012, Art. 7 GrCh Rn. 4.

867 Vgl. auch 4. Teil. D. I. 1.) a) aa) (1).

(2) Sachlicher Schutzbereich

Zunächst ist auch der sachliche Schutzbereich der Achtung des Privatlebens an Art. 8 EMRK auszurichten.[868] Darüber hinaus ist er wohl nicht allgemeingültig zu definieren und mehr als ein bloßes Recht, „nicht belästigt zu werden".[869] Für den EGMR stellt die „Nicht-Öffentlichkeit" ein wichtiges Kriterium für das Bestehen von Privatheit dar mit der Folge, dass ein Öffentlichkeitsbezug einen Ausschluss des Schutzbereichs herbeiführen kann.[870] Dabei handelt es sich wohl jedoch um eine Trennung, die angesichts zahlreicher Interaktionen in sozialen Netzwerken so weit verschwommen ist, dass sie heute, streng angewendet, wohl zu einer Aushöhlung des Grundrechtsschutzes führen würde. Denn die Kommunikation stellt eine wichtige Ausdrucksform des Privatlebens dar.[871]

Der Begriff der Achtung ist in Anlehnung an die Formulierung in der EMRK gewählt und ist damit auch schwächer zu werten als der Begriff des „Rechts", wodurch den Mitgliedstaaten auch ein weiterer Beurteilungsspielraum zukommt.[872]

Die Rechtsprechung hat durch die Herausbildung geschützter Bereiche den Begriff des Privatlebens weiter präzisiert. So sind das Selbstbestimmungsrecht über den Körper, die Privatsphäre sowie die freie Gestaltung der Lebensführung vom Schutzbereich des Privatlebens mitumfasst.[873] Selbst die geschäftlichen und beruflichen Beziehungen sind in den Schutzbereich des Privatlebens einbezogen, da bei zwischenmenschlichen Beziehungen eine Trennung kaum möglich wäre.[874]

---

868 Siehe 4. Teil. D. I. 1.) a) aa) (2).

869 Bernsdorff in Meyer, EU-GrCh, Art. 7 Rn. 19.

870 Bernsdorff in Meyer, EU-GrCh, Art. 7 Rn. 19; wohl anders auch Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1182.

871 So auch Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1181.

872 So auch wohl Knecht in Schwarze, EU, 2012, Art. 7 GrCh Rn. 6; genauer dazu Tettinger in Tettinger/Stern, Europäische Grundrechtecharta, 2006, Art. 7 Rn. 5; Bernsdorff in Meyer, EU-GrCh, Art. 7 Rn. 16.

873 Tettinger in Tettinger/Stern, Europäische Grundrechtecharta, 2006, Art. 7 Rn. 10 ff.

874 EGMR Urt. v. 16.12.1992, Nr. 13710/88 (Rn. 29), NJW 1993, 718 (718 f.) Niemietz/Deutschland; Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1203.

Durch die Parallelität des Grundrechtsschutzes mit Art. 8 EMRK werden über den Schutz der Privatsphäre auch die individuelle Kommunikation sowie der personenbezogene Datenschutz von der Achtung des Privatlebens mitgeschützt, obwohl Art. 8 GrCh hier spezieller ist.[875] Insoweit kommt es hier zu einer Überschneidung bzw. Dopplung des Schutzes.

Wie schon in Art. 8 EMRK umfasst der Schutzbereich neben einem Abwehrrecht gegenüber dem Staat auch eine Schutzpflicht, das Familienleben gegenüber Dritten – wie hier Postdienstleistern – zu schützen. In den Bereich der Schutzpflicht fiele auch § 41a PostG. Geschützt werden hier parallel zu Art. 8 EMRK die personenbezogenen Daten, die im Zusammenhang mit einer Postsendung als Teil der individuellen Kommunikation stehen.

bb) Eingriff in die Achtung des Privatlebens

Ein Eingriff in die Achtung des Privatlebens kann durch ein Handeln oder auch ein Unterlassen vorliegen.[876] Beeinträchtigungen können durch eine Unterlassungspflicht oder die Nichterfüllung einer Schutzpflicht vorliegen.[877]

Den Eingriff durch § 41a PostG würde die Nichterfüllung einer Schutzpflicht durch eine unzureichende Ausgestaltung der Ermächtigungsgrundlage darstellen.

cc) Rechtfertigung von Eingriffen in die Achtung des Privat- und Familienlebens

(1) Qualifizierter Gesetzesvorbehalt

Gemäß Art. 52 Abs. 3 GrCh richten sich die möglichen legitimen Einschränkungen ebenfalls nach Art. 8 EMRK.[878] Damit handelt es sich hier ebenfalls um einen qualifizierten Gesetzesvorbehalt mit den Schranken des Art. 8 Abs. 2 EMRK.

---

875 Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1183; Tettinger in Tettinger/Stern, Europäische Grundrechtecharta, 2006, Art. 7 Rn. 14 f.

876 Bernsdorff in Meyer, EU-GrCh, Art. 7 Rn. 17.

877 Bernsdorff in Meyer, EU-GrCh, Art. 7 Rn. 17.

878 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

Der EuGH hat in der Vergangenheit einen Maßstab angewendet, der Eingriffe als gerechtfertigt ansah, soweit diese dem Gemeinwohl geschuldet waren und das Grundrecht nicht in seinem Wesensgehalt angetastet haben.[879]

Damit sind bei einem Eingriff dieselben Wertungen zu ziehen wie bei Art. 8 EMRK.[880] Folglich wären die Anforderungen des qualifizierten Gesetzesvorbehalts auch gegenüber der Achtung des Familienlebens gemäß Art. 7 GrCh durch § 41a PostG erfüllt.

(2) Schranken-Schranken

Die Rechtfertigungsvoraussetzungen von Art. 8 Abs. 2 EMRK sind als Maßstab für eine Verhältnismäßigkeitsprüfung anzulegen.

Entsprechend der Verhältnismäßigkeitsprüfung im Rahmen von Art. 8 EMRK wäre § 41a PostG auch gegenüber der Achtung des Familienlebens verhältnismäßig.[881]

dd) Zwischenergebnis

Der Eingriff durch § 41a PostG in den Schutzbereich der Achtung des Familienlebens wäre gerechtfertigt.

b) Achtung der Kommunikation

Die Achtung der Kommunikation aus Art. 7 GrCh könnte durch § 41a PostG ebenfalls verletzt sein.

aa) Schutzbereich

So könnte der Schutzbereich der Achtung der Kommunikation durch § 41a PostG eröffnet sein.

---

879 So bei EuGH, Rs. 265/87, Schräder/Hauptzollamt Gronau, Slg 1989, 2268 Rn. 15; Kommission/Bundesrepublik, Slg. 1992, I-2601, 2609 Rn. 23; Knecht in Schwarze, EU, 2012, Art. 7 GrCh Rn. 11.

880 Vgl. 4. Teil. D. I. 1.) a) cc).

881 Vgl. 4. Teil. D. I. 1.) a) cc) (2).

(1) Persönlicher Schutzbereich

Der persönliche Schutzbereich der Achtung der Kommunikation ist ebenfalls Art. 8 EMRK nachgebildet und hat den gleichen Gewährleistungsumfang wie die Achtung des Privatlebens.[882] Die Achtung der Kommunikation wird aufgrund einer ähnlichen Gefährdungslage auch auf juristische Personen angewendet.[883]

Der persönliche Schutzbereich der Achtung der Kommunikation ist somit sowohl für natürliche als auch für juristische Personen eröffnet.

(2) Sachlicher Schutzbereich

Dem Gewährleistungsumfang von Art. 8 EMRK entsprechend umfasst die Achtung der Kommunikation das Brief-, Post- und Fernmeldegeheimnis sowie „neuere" Kommunikationsformen wie E-Mails und SMS.[884] Er ist dabei weit zu verstehen und offen für neue Kommunikationsformen.[885] Als Fernkommunikation ist auch der Austausch unter Benutzung einer – womöglich von einem Dritten beherrschten – technischen Einrichtung vom Schutzbereich mitumfasst.[886]

In Abgrenzung zu Art. 11 GrCh wird hier nur der Übermittlungsvorgang selbst geschützt.[887]

§ 41a PostG lässt die Verwendung personenbezogener Daten zu, die unmittelbar mit dem Übermittlungsvorgang im Zusammenhang stehen. Damit ist der Übermittlungsvorgang betroffen und der sachliche Schutzbereich wäre eröffnet.

---

882 Vgl. 4. Teil. D. I. 1.) a) aa) (1).

883 Grabenwarter, EMRK, § 22 Rn. 4; Knecht in Schwarze (Hrsg.), EU-Kommentar, 3. Aufl., 2012, Art. 7 GrCh Rn. 4.

884 Vgl. Kugelmann, EuGRZ 2003, S. 16 (22); Kingreen in Callies/Ruffert, EUV-AEUV, Art. 7 GrCh Rn. 10.

885 Bernsdorff in Meyer, EU-GrCh, Art. 7 Rn. 24.

886 Bernsdorff in Meyer, EU-GrCh, Art. 7 Rn. 24.

887 Kingreen in Callies/Ruffert, EUV-AEUV, Art. 7 GrCh Rn. 10.

bb) Eingriffe in die Achtung der Kommunikation

Als Eingriff in die Achtung der Kommunikation wird man parallel zu Art. 8 EMRK die Beeinträchtigung des Kommunikationsweges ansehen müssen.[888] Einen Eingriff in die Kommunikation wird man bei jeder Beeinträchtigung und jeder Kenntnisverschaffung über die Kommunikation selbst oder ihre Umstände annehmen müssen. Allein die Möglichkeit einer heimlichen Überwachung kann eine Vorwirkung entfalten und der Kommunikation ihre Unbefangenheit nehmen.[889]

Eine Verarbeitung von personenbezogenen Daten, die im Zusammenhang mit dem Kommunikationsvorgang stehen, stellt einen Eingriff in die Achtung der Kommunikation dar.[890] Damit könnte eine Schutzpflichtverletzung des Gesetzgebers durch den Erlaubnistatbestand des § 41a PostG vorliegen.

cc) Rechtfertigung von Eingriffen in die Achtung der Kommunikation

Ein Eingriff in die Achtung der Kommunikation bedarf einer Rechtfertigung, die ihrerseits verhältnismäßig ist.

(1) Qualifizierter Gesetzesvorbehalt

Auch bei der Achtung der Kommunikation richten sich die möglichen legitimen Einschränkungen gemäß Art. 52 Abs. 3 GrCh nach Art. 8 EMRK.[891] Folglich handelt es sich hier ebenfalls um einen qualifizierten Gesetzesvorbehalt mit den Schranken des Art. 8 Abs. 2 EMRK. Eine Überwachung des Briefverkehrs muss dabei normativ angeordnet und hinreichend bestimmt sein.[892]

---

888 Vgl. 4. Teil. D. I. 1.) a) bb).

889 Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1338.

890 Vgl. 4. Teil. D. I. 1.) a) bb).

891 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

892 Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1343.

Damit sind bei einem Eingriff dieselben Wertungen zu ziehen wie bei Art. 8 EMRK.[893] Folglich wären die Anforderungen des qualifizierten Gesetzesvorbehalts auch gegenüber der Achtung der Kommunikation gemäß Art. 7 GrCh durch § 41a PostG erfüllt.

(2) Schranken-Schranken

Die Rechtfertigungsvoraussetzungen von Art. 8 Abs. 2 EMRK sind ebenfalls als Maßstab für eine Verhältnismäßigkeitsprüfung anzulegen. Dabei ist das Sicherheitsinteresse der Allgemeinheit mit der Achtung der Kommunikation abzuwägen.

Bezüglich der Prüfung des legitimen Zweckes, der Geeignetheit und der Erforderlichkeit ist auf die Prüfung der Achtung des Privatlebens gemäß Art. 8 EMRK zu verweisen, da diesen Überlegungen der gleiche Maßstab und die gleichen Wertungen zugrundeliegen.[894] Schließlich darf im Rahmen einer Angemessenheitsprüfung das Schutzinteresse des Einzelnen vor Achtung seiner Kommunikation das Sicherheitsinteresse der Allgemeinheit nicht überwiegen. Bezüglich der konkreten Verhältnismäßigkeitsprüfung kann hier auf die Untersuchung der Achtung des Briefverkehrs verwiesen werden, dem der gleiche Prüfungsmaßstab zugrunde liegt.

§ 41a PostG wäre demnach auch im Hinblick auf die Achtung der Kommunikation verhältnismäßig.

dd) Zwischenergebnis

Der Eingriff durch § 41a PostG in den Schutzbereich der Achtung der Kommunikation wäre gerechtfertigt.

---

[893] Vgl. 4. Teil. D. I. 1.) a) cc) (1).

[894] Vgl. 4. Teil. D. I. 1.) a) cc) (2).

c) Zwischenergebnis

Der Eingriff in Art. 7 GrCh durch § 41a PostG wäre gerechtfertigt und das Grundrecht weder in der Ausprägung der Achtung des Privatlebens noch der Achtung der Kommunikation verletzt.

2. Art. 8 GrCh, Schutz personenbezogener Daten

Gemäß Art. 8 GrCh hat jede Person *„das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden"*. Weiterhin hat jede Person *„das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken"*.

Die Norm ist dem Datenschutzrecht der Union sowie des Europarates nachgebildet.[895] Hauptsächlich bezieht sich Art. 8 GrCh dabei auf Art. 286 EG (= Art. 16 AEUV), die Richtlinie 95/47/EG sowie Art. 8 EMRK und das Übereinkommen zum Schutz des Menschen bei automatisierter Verarbeitung personenbezogener Daten" des Europarates vom 28.01.1981.[896] Sie steht dabei in einem engen Verhältnis zu Art. 7 GrCh, in dessen Rahmen die Achtung des Familienlebens das Recht auf informationelle Selbstbestimmung mitumfasst, sowie dem Zugang zu Dokumenten aus Art. 42 GrCh, dessen Gewährleistungen notwendige Ergänzungen für einen effektiven Schutz personenbezogener Daten sind.[897] Ergänzt wird die Norm weiterhin durch Art 16 AEUV, Art. 39 EUV sowie die VO (EG) Nr. 45/2001.[898] Neben dem grundrechtlichen Schutz personenbezogener Daten beinhaltet Art. 8 GrCh auch ein Auskunftsrecht (Art. 8 Abs. 2 S. 2 GrCh) und fordert die Einrichtung von Datenschutzbeauftragten (Art. 8 Abs. 3 GrCh).

---

895 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

896 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

897 Bernsdorff in Meyer, EU-GrCh, Art. 8 Rn. 13.

898 GrCh/aktualisierte Erläuterungen vom 14.12.2007, wiedergegeben in EUGRZ 2008, S. 92 ff.

a) Schutzbereich

Zunächst könnte durch § 41a PostG der Schutzbereich von Art. 7 GrCh eröffnet sein.

aa) Persönlicher Schutzbereich

Der Wortlaut der Norm gesteht jeder „Person" das Recht auf Schutz personenbezogener Daten zu. Die Formulierung „jede natürliche Person", wurde hingegen bewusst nicht übernommen.[899] Unbestritten werden alle natürlichen Personen vom Schutzbereich umfasst.[900]

Umstritten hingegen ist die Einbeziehung juristischer Personen. Die Datenschutzrichtlinie, auf die sich Art. 8 GrCh bezieht, schützt nur natürliche Personen.[901] Dagegen spräche eine Nähe zum Schutz der Privatlebens, dass unter Umständen juristische Personen wohl auch geschützt werden. Im Bereich der elektronischen Kommunikation,wurde die RL 95/46/EG durch die RL 02/58/EG erweitert und erkennt das Datenschutzinteresse juristischer Personen ausdrücklich an. Der EuGh hat den Schutz juristischer Personen zumindest dann angenommen, wenn natürliche Personen erkennbar hinter der juristischen Person stehen.[902] Schließlich spricht die Nähe zu Art. 8 EMRK, der ebenfalls personenbezogene Daten schützt und der auf juristische Personen gerade im Bereich des Datenschutzes anwendbar ist, für einen Schutz juristischer Personen.

§ 41a PostG erlaubt die Verwendung personenbezogener Daten natürlicher wie auch juristischer Personen. Folglich wäre der persönliche Schutzbereich eröffnet.

---

899 Bernsdorff in Meyer, EU-GrCh, Art. 8 Rn. 6.

900 Wolffgang in Lenz/Borchardt, EU-Verträge Kommentar, 6 Aufl., Köln 2012, Art. 8 EMRK Rn. 2.

901 Erwägungsgrund 24; Johlen in Tettinger/Stern, Europäische Grundrechtecharta, 2006, Art. 8 Rn. 29.

902 EuGH Rs. C-92/09 und C-93/09 Rn. 53; so auch dazu die SCHLUSSANTRÄGE DER GENERALANWÄLTIN ELEANOR SHARPSTON vom 17. Juni 2010 Rn. 72.

bb) Sachlicher Schutzbereich

Der Umfang des Rechts auf Schutz personenbezogener Daten orientiert sich an den Gewährleistungen der bisherigen unionalen Regelungen.[903] Entsprechend Art. 2a RL 95/45/EG sind demnach *„personenbezogene Daten alle Informationen über eine bestimmte oder bestimmbare natürliche Person („betroffene Person"); als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind"*. So sollen umfassend alle personenbezogenen Daten geschützt werden.[904]

Fraglich erscheint, wie weit der sachliche Schutzbereich ausgestaltet ist, orientiert man sich am bisherigen Datenschutzrecht der Union. Die RL 95/46/EG klammert in ihrem Art. 3 Abs. 2 Verarbeitungen *„betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohls, wenn die Verarbeitung die Sicherheit des Staates berührt) und die Tätigkeiten des Staates im strafrechtlichen Bereich"* aus. Dies könnte dafür sprechen, den Schutzbereich von Art. 8 GrCh ebenfalls entsprechend einzugrenzen[905]. Unterstützt werden könnte dies neben der RL 95/46/EG vom Wortlaut von Art. 51 GrCh.[906] Dieser will die Schaffung neuer Zuständigkeiten durch die GrCh verhindern. Den Schutzbreich von Grundrechten auf den Anwendungsbereich einzelner Gesetze zu beschränken, würde jedoch zu einer Aushöhlung des Grundrechtsschutzes führen. Zudem wird diese Beschränkung nicht vom Wortlaut der Norm gestützt und widerspricht dem Sinn und Zweck eines umfassenden Grundrechtsschutzes. Weiterhin widerspricht die Systematik des Grundrechtsschutzes im Zusammenspiel mit Art. 7 GrCh und Art. 8 EMRK einem solchen

---

903 Bernsdorff in Meyer, EU-GrCh, Art. 8 Rn. 14.

904 Rengeling/Szczekalla, Grundrechte in der Europäischen Union – Charta der Grundrechte und Allgemeine Rechtsgrundsätze, 2004, § 16 Schutz der Privatsphäre, Art. 8 Rn. 681; Johlen in Tettinger/Stern, Europäische Grundrechtecharta, 2006, Art. 8 Rn. 31 ff.

905 So wohl Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1377.

906 So Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1377.

Ausschluss, da dieser für die anderen Grundrechte so nicht gilt Schließlich wird mit der Rechtfertigungsebene ein ausreichender Mechanismus zum Ausgleich mit anderen Rechtsgütern zur Verfügung gestellt. Einem Ausschluss der öffentlichen Sicherheit, der Landesverteidigung sowie der Sicherheit des Staates aus dem Schutzbereich von Art. 8 GrCh ist daher zu widersprechen.

Weiterhin handelt es sich bei Art. 8 GrCh nicht nur um ein Abwehrrecht gegenüber dem Staat. Es besteht darüber hinaus eine Schutzpflicht der öffentlichen Gewalt, die Grundrechtsträger vor Einwirkungen durch Dritte zu schützen.[907] Anders als das BDSG unterscheidet Art. 8 GrCh nicht zwischen öffentlichen und nichtöffentlichen Stellen. Dies erscheint angesichts moderner Datenverarbeitungsmöglichkeiten und der Gefahren, die dabei von nichtöffentlichen Stellen ausgehen, sinnvoll. Daraus folgt jedoch auch eine Schutzpflicht der öffentlichen Gewalt, die Grundrechtsträger vor der Datenverarbeitung durch nichtöffentliche Stellen zu schützen.[908]

§ 41a PostG beträfe die Verarbeitung von Daten, die mit Personen in einem Zusammenhang stehen. Aus der Schutzpflicht des Staates ergäbe sich hier auch eine Schutzpflicht, natürliche und juristische Personen vor einer Datenverarbeitung durch die Postdienstleister zu schützen. Der sachliche Schutzbereich wäre damit eröffnet.

b) Eingriffe in den Schutz personenbezogener Daten

Ein Eingriff in den Schutz personenbezogener Daten liegt bei jeder Verwendung solcher Daten vor.[909] Art. 2 b RL 95/46/EG definiert als Verarbeitung personenbezogener Daten *„jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Speichern, die Organisation, die Aufbewahrung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Benutzung, die Weitergabe durch*

---

907 Rengeling/Szczekalla, Grundrechte in der Europäischen Union – Charta der Grundrechte und Allgemeine Rechtsgrundsätze, 2004, § 16 Schutz der Privatsphäre, Art. 8 Rn. 684.

908 So auch Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1388 ff.

909 So auch Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1404.

Übermittlung, Verbreitung oder jede andere Form der Bereitstellung, die Kombination oder die Verknüpfung sowie das Sperren, Löschen oder Vernichten".

Damit ist von einem weiten Verarbeitungsbegriff auszugehen, der alle Arten der Verwendung von Daten umfassen möchte. Der Begriff ist dabei äußerst flexibel zu verstehen, um auch gegebenenfalls neue Verarbeitungsformen einzuschließen und langfristig einen effektiven Schutz zu gewährleisten.[910] Ob die Datenverarbeitung manuell oder automatisiert erfolgt, ist unerheblich.[911] Auf einen bei der Verarbeitung entstandenen Nachteil kommt es beim Eingriff nicht an.[912] Ein Eingriff wird verneint, wenn der Betroffene ausreichend informiert wurde und einwilligt.[913] Systematisch wäre dies in der Regel eine Frage der Rechtfertigung. Der Wortlaut von Art. 8 GrCh *„oder auf einer sonstigen gesetzlich geregelten Grundlage"* spricht jedoch dafür, dass hier bereits kein Eingriff vorliegen soll, mit der Folge, dass auch die Schrankenregelungen nicht greifen.[914]

Ein Eingriff läge bei einer Datenverarbeitung zwecks Risikoanalyse unstreitig vor. Damit könnte eine Schutzpflichtverletzung des Gesetzgebers durch § 41a PostG vorliegen.

c) Rechtfertigung von Eingriffen in den Schutz personenbezogener Daten

Ein Eingriff in den Schutz personenbezogener Daten bedarf einer Rechtfertigung, die ihrerseits verhältnismäßig ist.

aa) Qualifizierter Gesetzesvorbehalt

Die Rechtfertigung von Eingriffen in den Schutz personenbezogener Daten richtet sich nach Art. 8 Abs. 2 EMRK. Als Auslegungshilfen können die RL 95/46/

910 Im Ergebnis auch Bernsdorff in Meyer, EU-GrCh, 8 Rn. 16.

911 Bernsdorff in Meyer, EU-GrCh, Art. 8 Rn. 16.

912 Kingreen in Callies/Ruffert, EUV, Art. 8 GrCh Rn. 12.

913 SchEuGH Slg. 2000, 3; I-4989 Rn. 74.

914 So auch Kingreen in Callies/Ruffert, EUV, Art. 8 GrCh Rn. 13.

EG sowie die VO Nr. 45/2001 herangezogen werden.[915] Den Rechtfertigungstatbeständen ist eine Verarbeitung unter Zweckbindung und nach Treu und Glauben vorangestellt und damit für alle Rechtfertigungsgründe bindend.[916] Der Zweck muss klar benannt sein und darf sich nicht in generalisierenden Formulierungen erschöpfen.[917]

Zunächst ist ein Eingriff in den Schutzbereich gerechtfertigt, wenn die betroffene Person eingewilligt hat.

Weiterhin kann ein Eingriff gemäß Art. 8 Abs. 2 GrCh gerechtfertigt sein, wenn er auf einer *„gesetzlich geregelten legitimen Grundlage"* beruht.

Eine weitere Schranke könnte die Kollisionsregel in Art. 51 Abs. 2 GrCh darstellen. Bei bereits in den Verträgen bestehenden Gewährleistungen sind deren Umfang und Tragweite spezieller und für die Bestimmung der Rechtfertigungsmöglichkeiten maßgeblich.[918] Jedoch besteht in der Lehre Einigkeit darüber, dass Art. 8 GrCh nicht im Sinne des Art. 52 Abs. 2 GrCh im Vertrag verankert ist, sondern diesem lediglich entnommen ist.[919] Folglich greift nicht die spezielle Regel des Art. 52 Abs. 2 GrCh, sondern die allgemeine des Art. 51 Abs. 1 GrCh.[920]

Durch die Anwendung der Schranken von Art. 8 Abs. 2 EMRK wären bei einem Eingriff durch § 41a PostG auch dieselben Wertungen zu ziehen.[921] Folglich wären die Anforderungen des qualifizierten Gesetzesvorbehalts auch gegenüber dem Schutz personenbezogener Daten gemäß Art. 7 GrCh durch

---

915 Wolffgang in Lenz/Borchardt, EU-Verträge Kommentar, 6. Aufl., Köln 2012, Art. 8 EMRK Rn. 5.

916 Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1426.

917 Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1432 ff.; Johlen in Tettinger/Stern, Europäische Grundrechtecharta, 2006, Art. 8 Rn. 45.

918 Wolffgang in Lenz/Borchardt, EU-Verträge Kommentar, 6 Aufl., Köln 2012, Art. 52 EMRK Rn. 16.

919 Johlen in Tettinger/Stern, Europäische Grundrechtecharta, 2006, Art. 8 Rn. 42; anders Bernsdorff in Meyer, EU-GrCh, Art. 8 Rn. 17.

920 Johlen in Tettinger/Stern, Europäische Grundrechtecharta, 2006, Art. 8 Rn. 42; im Ergebnis wohl auch Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1430 f.

921 Vgl. 4. Teil. D. I. 1.) a) cc).

§ 41a PostG erfüllt. Die Heranziehung des unionalen Datenschutzrechts verändert diese Wertung nicht. Die Zweckbindung der Verarbeitung wie auch eine Verarbeitung nach Treu und Glauben wären von § 41a PostG berücksichtigt.

bb) Schranken-Schranken

Die Verhältnismäßigkeit richtet sich nach der Intensität des Eingriffs und der Kollision mit anderen Grundrechten. Eine weitere Hilfestellung bei der Bestimmung der Erforderlichkeit können zwei Grundsätze insbesondere für die sicherheits- und polizeirechtliche Datenverarbeitung geben.[922] Erstens der „Vorrang der unmittelbaren vor der mittelbaren Datenerhebung“ und zweitens der „Vorrang der offenen vor der verdeckten Datenerhebung“.[923]

Für den Zweck der Terrorismusbekämpfung wird dem Gesetzgeber ein großer Beurteilungsspielraum zugestanden.[924]

Bezüglich der Prüfung des legitimen Zweckes, der Geeignetheit und der Erforderlichkeit ist grundsätzlich auf die Prüfung der Achtung des Privatlebens gemäß Art. 8 EMRK zu verweisen, da diesen Überlegungen der gleiche Maßstab und die gleichen Wertungen zugrunde liegen.[925] Darüber hinaus sind für die Erforderlichkeitsprüfung die Grundsätze des „Vorranges der unmittelbaren vor der mittelbaren Datenerhebung“ und „des Vorranges der offenen vor der verdeckten Datenerhebung“ zu berücksichtigen. Die Daten würden nicht bei Dritten eingeholt, sondern direkt beim Betroffen, insoweit erfolgte die Datenerhebung offen und direkt. Eine Offenlegung der Risikoanalyse und des Verfahrens im Sinne eines transparenten Vorganges würde jedoch dem Sinn und Zweck bzw. dem Ziel der Sicherheitssteigerung zuwiderlaufen. Für die Prüfung der konkreten Maßnahme anhand der in § 41a PostG verankerten Verhältnismäßigkeitsprüfung wäre ein

922 Kingreen in Callies/Ruffert, EUV, Art. 8 GrCh Rn. 16.

923 Kingreen in Callies/Ruffert, EUV, Art. 8 GrCh Rn. 16.

924 Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1459.

925 Vgl. 4. Teil. D. I. 1.) a) cc) (2).

strengerer Maßstab bei personalisierten Maßnahmen (Überprüfbarkeit, konkrete Gefahr, Folgen der Datenverarbeitung z. B. Einreiseverbot) zu beachten.[926]

Darüber hinaus ist bezüglich der Angemessenheit des Tatbestandes von § 41a PostG auf die Prüfung der Rechtfertigung des Rechts auf Achtung des Privatlebens zu verweisen, die gerade auch im Hinblick auf die Intensität des Erlaubnistatbestandes eine Abwägung vornimmt.

§ 41a PostG wäre demnach auch im Hinblick auf den Schutz personenbezogener Daten verhältnismäßig.

3. Zwischenergebnis

§ 41a PostG würde weder Art. 7 noch Art. 8 GrCh verletzen. Grundrechte nach der Europäischen Grundrechtecharta wären demnach nicht verletzt.

III. Grundrechte nach dem Grundgesetz

Das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG sowie das Brief-, Post- und Fernneldegeheimnis aus Art. 10 GG könnten durch § 41a PostG betroffen sein.

1. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Das Recht auf informationelle Selbstbestimmung

Gemäß Art. 2 Abs. 1 GG hat jeder *„das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt“*. Zunächst leitet sich *„daraus die Garantie der allgemeinen Handlungsfreiheit als Auffanggrundrecht“* ab, die gegen-

926 Frenz, Handbuch Europarecht Bd. 4, § 4 Rn. 1462 ff.

über den anderen Grundrechten subsidiär ist.[927] Weiterhin wird aus Art. 2 Abs. 1 GG i. V. m. Art 1 Abs. 1 GG der Schutz des allgemeinen Persönlichkeitsrechts abgeleitet. Ziel des allgemeinen Persönlichkeitsrechts ist es, *„die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen zu gewährleisten, die sich durch die traditionellen konkreten Freiheitsgarantien nicht abschließend erfassen lassen“.*[928]

Aus diesem Schutzgedanken heraus haben sich mehrere präzisere weitergehende geschützte Komplexe herausgebildet, so der Schutz der Selbstdarstellung, das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme sowie das Recht auf informationelle Selbstbestimmung.

Beim Recht auf informationelle Selbstbestimmung handelt es sich um einen vom Bundesverfassungsgericht mit dem Volkszählungsurteil vom 15.12.1983 entwickelten Schutz der Privatsphäre, der infolge neuer technischer Entwicklungen notwendig wurde.[929]

a) Schutzbereich

Zunächst gilt es, den persönlichen und sachlichen Schutzbereich zu untersuchen.

aa) Persönlicher Schutzbereich

Der Schutz des allgemeinen Persönlichkeitsrechts und damit auch der Schutz des Rechts auf informationelle Selbstbestimmung umfasst alle natürlichen Personen.[930] Auch Minderjährige werden über Art. 2 Abs. 1 GG geschützt, das seine besondere Ausprägung in einem „Persönlichkeitswerdungsrecht“ findet.[931] Ver-

---

927 Sodan in Sodan, Grundgesetz Beck'scher Kompakt-Kommentar, Art. 2 Rn. 1.

928 BVerfGE 54, S. 148/153; 72, 155/170.

929 Di Fabio in Maunz/Dürig, GG, Art. 2 GG Rn. 173.

930 Sodan in Sodan, Grundgesetz Beckscher Kompakt-Kommentar, Art. 2 Rn. 9a; Dreier in Dreier, GG, Art. 2 GG Rn. 81; Kunig in v. Münch/Kunig, Art. 2 Rn. 39.

931 Zu den Besonderheiten des Minderjährigenschutzes siehe Dreier in Dreier, GG, Art. 2 GG Rn. 81, insbesondere Fn. 321.

storbene werden über den postmortalen Persönlichkeitsschutz vom Schutzbereich ebenfalls umfasst.[932]

Juristischen Personen wird mittlerweile überwiegend ebenfalls das Recht auf informationelle Selbstbestimmung zugesprochen.[933] Diesen wird ein *„Grundrechtsschutz vor Gefährdungen, die von staatlichen informationellen Maßnahmen ausgehen können“*, eingeräumt.[934]

Dogmatisch bedürfte es hier wohl einer kaum sauber abgrenzbaren Aufspaltung des Rechts auf informationelle Selbstbestimmung in einen aus der Menschenwürde aus Art. 1 Abs. 1 GG und aus der allgemeinen Handlungsfreiheit aus Art. 2 Abs. 1 GG abzuleitenden Teil. Jedoch wird man natürlich auch hier einen Schutz nur so weit auf juristische Personen anwenden können, wie er seinem Wesen nach auf diese anwendbar ist. So kann sich eine juristische Person sicherlich nicht auf den Schutz ihrer Intimsphäre berufen. Die Tatsache, dass das BDSG nur personenbezogene Daten schützt, spricht zumindest dafür, dass der Gesetzgeber keine Verpflichtung sah, in Ausgestaltung des Rechts auf informationelle Selbstbestimmung juristische Personen gleich natürlichen Personen zu schützen. Jedoch wird man angesichts des Umfangs an massenhafter Datenverarbeitung, juristischen Personen zumindest einen partiellen Grundrechtsschutz nicht verwehren können.

So hat der BGH richtig ausgeführt *„Eine Ausdehnung der Schutzwirkung dieses Rechts über natürliche Personen hinaus auf juristische Personen erscheint – auch mit Blick auf Art. 19 Abs. 3 GG – nur soweit gerechtfertigt, als sie aus ihrem Wesen als Zweckschöpfung des Rechts und ihren Funktionen dieses Rechtsschutzes bedürfen. Dies ist der Fall, wenn sie in ihrem sozialen Geltungsbereich als Arbeitgeber oder als Wirtschaftsunternehmen betroffen werden.“*[935]

---

[932] Dreier in Dreier, GG, 2. Aufl. 2004, Art. 2 GG Rn. 81.

[933] So auch Sodan in Sodan, Grundgesetz Beckscher Kompakt-Kommentar, Art. 2 Rn. 9a; im Grundsatz ebenfalls Dreier in Dreier, GG, Art. 2 GG Rn. 82. Weitergehend bei Dreier Fn. 328; wohl anders Kunig in v. Münch/Kunig, Art. 2 Rn. 39.

[934] BVerfGE 118, S. 168/204.

[935] BVerwGE 82, 76 (78); auch BGHZ 81, S. 75 (78).

Mit § 41a PostG würden Informationen verarbeitet werden, die im Bezug mit bestimmten oder bestimmbaren Personen stünden. Daher wäre ein Personenbezug der Daten unstrittig gegeben und natürliche Personen eindeutig geschützt. Für juristische Personen geht von einer Risikoanalyse die gleiche Gefährdung aus wie für natürliche Personen, da die Ergebnisse und Konsequenzen über das Risiko einer Sendung eine juristische Person genauso treffen.

Damit ist der persönliche Schutzbereich von Art. 8 GrCh für natürliche als auch juristische Personen eröffnet.

bb) Sachlicher Schutzbereich

Der Schutzbereich des Rechts auf informationelle Selbstbestimmung beinhaltet das Recht *„selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen“*.[936] Daraus ergibt sich auch – den datenschutzrechtlichen Bestimmungen vorausgehend – eine allgemeine Integrität personenbezogener Daten.[937] So schützt schon daraus resultierend Art. 2 Abs. 1 GG, – was im Bundesdatenschutzgesetz präzisiert und ausgeformt ist – *„vor Feststellen, Verwenden, Speichern, Weitergeben und Veröffentlichen personenbezogener Daten“*.[938] Damit wird auch vor der Herstellung eines Persönlichkeitsbildes umfassend geschützt.[939] Dieser Schutz wird durch die Möglichkeiten, mittels moderner Datenverarbeitung durch die Verknüpfung einzelner Informationen – beispielsweise in sozialen Netzwerken – präzise Persönlichkeitsprofile zu erstellen, besonders relevant.

Der Schutz der Selbstdarstellung umfasst ebenfalls den Schutz der eigenen Darstellung innerhalb der Kommunikation mit Dritten.[940] Dieser Schutz bezieht sich zunächst auf die Nutzung von Telekommunikationseinrichtungen.[941] Jedoch ist

---

936 BVerfGE 117, 202/228; 120, 274/312; 128, 1/42.

937 Starck in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 2 Abs. 1 Rn. 114.

938 Starck in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 2 Abs. 1 Rn. 114.

939 Dreier in Dreier, GG, 2. Aufl. 2004, Art. 2 GG Rn. 78.

940 Hofmann in Schmidt-Bleibtreu/Klein, GG, Art 2 GG Rn. 32; BVerfGE 54, 148 [155].

941 BVerfGE 85, 386 [396].

zu überlegen, ob durch moderne massenhafte Datenverarbeitungsmöglichkeiten eine ähnliche Gefährdungslage auch nicht für andere Kommunikationsformen besteht. Der Schutz bei Nutzung von Telekommunikationseinrichtungen bezieht sich darauf, dass Dritte ohne Zustimmung der Betroffenen in ein Gespräch mit einbezogen werden.[942] Dieser Schutz vor der Kenntnisnahme von Kommunikation durch Dritte bei technischen Einrichtungen dürfte zu verallgemeinern sein.

Der Schutzbereich umfasst neben einer Abwehrfunktion gegenüber dem Staat auch eine Schutzfunktion des Staates gegenüber den Grundrechtsträgern.[943] Diese Schutzfunktion kann sich auch durch eine Regelungspflicht des Verhältnisses der Grundrechtsträger untereinander äußern.[944] Dabei wird regelmäßig eine Abwägung zwischen den (Grund-)Rechten der Betroffenen vorzunehmen sein. So kann das allgemeine Persönlichkeitsrecht, u.a. mit der Meinungs- Kunst-, oder Versammlungsfreiheit kollidieren.[945] Diese Konflikte sind dann auf dem Wege der praktischen Konkordanz aufzulösen. Gerade im Verhältnis von Grundrechtsträgern, zwischen denen Ungleichgewichte bestehen, wie zwischen Verbrauchern und Unternehmern oder Kunden/bzw. Nutzern von Technologien und Anbietern, dürfte dieser Regelungspflicht eine große Bedeutung hinsichtlich eines effektiven Grundrechtsschutzes zukommen.

Für die Eröffnung des Schutzbereichs ist die Intensivität, mit der das Recht auf informationelle Selbstbestimmung tangiert wird, zunächst unerheblich.[946] Die technischen Möglichkeiten führen dazu, dass es *„kein belangloses Datum"* mehr gibt und daher für die Eröffnung des Schutzbereichs nicht unterschieden wird, ob in die Intim-, Privat- oder Sozialsphäre eingegriffen wurde, weil auch die Verknüpfung von Informationen aus der Sozialsphäre Rückschlüsse auf die

---

942 Hofmann in Schmidt-Bleibtreu/Klein, GG, Art 2 GG Rn. 32.

943 Kunig in v. Münch/Kunig, Grundgesetz, 6. Aufl. 2012, Art. 2 Rn. 40.

944 So auch Hofmann in Schmidt-Bleibtreu/Klein, GG, Art 2 GG Rn. 32.

945 Genauer dazu Dreier in Dreier, GG, 2. Aufl. 2004, Art. 2 GG Rn. 92, sowie der Fußnotenapparat hierzu.

946 Dreier in Dreier, GG, 2 Aufl. 2004, Art. 2 GG Rn. 80.

Intim- und Privatsphäre zulassen kann und sich aus ihnen Persönlichkeitsbilder und Profile erstellen lassen.[947]

§ 41a PostG beträfe die Verwendung von Daten, die im Zusammenhang mit Personen stehen. Eine umfassende Sammlung von Daten und ihre Auswertung in Form einer Risikoanalyse erlaubt Rückschlüsse auf das Kommunikationsverhalten Einzelner. Der Stellenwert des Universaldienstes führt zudem zu einem Ungleichgewicht zwischen dem Verbraucher bzw. Kunden und dem Universaldienstanbieter DPAG. Der Schutzbereich des Rechts auf informationelle Selbstbestimmung wäre folglich eröffnet.

b) Eingriffe in das Recht auf informationelle Selbstbestimmung

Als Eingriffe in das Recht auf informationelle Selbstbestimmung kommen zunächst Handlungen des Staates entsprechend dem klassischen Eingriffsbegriff in Frage. Weiterhin kommen Maßnahmen in Betracht, die unter staatlichen Zwang oder daraus resultierend vollzogen werden.[948]

Jedoch deckt der klassische Eingriffsbegriff bei weitem nicht alle Möglichkeiten der Beeinträchtigung des Rechts auf informationelle Selbstbestimmung ab. Das Erheben, Verwerten und Sammeln von Daten ist auch ohne bestimmte Zielrichtung auf einen Grundrechtsträger und ohne dessen Zutun möglich. Die sich dabei ergebenden Datensammlungen können jedoch erheblich sein und umfassende Persönlichkeitsbilder erzeugen. Daher sind *„alle Formen der Kenntnisnahme, Aufzeichnung und Verwertung“* personenbezogener Daten als Eingriffe anzusehen.[949]

Angesichts einer so breiten Ausdehnung des Eingriffsbegriffs ist die Anwendung einer Bagatellgrenze umstritten. So wird eine Unterscheidung zwischen nicht eingriffswürdigen „bloß nachteiligen Betroffenheiten“ und eingriffswürdi-

947 BVerfGE 65, 1/45; Dreier in Dreier, GG, Art. 2 GG Rn. 80; Kunig in v. Münch/Kunig, GG, Art. 2 Rn. 41.

948 Beispiel siehe Dreier in Dreier, GG, Art. 2 GG Rn. 83.

949 Dreier in Dreier, GG, Art. 2 GG Rn. 83; auch Di Fabio in Maunz/Dürig, GG, Art. 2 Rn. 176.

gen *Sachverhalten „die das Gefährdungspotenzial für eine wesentliche Hemmung der freien Selbstbestimmung aufweisen"* erörtert.[950] Eine solche Einteilung scheint jedoch kaum praktikabel. Wann potenzielle oder tatsächliche Hemmungen vorliegen, ist eine Frage der Wertung und Prognose. Zudem sind die Begriffe kaum bestimm- und sehr dehnbar. Es erscheint daher sinnvoller, Fragen der Bagatellhaftigkeit im Rahmen der Verhältnismäßigkeit zu erörtern.

Ein Eingriff in das Recht auf informationelle Selbstbestimmung ist unzweifelhaft durch die Verwendung von Daten zwecks Risikoanalyse und die damit verbundenen Auswirkungen auf das Kommunikationsverhalten des Einzelnen gegeben. Der Gesetzgeber könnte hier seine Schutzpflicht, Dritte vor dieser Datenverarbeitung zu schützen, verletzen.

c) Rechtfertigung von Eingriffen in das Recht auf informationelle Selbstbestimmung

Die Informationsverarbeitung – auch personenbezogener Daten – ist notwendiger und nicht wegzudenkender Bestandteil einer Wissens- und Informationsgesellschaft. Daher ist auch das Recht auf informationelle Selbstbestimmung nicht schrankenlos gewährleistet, sondern kann durch eine gesetzliche Ermächtigungsgrundlage eingeschränkt werden.[951]

aa) Gesetzesvorbehalt

Art. 2 Abs. 1 Hs. 2 GG enthält grundsätzlich eine Schrankentrias aus den Rechten anderer, der verfassungsmäßigen Ordnung sowie dem Sittengesetz. Im Ergebnis wird diese jedoch wie ein einfacher Gesetzesvorbehalt gelesen.[952]

---

[950] Dreier in Dreier, GG, Art. 2 GG Rn. 84; Hoffmann-Riem informationelle Selbstbestimmung in der Informationsgesellschaft, in AöR 1998, 123 (1998), 513 (531f); Kloepfer/Breitkreutz, Videoaufnahmen und Videoaufzeichnungen als Rechtsproblem, in DVBL 1998, S. 1149 (1152).

[951] Di Fabio in Maunz/Dürig, GG, Art. 2 GG Rn. 179; BVerfGE 65, S. 45; 78, 77/85; BVerfG, NJW 1988, 3009 f.

[952] Sondan in Sodan, Grundgesetz Beckscher Kompakt-Kommentar, 2. Aufl. München 2011, Art. 2 Rn. 12 ff.; zur Schrankentrias ausführlicher BVerfGE 6 S. 32/38; Jarass in Jarass/Pieroth, Art. 2 Rn. 13 f.

Im Verhältnis Privater zueinander stellt sich die Situation anders dar als im Verhältnis Staat – Bürger. Da Private zunächst unmittelbar keine Grundrechtsverpflichteten sind, besteht für Sie zunächst kein genereller Rechtfertigungsbedarf für einen Eingriff in das Recht auf informationelle Selbstbestimmung, und folglich besteht zunächst keine Notwendigkeit einer gesetzlichen Ermächtigungsgrundlage.[953] Jedoch kommt dem Staat durch seine Schutzpflicht zu, Betroffene vor der Grundrechtsverletzung durch Dritte (Private) zu schützen.[954] Insoweit trifft den Staat eine Regelungspflicht. Dieser Pflicht ist der Gesetzgeber im BDSG für den Schutz personenbezogener Daten durch ein generelles Verbot der Datenverwendung mit Erlaubnisvorbehalt nachgekommen.[955]

§ 41a PostG als Parlamentsgesetz erfüllte den Gesetzesvorbehalt des Rechts auf informationelle Selbstbestimmung.

bb) Schranken-Schranken

Eine gesetzliche Ermächtigungsgrundlage muss Anforderungen an ihre formelle und materielle Verfassungsmäßigkeit – insbesondere an die Bestimmtheit und die Verhältnismäßigkeit – gerecht werden. Dabei werden an eine Ermächtigungsgrundlage jedoch hohe Anforderungen gestellt.[956] So müssen Einschränkungen des Rechts auf informationelle Selbstbestimmung nur im überwiegendem Allgemeininteresse hingenommen werden und auch nur so weit wie es zum Schutz öffentlicher Interessen unerlässlich ist.[957]

Die Anforderungen an eine Rechtfertigung steigen dabei mit der Intensität der Datenverarbeitung.[958]

---

953 Di Fabio in Maunz/Dürig, GG, Art. 2 GG Rn. 189.

954 Di Fabio in Maunz/Dürig, GG, Art. 2 GG Rn. 189.

955 Ein ausführlicher Überblick über weitere Normen die diesem Schutzauftrag nachkommen findet sich bei Dreier in Dreier, GG, Art. 2 GG Rn. 89, sowie weitergehende Literatur in der dortigen Fn. 365.

956 Di Fabio in Maunz/Dürig, GG, Art. 2 GG Rn. 181.

957 Starck in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 2 Abs. 1 Rn. 114 ff.; BVerfGE 67,100/143; 78, 77/85; 84, 239/279 f.

958 Starck in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 2 Abs. 1 Rn. 114 ff.

Trotz des Bedarfs flexibler und anpassungsfähiger Regelungen, müssen die eine Ermächtigungsgrundlage legitimierenden Zwecke – im Sinne der Normenklarheit – hinreichend bestimmt sein.[959] Auch hier gilt, dass die Anforderungen an die Bestimmtheit mit Eingriffstiefe steigen.[960] Damit sind auch Generalklauseln prinzipiell möglich.[961] Die Rechtfertigung eines Eingriffs ist abgestuft nach der Intensität und dem betroffenen Bereich zu betrachten.[962]

Eine Orientierung kann die Sphärentheorie bieten, nach der zwischen Intim-, Privat- und Gesellschaftssphäre unterschieden wird. Auch wenn der Schutz vor automatisierter Datenverarbeitung nicht grundsätzlich von der Sphäre abhängt, kann die Theorie dabei helfen, die Eingriffstiefe und den damit verbundenen Rechtfertigungsaufwand zu bestimmen. Das BDSG bedient sich einer ähnlichen Systematik, indem zwischen „normalen" personenbezogenen Daten und solchen mit höchstpersönlichem Bezug unterschieden wird.

Die Intimsphäre wird als Kernbereich der Persönlichkeit verstanden und soll absoluten Schutz genießen und nicht mit anderen Rechtsgütern abgewogen werden dürfen.[963] Die besondere Nähe des Persönlichkeitsrechtskerns zur Menschenwürde rechtfertigt einen absoluten Schutz. Jedoch wird teilweise die mangelnde Präzision in der Definition bemängelt, sodass eine Abgrenzung zwischen Intim- und Privatsphäre schwerfällt.[964] Grundsätzlich ist auf den Sozialbezug des betroffenen Bereiches abzustellen.[965] Je größer der Sozialbezug ist, desto eher ist ein Eingriff der Privat-, oder bei Öffentlichkeit sogar der Gesellschaftssphäre zu-

---

959 Di Fabio in Maunz/Dürig, GG, Art. 2 GG Rn. 180 f.; BVerfGE 65, S. 1 (44).

960 Murswiek in, Sachs, GG, Art. 2 Rn. 121.

961 Di Fabio in Maunz/Dürig, GG, Art. 2 GG Rn. 182; Vogelsang, Der Übergangsbonus in DVBL 1989, S. 963 (967 f.).

962 Starck in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 2 Abs. 1 Rn. 116.

963 Dreier in Dreier, GG, Art. 2 GG Rn. 87; BVerfGE 6, S. 32/41; 34, 238/245; 35, 35/39; 38, 312/320; 80, 367/373 f.; 103, 21/31.

964 Dreier in Dreier, GG, 2. Aufl. 2004, Art. 2 GG Rn. 78. Kritisch zur Definition: Degenhart, Das allgemeine Persönlichkeitsrecht in JuS 1992, S. 361 (363); Pieroth/Schlink/Kingreen/Poscher, Grundrechte Staatsrecht II, 33. Aufl. 2017 Heidelberg, § 7 Rn. 411 ff..

965 Di Fabio in Maunz/Dürig, GG, Art. 2 GG Rn. 159.

zuordnen. Eingriffe in die Privatsphäre sind nicht grundsätzlich ausgeschlossen, bedürfen jedoch einer besonderen Rechtfertigung, die im überwiegenden Interesse des Gemeinwohls liegt.[966]

Eine Rolle bei der Abwägung, spielt dabei die Form, in der Daten verarbeitet werden. Anonymisierte Datenverarbeitung ist als eingriffsärmer einzustufen als in personifizierter Form.[967] Die Verhältnismäßigkeit eines Eingriffes richtet sich auch nach den „verfahrensrechtlichen Schutzvorkehrungen", wie „Aufklärungs-, Auskunfts- und Löschungspflichten".[968]

Grundsätzlich liegen der Abwägung des Rechts auf informationelle Selbstbestimmung parellele Wertungen zugrunde, wie bei der Prüfung des Rechts auf Achtung des Privatlebens aus Art. 8 EMRK sowie der Achtung des Familienlebens aus Art. 7 GrCh.[969] Darüber hinaus ist die durch § 41a PostG zulässige Datenverarbeitung als Eingriff in die Gesellschaftssphäre zu werten. Bei den erfassten personenbezogenen Daten handelt es sich um öffentlich zugängliche Informationen. Die Prüfung unterliegt damit einer gewöhnlichen Verhältnismäßigkeitsprüfung. Diese ist entsprechend den Wertungen von Art. 8 EMRK sowie Art. 7, 8 GrCh zu bejahen.

d) Zwischenergebnis

Ein Eingriff durch Art. 41a PostG in Art 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG wäre demnach gerechtfertigt.

---

966 Di Fabio in Maunz/Dürig, GG, Art. 2 GG Rn. 159.

967 Im Ergebnis auch Starck in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 2 Abs. 1 Rn. 117.

968 BVerfGE 113, 29/57 f.; Di Fabio in Maunz/Dürig, GG, Art. 2 GG Rn. 178; Jarass, Art. 2 GG.

969 Vgl. 4. Teil. D. I. 1.) a) cc) (2).

2. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Ausgangspunkt für das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (im weiteren IT-Grundrecht[970]) aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ist ein Urteil des Bundesverfassungsgerichts von 27.02.2008.

Das grundrechtliche Schutzbedürfnis, folgt *„aus der Bedeutung der Nutzung informationstechnischer Systeme für die Persönlichkeitsentfaltung und aus den Persönlichkeitsgefährdungen, die mit dieser Nutzung verbunden sind".*[971] *„Der Einzelne ist darauf angewiesen, dass der Staat die mit Blick auf die ungehinderte Persönlichkeitsentfaltung berechtigten Erwartungen an die Integrität und Vertraulichkeit derartiger Systeme achtet."* [972] Der Schutzbereich des IT-Grundrechts geht über die Schutzbereiche von Art. 10 und Art. 13 GG hinaus.[973] Dies nimmt das BVerfG auch für das Allgemeine Persönlichkeitsrecht (APR) an.[974] Jedoch werden diese Grundrechte als spezieller angesehen, so dass das IT-Grundrecht subsidiär zurücktritt und nur zur Anwendung kommt, wenn diese nicht betroffen sind.[975] Im Verhältnis zum APR findet letztlich eine Vorverlagerung des Schutzes auf die Infrastruktur selbst statt, die bisher lediglich präventiv im Fokus stand, soweit es um Schutz durch Gestaltung der Infrastruktur ging.[976]

---

970 Auch wenn der Begriff IT-Grundrecht nicht den vollen Charakter des Grundrechts wiedergibt, wird er zunehmend in der Literatur verwendet und dient der sprachlichen Vereinfachung und „Handhabbarkeit".

971 BVerfG, 1 BvR 370/07 vom 27.02.2008 Rn. 181.

972 BVerfG, 1 BvR 370/07 vom 27.02.2008 Rn. 181.

973 Britz, Gabriele, Vertraulichkeit und Integrität informationstechnischer Systeme in DÖV 2008, S. 411 (412).

974 Anders Britz, Gabriele, Vertraulichkeit und Integrität informationstechnischer Systeme in DÖV 2008, S. 411 (414).

975 Britz, Gabriele, Vertraulichkeit und Integrität informationstechnischer Systeme in DÖV 2008, S. 411 (414), BVerfG, 1 BvR 370/07 vom 27.02.2008 Rn. 184.

976 Hoffmann-Riem, Wolfgang, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme in JZ 2008, S. 1009 (1016).

§ 41a PostG betrifft die Schutzbereiche von Art. 10 GG wie auch den Schutz auf informationelle Selbstbestimmung. Daher tritt das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme subsidiär zurück.

3. Art. 10 GG, Brief-, Post- und Fernmeldegeheimnis

„Art. 10 gehört zum Urgestein konstitutioneller Gewährleistungen gegen den Übermut staatlicher Neugier."[977]

Nach Art. 10 GG sind das „Briefgeheimnis sowie das Post- und Fernmeldegeheimnis" unverletzlich. Damit soll die private Fernkommunikation vor einer Beeinträchtigung aufgrund von möglicher staatlicher Kenntnisnahme geschützt werden.[978]

„Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt."[979]

Trotz des Wortlautes wird Art. 10 Abs. 1 GG als einheitliches Grundrecht gesehen, wodurch sich Abgrenzungs- und Konkurrenzprobleme vermeiden lassen.[980]

a) Schutzbereich

Zunächst könnte der Schutzbereich von Art. 10 GG durch § 41a PostG eröffnet sein.

---

977 Löwer in v. Münch/Kunig, GG, Art. 10 GG Rn. 81.

978 BVerfGE 115, S. 166/182; BVerfGE 107, S. 299/313; Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 1.

979 Art. 10 Abs. 2 GG.

980 Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 1; anders Hermes in Dreier, GG, Art. 10 GG Rn. 25.

aa) Persönlicher Schutzbereich

Geschützt werden grundsätzlich natürliche wie auch inländische juristische Personen.[981] Vom Schutzbereich ausgenommen sind juristische Personen des öffentlichen Rechts mit Ausnahme der Trias von öffentlichen Rundfunkanstalten, den Kirchen sowie Universitäten.[982]

§ 41a PostG betrifft natürliche als auch juristische Personen gleichermaßen.

bb) Sachlicher Schutzbereich

Geschützt ist mit dem Briefgeheimnis die körperliche Übermittlung von Briefen.[983] *„Als Brief ist jede mit einem verkörperten Medium verbundene Kommunikation an einen oder mehrere bestimmte Empfänger anzusehen.“*[984] In den Schutzbereich fällt auch schon die Möglichkeit der Kommunikation und der Schutz gegen die Untersuchung, ob kommuniziert wurde.[985] In den Schutzbereich des Briefgeheimnisses fällt ein Brief, soweit er sich nicht im Machtbereich eines Postdienstleisters befindet und folglich nicht unter das Postgeheimnis fällt.[986]

Weiterhin geschützt wird mit dem Postgeheimnis die Erbringung von Postdienstleistungen.[987] In Verbindung mit § 39 PostG wird jeder, der Postdienstleistungen erbringt, zum Stillschweigen über alle Postsendungen und alle postali-

---

981 Guckelberger in Schmidt-Bleibtreu/Klein, GG, Art. 10 GG Rn. 8 ff.; Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 10; Hermes in Dreier, GG, Art. 10 GG Rn. 26; vermittelnd Gusy in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 10 GG Rn. 24.

982 Löwer in v. Münch/Kunig, GG, Art. 10 GG Rn. 6; Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 10.

983 Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 3.

984 Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 3; Gusy in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 10 GG Rn. 27.

985 Hermes in Dreier, GG, 3. Aufl. 2013, Art. 10 GG Rn. 31; Jarass, Art. 10 GG in Jarass/Pieroth, GG, 12. Aufl., 2012 Rn. 3; Pieroth/Schlink/Kingreen/Poscher, Grundrechte Staatsrecht II, 33. Aufl. 2017 Heidelberg, § 19, Rn. 887 ff..

986 Löwer in v. Münch/Kunig, GG, 6. Aufl. 2012, Art. 10 GG Rn. 16.

987 Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 3.

schen Vorgänge verpflichtet.[988] Davon erfasst wird die körperliche Überbringung von Postsendungen, unter anderem Briefen, Päckchen, Paketen und Kleingütern, durch eine postalische Infrastruktur.[989] Ausgeschlossen ist die unkörperliche Übermittlung.[990] Geschützt wird der gesamte Übermittlungsvorgang im Machtbereich des Postdienstleisters von der Abgabe bis zur Ablieferung beim Empfänger.[991] Eine Besondere Schutzpflichtdimension des Postgeheimnisses ist mit der Privatisierung der Deutschen Bundespost entstanden.[992] Die Deutsche Bundespost ist nicht mehr als öffentliche Stelle Grundrechtsverpflichteter, weswegen den Staat eine besondere Schutzpflicht in diesem Bereich trifft (§§ 39 ff. PostG).[993] Er hat dafür zu sorgen, dass die Grundrechtsadressaten vor Beeinträchtigungen Dritter, auch der Postdiensteanbieter geschützt werden.[994] Das Postgeheimnis bezieht sich nicht nur auf den Universaldienst und bezieht damit auch sonstige private Postdienstleister mit ein.[995] Dessen Schutzwirkung erstreckt sich auf alle Datenverarbeitungsprozesse, die sich an die Kenntnisnahme anschließen.[996] Die Schutzwirkung erstreckt sich auch auf Private, die als Hilfspersonen der staatlichen Aufgabenerfüllung in Anspruch genommen werden.[997]

---

988 Guckelberger in Schmidt-Bleibtreu/Klein, GG, Art. 10 GG Rn. 13.

989 Löwer in v. Münch/Kunig, GG, Art. 10 GG Rn. 17; Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 4.

990 Löwer in v. Münch/Kunig, GG, Art. 10 GG Rn. 17; Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 4.

991 Löwer in v. Münch/Kunig, GG, 6. Aufl. 2012, Art. 10 GG Rn. 17; Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 4.

992 Groß, Die Schutzwirkung des Brief-, Post-, und Fernmeldegeheimnisses nach der Privatisierung der Post, in JZ 1999, S. 326 (327); Grote/Marauhn, EMRK/GG Konkordanzkommentar, 2006, Kap. 16 Rn. 21; Hermes in Dreier, GG, 3. Aufl. 2013, Art. 10 GG Rn. 48.

993 Löwer in v. Münch/Kunig, GG, Art. 10 GG Rn. 9 f.; vermittelnd Gusy in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 10 GG Rn. 28 ff..

994 So auch Hermes in Dreier, GG, Art. 10 GG Rn. 92 ff.; vermittelnd Gusy in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 10 GG Rn. 30 ff.; BVerfGE 106, S. 28/37.

995 Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 7.

996 BVerfG, Urteil vom 02.03.2010 – BvR 256/08, 1 BvR 263/07, BvR 586/08 in MMR 2010, S. 356 (358).

997 BVerfG, Urteil vom 02.03.2010 – BvR 256/08, 1 BvR 263/07, BvR 586/08 in MMR 2010, S. 356 (359).

Das Fernmeldegeheimnis schützt *„die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs“*.[998] Der Begriff der Fernmeldung ist überkommen, weswegen man heute präziser von Telekommunikation spricht.[999] Der Terminus ist entwicklungsoffen und umfasst „unkörperliche Formen der Übermittlung“, wie Kabel oder Funk, analoge, digitale, elektromagnetische, akustische oder optische Signale.[1000] Umfasst werden auch Computernetzwerke und das Internet und damit auch E-Mail-Verkehr.[1001] Die Eröffnung des Schutzbereichs richtet sich in diesen Fällen nach dem Adressaten der Information. Die Qualität der Information und ob sie politisch, privat oder geschäftlich ist, ist dabei unerheblich.[1002] Frei verfügbare an die Allgemeinheit gerichtete Informationen fallen im Gegensatz zu Nachrichten an bestimmte Personen nicht in den Schutzbereich.[1003]

Geschützt wird der Übermittlungsvorgang vom Absenden bis zum Empfang.[1004] Insbesondere werden auch die Art und Weise der Kommunikation sowie die Übermittlungsdaten und Ort und Zeit der Kommunikation vom Schutzbereich umfasst.[1005]

Die Risikoanalyse und Verwendung von Daten kann mit Vorabinformationen vollzogen werden, bevor sie in den Machtbereich der Post gelangen und fiele so

---

998 BVerfGE 115, S. 166/182; 124 43/54.

999 BVerfGE 106, S. 28/36; Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 5; so auch Hermes in Dreier, GG, 3. Aufl. 2013, Art. 10 GG Rn. 36 f.

1000 BVerfGE 106, S. 28/36; 120, 274/307; 124, 43/54; Hermes in Dreier, GG, Art. 10 GG Rn. 36; vermittelnd Gusy in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 10 GG Rn. 60; Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 5.

1001 Gusy in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 10 GG Rn. 60 ff.; BVerfGE 120, S. 274/307; Löwer in v. Münch/Kunig, Grundgesetz, 6. Aufl. 2012, Art. 10 GG Rn. 19 f.; Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 5; Guckelberger in Schmidt-Bleibtreu/Klein, GG, Art. 10 GG Rn. 27.

1002 Hermes in Dreier, GG, Art. 10 GG Rn. 41.

1003 Löwer in v. Münch/Kunig, GG, Art. 10 GG Rn. 6; vermittelnd Gusy in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 10 GG Rn. 64.

1004 Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 5.

1005 BVerfGE 115, S. 166/183; 121, 1/22; Jarass, Art. 10 GG in Jarass/Pieroth, GG, 12 Aufl., 2012 Rn. 9; Löwer in v. Münch/Kunig, GG, Art. 10 GG Rn. 24 f.

unter das Briefgeheimnis. Sie kann jedoch auch erst im Machtbereich der Post mit später erhobenen Daten vollzogen werden und fiele so unter das Postgeheimnis. §41a PostG legt sich auf keinen Verfahrensablauf fest. Daher sind beide Varianten denkbar und das Brief- wie auch das Postgeheimnis könnten betroffen sein. Während das Briefgeheimnis jedoch nur Briefe als solche schützt, schützt das Postgeheimnis alle Postsendungen. Das Postgeheimnis erstreckt sich auf alle Datenverarbeitungsprozesse durch die Post, vor deren Folgen der Staat Dritte zu schützen hat.

Durch die Einheitlichkeit des Grundrechtsschutzes ist folglich der Schutzbereich des Brief- und Postgeheimnisses eröffnet.

b) Eingriffe in den Schutzbereich

Grundsätzlich ist es allen Grundrechtsverpflichteten untersagt *„Vorkehrungen zum Schutz der Vertraulichkeit von Kommunikation zu beeinträchtigen“.*[1006]

„Ein Grundrechtseingriff ist jede Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten sowie jede Auswertung ihres Inhalts oder sonstige Verwendung durch die öffentliche Gewalt.“[1007] Das Anordnen solcher Maßnahmen und ihre Ermöglichung gelten ebenfalls als Eingriff.[1008] Eine Beeinträchtigung liegt ebenfalls vor, wenn die Übermittlungsdaten erfasst oder gespeichert werden.[1009] Nicht als Eingriff gewertet wird die Verhinderung von Kommunikation.[1010] Als Eingriff zu qualifizieren sind hingegen betriebsbedingte Maßnahmen.[1011] Bei

---

[1006] Vermittelnd Gusy in v. Mangoldt/Klein/Starck, GG, Bd. 1, Art. 10 GG Rn. 35.

[1007] BVerfG, Urteil vom 02.03.2010 – BvR 256/08, 1 BvR 263/07, BvR 586/08 in MMR 2010, S. 356 (358 f.).

[1008] BVerfGE 124, S. 43/58; 100, 313/366; Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 11; anderer Ansicht ist wohl der BGH, NJW 1994, S. 596 (598).

[1009] BVerfGE 110, S. 33/52 f.; BverfGE 100, S. 313/358 ff.; Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 11 ff.

[1010] Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 12; Hermes in Dreier, GG, Art. 10 GG Rn. 82; anderer Ansicht ist Durner in Maunz/Dürig, GG, Art. 10 Rn. 53.

[1011] Pieroth/Schlink/Kingreen/Poscher, Grundrechte Staatsrecht II, 33. Aufl. 2017 Heidelberg, § 19. Rn. 898 ff.; BVerfGE 124, 43/58.

„gestaffelten" Eingriffen (z. B. Erhebung, Abruf durch ein Behörde, Übermittlung etc.) bedarf jeder einzelne Schritt einer Rechtfertigung.[1012]

Aufgrund der ausgeprägten Dimension der Schutzpflicht kommt in besonderer Weise auch ein Unterlassen als Eingriff in Frage.

Ein Eingriff läge hier durch die Verletzung der Schutzpflicht des Gesetzgebers vor, Dritte vor der Datenverarbeitung die § 41a PostG ermöglicht, zu schützen.

c) Rechtfertigung von Eingriffen in den Schutzbereich

Art. 10 Abs. 2 GG enthält einen allgemeinen Gesetzesvorbehalt sowie eine besondere Eingriffsermächtigung zum Staats- und Verfassungsschutz.

aa) Gesetzesvorbehalt

Art. 10 Abs. 2 S. 1 GG enthält einen allgemeinen Gesetzesvorbehalt. Dieser kann durch ein förmliches Gesetz erfüllt werden, jedoch auch durch eine formell-gesetzliche Ermächtigung durch Rechtsverordnung, Satzung oder einen Verwaltungsakt.[1013] Die Gesetzgebungskompetenz für das Post- und Telekommunikationswesen ist eine ausschließliche Bundeskompetenz gemäß Art. 73 Abs. 1 Nr. 7 GG.[1014] Ländergesetze kommen dagegen im Gefahrenabwehrrecht in Betracht.[1015]

Art. 10 Abs. 2 S. 2 GG enthält eine besondere Regelung zum Schutze der freiheitlich demokratischen Grundordnung. Diese erlaubt eine präventive heimliche Kontrolle der Kommunikation mit einer nachträglichen Kontrolle.

Zunächst wäre § 41a PostG ein auf Bundesebene verabschiedetes Parlamentsgesetz. Darüber hinaus diente § 41a PostG dem Schutze der freiheitlich demokratischen Grundordnung.

§41a PostG würde damit dem Gesetzesvorbehalt genügen.

[1012] Hermes in Dreier, GG, Art. 10 GG Rn. 67.

[1013] Jarass in Jarass/Pieroth, GG, Art. 10 Rn. 16; Löwer in v. Münch/Kunig, GG, Art. 10 GG Rn. 30; BVerfGE 125, 260/313; Hermes in Dreier, GG, 3 Aufl. 2013, Art. 10 GG Rn. 61.

[1014] Löwer in v. Münch/Kunig, GG, Art. 10 GG Rn. 31.

[1015] Löwer in v. Münch/Kunig, GG, Art. 10 GG Rn. 31.

bb) Schranken-Schranken

Bei Eingriffen zum Zwecke der Gefahrenabwehr ist besonders auf das Zitiergebot und einen eng begrenzten Verwendungszweck zu achten.[1016] Die Staatsschutzklausel wird mit Blick auf das Bestimmtheitsgebot restriktiv ausgelegt.[1017] Dafür muss sich die Gefährdung aus nachprüfbaren tatsächlichen Anhaltspunkten ergeben.[1018] Der Grundrechtseingriff muss Gemeinwohlzwecken dienen und verhältnismäßig sein.[1019] Dabei kann die Verhältnismäßigkeit einer Maßnahme von Sicherungen durch Organisation und Verfahren abhängen.[1020] Schließlich bestehen sehr hohe Hürden für eine anlasslose Speicherung personenbezogener Daten.[1021]

Zunächst wäre das Zitiergebot erfüllt („Das Brief- und Postgeheimnis nach Art. 10 des Grundgesetzes wird zu diesem Zweck eingeschränkt."). Darüber hinaus müsste der Erlaubnistatbestand verhältnismäßig sein. Bezüglich der Prüfung des legitimen Zweckes, der Geeignetheit und der Erforderlichkeit ist auf die Prüfung der Achtung des Privatlebens gemäß Art. 8 EMRK zu verweisen.[1022] Insbesondere sind der Schutz vor erheblichen Gefahren für das Gemeinwohl, die öffentliche Sicherheit sowie die postalische Lieferkette als Gemeinwohlzecke einzuordnen. Weiterhin müsste §41a PostG verhältnismäßig sein. Dafür dürfte das Schutzinteresse des Einzelnen und der Allgemeinheit am Brief- und Postgeheimnis das Sicherheitsinteresse der Allgemeinheit nicht überwiegen. Zunächst ist mit der Verarbeitung von Verkehrsdaten ein Eingriff in den Kern privater Lebensgestaltung abzulehnen.

1016 Hermes in Dreier, GG, 3. Aufl. 20013, Art. 10 GG Rn. 83.

1017 Hermes in Dreier, GG, Art. 10 GG Rn. 62 ff.; Grote/Marauhn, EMRK/GG Konkordanzkommentar, 2006, Kap. 16 Rn. 23.

1018 Grote/Marauhn, EMRK/GG Konkordanzkommentar 2006, Kap. 16 Rn. 23; BVerfGE 67, S. 157 (179).

1019 BVerfGE 67, S. 157/175; Jarass, Art. 10 GG in Jarass/Pieroth, GG, 12. Aufl., 2012 Rn. 20 f.; Guckelberger in Schmidt-Bleibtreu/Klein, GG, Art. 10 GG Rn. 43.

1020 Hermes in Dreier, GG, Art. 10 GG Rn. 71, 97.

1021 BVerfG, Urteil vom 02.03.2010 – BvR 256/08, 1 BvR 263/07, BvR 586/08 in MMR 2010, S. 356 (359); Hermes in Dreier, GG, Art. 10 GG Rn. 69.

1022 Vgl. 4. Teil. D. I. 1.) a) cc) (2).

Bei einer generalisierten präventiven Datenverarbeitung führt das Anknüpfen an tatsächliche hinreichende Anhaltspunkte zunächst nicht weiter, da gerade der gesamte Sendungsstrom von der Datenverarbeitung erfasst werden soll. Es handelt sich bei der Datenverarbeitung vielmehr um die eigentliche vorgelagerte Untersuchung, anhand derer festgestellt werden soll, ob hinreichende tatsächliche Anhaltspunkte vorliegen, um potenziell gefährdete Sendungen physisch zu untersuchen. Die Untersuchung, die bisher von einem Mitarbeiter eines Universaldienstleisters durch optische Begutachtung vollzogen wurde, würde so durch eine informatorische Komponente ersetzt oder ergänzt. Eine Feststellung tatsächlich hinreichender Anhaltspunkte setzt eine vorangegangene Untersuchung voraus.

Eine parallele Situation liegt der Vorratsdatenspeicherung zugrunde. Hier werden Verkehrsdaten verdachtslos flächendeckend verarbeitet.[1023] Dafür muss jedoch ein bestimmter Rahmen gewahrt sein. Die Datensammlung muss einen Datensicherheitsstandard gewährleisten. Der Datenzugriff ist nur für hochrangige Gemeinwohlbelange zulässig. Diese Anforderungen müssten im Rahmen der Verhältnismäßigkeitsprüfung der § 41a PostG umsetzenden Maßnahme zu beachten sein und sind mit der Verhältnismäßigkeitsprüfung im Gesetz angelegt.

Weiterhin sicherte die Kontrolle durch ein unabhängiges Gremium die Verfassungsmäßigkeit des Verfahrens.

§ 41 a PostG wäre demnach angemessen und somit verhältnismäßig.

4. Zwischenergebnis

§ 41a PostG würde demnach nicht gegen Grundrechte, insbesondere Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 sowie Art. 10 GG verstoßen.

IV. Zwischenergebnis

§ 41a PostG wäre auf allen Grundrechtsebenen grundrechtskonform.[1024]

[1023] Löwer in v. Münch/Kunig, GG, Art. 10 GG Rn. 61.

[1024] Potenzielle Konkurrenzen müssen folglich nicht entschieden werden.

5. Teil |
Résumé

A. Ausgangslage

Das Verhältnis von Freiheit zu Sicherheit wird grundsätzlich durch die grundrechtlichen Gewährleistungen vorgegeben. Neben unantastbaren Kernbereichen des Grundrechtsschutzes gilt es durch Abwägung der betroffenen Interessen einen möglichst optimalen Ausgleich zwischen den verschiedenen Rechtsgütern herzustellen. Der Maßstab und die Wertungen, an denen es sich zu orientieren gilt, sind in Jahrzehnten durch die Lehre und die Rechtsprechung auf verschiedenen Ebenen entwickelt worden und ergeben heute ein engmaschiges Netz. Trotzdem bedürfen diese Vorgaben einer Übersetzung in konkrete und bestimmte Rechtsvorschriften und Ermächtigungsgrundlagen. Je tiefer der Grundrechtseingriff ist, desto detaillierter und konkreter muss die Ermächtigungsgrundlage ausgestaltet sein. Auf Handlungsgebieten wie der elektronischen Datenverarbeitung, die einem beschleunigten Wandel unterliegen, führt dies zu einem vermehrten und ständigen Bedarf an neuem und angepasstem legislatorischen Handeln. Die „Halbwertszeit" rechtlicher Vorgaben wird dabei immer kürzer. Die Geschwindigkeit von Gesetzgebungsverfahren kann gerade im europäischen Kontext damit kaum „schritthalten". Darüber hinaus führt die Spezialisierung und die Ausdifferenzierung der Fachgebiete zu einem erhöhten Bedarf an Expertise, die Prozesse weiter verlangsamt und eine tatsächliche demokratische Kontrolle durch die Legislative immer weiter erschwert. Die steigende Komplexität des Wortlautes von Regelungen führt zudem dazu dass die Betroffenen – insbesondere „normale" Bürger – ihre Rechte und Pflichten aus den Gesetzen kaum noch ablesen können. In der Summe resultiert daraus, dass der Gesetzgeber den technischen Entwicklungen hinterherhinkt und

vor der kaum lösbaren Aufgabe steht, zügig Regelungen zu erlassen, die auf der einen Seite detailliert und bestimmt Sachverhalte lösen und auf der anderen Seite für jedermann klar und verständlich sind. Dort, wo die gesetzlichen Regelungen der technischen Realität noch nicht angepasst wurden, stehen die beteiligten Akteure vor der Herausforderung, innerhalb des geltenden Rechts praxistaugliche Antworten auf drängende Fragen zu finden.

B. Betroffene Rechtsgebiete

Besonders an der Schnittstelle mehrerer Rechtsgebiete, wie in diesem Fall des Zoll-, Datenschutz- sowie des Postrechts wird deutlich, dass der Austausch zwischen den Rechtsgebieten, nicht immer jede Entwicklung des jeweils anderen Rechtsgebietes berücksichtigt, sodass die verschiedenen gesetzlichen Grundlagen gemeinsam betrachtet und zu einem Ausgleich gebracht werden müssen.

Die Komplexität des Themas gründet dabei in mehreren Entwicklungen, die sich gleichzeitig vollziehen und zu einem Ausgleich gebracht werden müssen. Auslöser des Prozesses hin zu mehr Sicherheit war die veränderte Sicherheitslage Anfang dieses Jahrtausends.

Diese wurde als Erstes vom Zollrecht aufgegriffen, da der Außenhandel der EU besonders sensibel auf eine fragile Sicherheitslage im Ausland reagiert und gravierende Auswirkungen auf Handel, Wirtschaftswachstum und Wohlstand innerhalb der EU hat. Um Handelsströme zu sichern, sollte der Zoll zum Wächter an der Pforten der EU werden. Während seine fiskalische Funktion in den Hintergrund trat, gewannen Sicherheitsaspekte immer weiter an Bedeutung. Verstärkt wurde diese Entwicklung durch neue technische Entwicklungen insbesondere im Bereich der elektronischen Datenverarbeitung, die eine Erhebung und Auswertung immer größerer Datenmengen zulässt. Die Aufzeichnung von Warenströmen ermöglicht so die Erstellung von Profilen und eine Bewertung des Risikos, das von Menschen und Waren ausgehen könnte.

An dieser Stelle tangiert das Sicherheitsbedürfnis die Grundrechte juristischer und natürlicher Personen und als Ausprägung dieser das Datenschutzrecht. Deutschland hat diesen Teil des Persönlichkeitsrechts mit den Landesdatenschutzgesetzen und dem BDSG relativ früh als bedroht erkannt und gesetzlich geregelt. Der Schutz personenbezogener Daten steht dabei im Fordergrund und folgt dem Grundgedanken, dass jeder Einzelne über die Verwendung seiner Daten bestimmen soll. Dies hat zu einem generellen Verbot der Verwendung von personenbezogenen Daten mit Erlaubnisvorbehalt geführt. Die massenhafte Datenverarbeitung und die Folgen von “Big Data“ hat man damals noch nicht kommen

sehen, die heute in einem Spannungsverhältnis zu den Erlaubnistatbeständen des BDSG und anderer Datenverarbeitungsermächtigungsgrundlagen stehen.

Beide Entwicklungen treffen wie im Brennglas im Postrecht aufeinander. Auf der einen Seite steht das Bedürfnis, zügig und möglichst kostengünstig Sendungen sicher von einem Ort zum anderen zu transportieren. Auf der anderen Seite handelt es sich um einen besonders sensiblen Bereich, der mehrere Grundrechte auf verschiedenen Ebenen tangiert. Hinzu kommt, dass hier ebenfalls der Wandel zur Ökonomisierung und Privatisierung vollzogen wurde und sich die Frage nach der Datenverarbeitung und gleichzeitig der Gefahrenabwehr durch Private stellt.

C. Die Sicherheit der postalischen Lieferkette

Alle drei Rechtsgebiete gilt es bei der Entwicklung von Lösungen, die die Sicherheit der postalischen erhöhen, zu beachten. Im Mittelpunkt steht dabei eine Risikoanalyse, die mittels elektronischer Datenverarbeitung Risikoprofile von Sendungen erstellt, um den Warenstrom in risikoarme und risikoreiche Sendungen zu unterteilen und so gleichzeitig die Geschwindigkeit wie auch die Sicherheit des Sendungsstroms zu steigern.

Je nach Qualität der Daten und Prüfungsziel kommen verschiedene Konstellationen in Betracht, wer wann Daten erhebt, verarbeitet und nutzt. Eine Risikoanalyse zu diesem Zweck durch die Post und die damit verbundenen Möglichkeiten der Datenverarbeitung auf Seiten der Post hat der Gesetzgeber jedoch bei den bisherigen Gesetzesnovellen nicht mitberücksichtigt. So besteht bisher mit Art. 46 UZK lediglich eine Ermächtigungsgrundlage zur Datenverwendung zwecks Risikoanalyse durch den Zoll. Die allgemeinen Ermächtigungsgrundlagen des BDSG, die der DPAG eine Verwendung von Daten zu Zwecken der allgemeinen Gefahrenabwehr ermöglichen könnten, werden durch die spezielleren Regelungen des Postrechts verdrängt und gesperrt. In diesem Bereich der Kommunikation hat der Gesetzgeber über § 39 PostG nicht nur die Verwendung personenbezogener Daten gesperrt, sondern ebenfalls die von Sachdaten.

D. Grundrechtsschutz

Zwingend ist dies nicht, der grundrechtliche Rahmen ließe eine Verwendung von Daten zu Zwecken der Gefahrenabwehr durch Private zu. Denkbar ist dies in Form einer Beleihung oder einer allgemeinen Ermächtigungsgrundlage. Maßgeblich für die Grundrechtskonformität ist die Ausgestaltung der Ermächtigungsgrundlage sowie ausreichende Kontrollmöglichkeiten. Im Ergebnis gilt es moderne Datenschutzstandards sicherzustellen, unabhängig davon, ob es sich um private oder staatliche Stellen handelt. Ein größtmöglicher Schutz personenbezogener Daten und damit der Persönlichkeitsrechte soll durch technische und organisatorische Maßnahmen sowie einen möglichst sparsamen Einsatz personenbezogener Daten sichergestellt werden.

So ist es möglich, die Bürger in ihren Grundrechten zu schützen und gleichzeitig die Sicherheit ihrer Kommunikation zu gewährleisten.

Literaturverzeichnis

Altmannsperger, Hans Joachim, Postrecht, 3. Aufl. 1985, Heidelberg, zitiert: Altmannsperger

Auernhammer, Herbert, Bundesdatenschutzgesetz, 4. Aufl. 2014, zitiert: Auernhammer, BDSG

Badura, Peter/von Danwitz, Thomas/Herdegen, Matthias/Sedemund, Joachim/Stern, Klaus, Beck'scher PostG-Kommentar, München 2004, zitiert: Bearbeiter in Badura/von Danwitz/Herdegen/Sedemund/Stern, Beck'scher PostG-Kommentar

Battis, Ulrich, Beleihung anläßlich der Privatisierung der Postunternehmen, in FS Peter Raisch zum 70. Geburtstag 1995, S. 355

Benz, Hanspeter, Die verfassungsrechtliche Zulässigkeit der Beleihung einer Aktiengesellschaft mit Dienstherrenbefugnissen, Dissertation, Tübingen 1995, S. 28f.

Bergmann, Lutz/Möhrle, Roland/Herb, Armin, Datenschutzrecht, Loseblattsammlung, Stand Januar 2014, zitiert: Bergmann/Möhrle/Herb, Datenschutzrecht

Bericht der Kommission an den Rat und das Europäische Parlament, KOM(1998) 471 endg. Vom 24.07.1998 über die Durchführung des Programms Zoll 2000

Bernsdorff, Norbert, Soziale Grundrechte in der Charta der Grundrechte der Europäischen Union, in VSSR 2001

Bizer, Johann, Datenschutz als Gestaltungsaufgabe, in DuD 2007, S. 725

Bracher, Christian-Dietrich, Gefahrenabwehr durch Private, Berlin 1987

Britz, Gabriele, Vertraulichkeit und Integrität informationstechnischer Systeme, in DÖV 2008, S. 411

Brühann/Wezembeek-Oppem, Mindeststandards oder Vollharmonisierung des Datenschutzes in der EG – Zugleich ein Beitrag zur Systematik von Richtlinien zur Rechtsangleichung im Binnenmarkt in der Rechtsprechung des Europäischen Gerichtshofs, in EuZW 2009, S. 639

Callies, Christian, Europa als Wertegemeinschaft – Integration und Identität durch europäisches Verfassungsrecht, in JZ 2004, S. 1033

Callfies, Christian/Ruffert, Matthias, EUV-AEUV, 5. Aufl. 2016 München, zitiert: Bearbeiter in Callies/Ruffert, EUV

Caspar, Johannes, Geoinformationen und Datenschutz am Beispiel des Internetdienstes Google Street View, in DÖV 2009, S. 965

Cavoukian, Ann, Privacy by Design, The 7 Foundational Principles, Toronto 2010

Däubler, Wolfgang/Klebe, Thomas/Wedde, Peter/Weichert, Thilo, Bundesdatenschutzgesetz, 5. Aufl., 2016 Frankfurt/Main, zitiert: Bearbeiter in Däubler/Klebe/Wedde/Weichert, BDSG

Degenhart, Christoph, Das allgemeine Persönlichkeitsrecht, Art. 2 I i.V. mit Art. 1 I GG, in JuS 1992, S. 361

Dreier, Horst, Grundgesetz, Bd. I, 3. Aufl. 2013, zitiert: Bearbeiter in Dreier, GG

Dreier, Horst, Grundgesetz, Bd. III, 3. Aufl. 2018, zitiert: Bearbeiter in Dreier, GG

Drews, Bill/Wacke, Gerhard/Martens,Wolfgang, Gefahrenabwehr Bd. 2, zitiert: Bearbeiter in Besonderes Verwaltungsrecht

Ehlers, Dirk, Europäische Grundrechte und Grundfreiheiten, 4. Aufl. 2014, zitiert: Bearbeiter in Ehlers, GuG

Eidenmüller, Alfred, Grundlagen des Post- und Postbankrechts, Frankfurt am Main 1983

Epping, Volker/Hillgruber, Christian, Beck'scher Online-Kommentar GG, Stand 15.08.2017 München, zitiert: Bearbeiter in Epping/Hillgruber, GG

Erbs, Georg/Kohlhaas, Max, Strafrechtliche Nebengesetze, Stand: 218. Ergänzungslieferung 2018, zitiert: Bearbeiter in Erbs/Kohlhaas, Strafrechtliche Nebengesetze

Frenz, Walter, Handbuch Europarecht, Bd. 4, 2009 Berlin, Heidelberg

Fuchs, Karl, Modernisierter Zollkodex und Komitologie, in ZfZ 2011, S. 282f.

Gola, Peter/Schomerus, Rudolf, BDSG, 12. Aufl. 2015, zitiert: Gola/Schomerus, BDSG

Grabenwarter, Christoph/Pabel, Katharina, Europäische Menschenrechtskonvention, 6. Aufl. 2016 München, zitiert: Grabenwarter, EMRK

Grabitz, Eberhard/Hilf, Meinhard/Nettesheim, Martin, Das Recht der Europäischen Union, Stand Januar 2017, 63. Ergänzungslieferung, zitiert: Bearbeiter in Grabitz/Hilf/Nettesheim, EUV

Grawert, Rolf, Der deutschen supranationaler Nationalstaat, in: ders. u.a. (Hrsg.), Festschrift für E.-W. Böckenförde, 1995, S. 125

Groß, Thomas, Die Schutzwirkung des Brief-, Post-, und Fernmeldegeheimnisses nach der Privatisierung der Post, in JZ 1999, S. 326

Grote/Marauhn, EMRK/GG Konkordanzkommentar, 2006 Tübingen

Harrings/Classen, EuZW 2008, S. 295, Europäische Informationsverwaltung durch behördliche Risikoanalyse, Regelungs- und Rechtsschutzdefizite beim internationalen Informationsaustausch am Beispiel des zollrechtlichen AEO Informationssystems zugleich Erwägungen zu einem unternehmensbezogenen Datenschutz

Hempel, Wolfgang (Bearbeiter), Postleidfaden. Leitfaden für die berufliche Bildung, Teil 1: Postverfassungsrecht, Heidelberg 1983

Herdegen, Matthias, Die Regulierung des Postuniversaldienstes: Abschied vom Markt?, in ZRP 1999, S. 63

Hoeren, Thomas/Sieber, Ulrich/Holznagel, Bernd, Handbuch Multimedia-Recht, Stand Januar 2018, 46. Ergänzungslieferung, zitiert: Bearbeiter in Hoeren/Sieber/Holznagel

Hoffmann-Riem, Wolfgang, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, in JZ 2008, S. 1009

Hoffmann-Riem, Wolfgang, Informationelle Selbstbestimmung in der Informationsgesellschaft, in AöR 1998, S. 513

IP/08/323, Brüssel, den 27.02.2008, Veröffentlichung der Postrichtlinie markiert denn Beginn der Vollständigen Marktöffnung

IP/08/928, Brüssel dem 13.06.2008, Binnenmarkt, Kommissar McCreevy veranstaltet hochrangige Konferenz zur Postmarktreform

Isensee, Josef/Kirchhof, Paul, Handbuch des Staatsrechts, Bd. III Das Handeln des Staates, 1988 Heidelberg, zitiert: Bearbeiter in Isensee/Kirchhof, Handbuch des Staatsrechts, Bd. III

Jarass, Hans, Charta der Grundrechte der Europäischen Union, 3. Aufl., 2016 München, zitiert: Jarass, EU-Grundrechte

Jarass, Hans/Pieroth, Bodo, Grundgesetz für die Bundesrepublik Deutschland, 14. Aufl. 2016, zitiert: Bearbeiter in Jarass/Pieroth, GG

Kämmerer, Ludwig, Die Rechtsgrundlagen des Weltpostvereins in Jahrbuch des Postwesens 1959

Karpenstein, Ulrich/Mayer, Franz, MRK, 2 Aufl. 2015 München, zitiert: Bearbeiter in Karpenstein/Mayer EMRK

Kilian, Wolfgang/Heussen, Benno, Computerrechts-Handbuch, Loseblatt. 3, 3. Ergänzungslieferung 17, zitiert: Bearbeiter in Kilian/Heussen CHB

Kirchhof, Paul, Verwalten durch „mittelbares" Einwirken, 1977

Kloepfer, Martin/Breitkreutz, Katharina, Videoaufnahmen und Videoaufzeichnungen als Rechtsproblem, in DVBL 1998, S. 114

KOM (2001) 51 endgültig, Strategie für die Zollunion

KOM (2003) 452 endgültig, Mitteilung der Kommission

KOM (2008) 884 endgültig, Bericht der Kommission an den Rat und das Europäische Parlament über die Anwendung der Postrichtlinie

Krüger, Christian/Polakiewicz, Jörg, Vorschläge für ein kohärentes System des Menschenrechtsschutzes in Europa, in EuGRZ 2001, S. 92

Kugelmann, Dieter, Der Schutz privater Individualkommunikation nach der EMRK in EuGRZ 2003, S. 16

Lenaerts, Koen, Die EU-Grundrechtecharta: Anwendbarkeit und Auslegung, in EuR 2012, S. 3

Leupold, Andreas/Glossner, Silke, Münchener Anwaltshandbuch, IT-Recht, 3. Aufl., München 2013, zitiert: Bearbeiter in Leupold/Glossner MAH IT-Recht

Lindner, Josef Franz, Grundrechtsschutz in Europa – System einer Kollisonsdogmatik, in EuR 2007 Heft 2, S. 160

Listl, Joseph, Handbuch des Kirchenrechts, 2. Aufl. 1999, zitiert: Bearbeiter in Listl, Handbuch des Kirchenrechts

Lux, Michael/Larrieu, Pierre-Jacques, Der Vorschlag für einen modernisierten Zollkodex – Teil I, in ZfZ 2006, S. 301ff.

Lux, Michael/Larrieu, Pierre-Jacques, Der Vorschlag für einen modernisierten Zollkodex – Teil II, in ZfZ 2006, S. 340

v. Mangoldt, Hermann/Klein, Friedrich/Starck, Christian, Das Bonner Grundgesetz, Bd. 1, 7. Aufl., 2018, zitiert: Bearbeiter in v. Mangoldt/Klein/Starck, GG, Bd. 1

v. Mangoldt, Hermann/Klein, Friedrich/Starck, Christian, Das Bonner Grundgesetz, Bd. 2, 7. Aufl., 2018, zitiert: Bearbeiter in v. Mangoldt/Klein/Starck, GG, Bd. 2

v. Mangoldt, Hermann/Klein, Friedrich/Starck, Christian, Das Bonner Grundgesetz, Bd. 3, 7. Aufl., 2018, zitiert: Bearbeiter in v. Mangoldt/Klein/Starck, GG, Bd. 3

Maunz, Theodor/Dürig, Günter, Grundgesetz-Kommentar, 81. Ergänzungslieferung, München 2017, zitiert: Bearbeiter in Maunz/Dürig, GG

Mehde, Veith, Gespaltener Grundrechtsschutz in der EU?, in EuGRZ 2008, S. 269

Meyer, Jürgen, Charta der Grundrechte der Europäischen Union, 4. Aufl. 2014, zitiert: Bearbeiter in Meyer, EU-GrCh

Mitteilung der Kommission an den Rat KOM (93) 632 endgültig „Die optimale Gestaltung des Binnenmarkts : Strategisches Programm" vom 22. Dezember 1993

Münch, Ingo/Kunig, Philipp, Grundgesetz, 6. Aufl. 2012, zitiert: Bearbeiter in Münch/Kunig, GG

Naumann, Kolja, Art. 52 Abs. 3 GrCh zwischen Kohärenz des europäischen Grundrechtsschutzes und Autonomie des Unionsrechts, in EuR 2008, S. 424

Nicolaysen, Gert, Die gemeinschaftsrechtliche Begründung von Grundrechten, in EuR 2003, 719f.

Ohnheiser, Ferdinand, Postrecht, 4. Aufl., Heidelberg 1984, zitiert: Ohnheiser, Postrecht

Ossenbühl, Fritz, Vorsorge als Rechtsprinzip im Gesundheits-, Arbeits- und Umweltschutz, NVwZ 1986, S. 161.

Pache, Eckhard/Rösch, Franziska, Die neue Grundrechtsordnung der EU nach dem Vertrag von Lissabon, in EuR 2009, S. 769

Pechstein, Matthias, Entscheidungen des EuGH, 7. Aufl. 2012 Tübingen

Peters, Anne/Altwicker, Tilman, Europäische Menschenrechtskonvention, 2. Aufl., 2012 München, zitiert: Peters, EMRK

Pieroth, Bodo/Schlink, Bernhard/Kingreen, Thorsten/Poscher, Ralf, Grundrechte Staatsrecht II, 33. Aufl. 2017 Heidelberg

Plath, Kai-Uwe, Bundesdatenschutzgesetz (BDSG), 2. Aufl. Köln 2016, zitiert: Bearbeiter in Plath, BDSG

Reflexionspapier des Gerichtshofes der Europäischen Union zu bestimmten Aspekten des Beitritts der Europäischen Union zur Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten, Luxemburg, den 5. Mai 2010

Rengeling, Hans-Werner/Szczekalla, Peter, Grundrechte in der Europäischen Union – Charta der Grundrechte und Allgemeine Rechtsgrundsätze, 2004

Reuter, Andrea, Modernisierung des Modernisierten Zollkodex, in ZfZ 2012, S. 149f.

Rogall, Klaus, Informationsbegriff und Gesetzesvorbehalt im Strafprozessrecht, 1992 Tübingen

Roßnagel, Alexander, Datenschutz in der künftigen Verkehrstelematik, in NVZ 2006, S. 281

Roßnagel, Alexander, Handbuch Datenschutzrecht, München 2003, zitiert: Bearbeiter in Roßnagel, Datenschutzrecht

Rost, Martin/Bock, Kirsten, Privacy by Design und die Neuen Schutzziele, in DuD 2011, S. 30

Rüsken, Reinhart, Zollrecht, Recht des grenzüberschreitenden Warenverkehrs, Loseblattsammlung, Stand: 12/2013, zitiert: Bearbeiter in Rüsken, Zollrecht

Sachs, Michael, Grundgesetz Kommentar, 7. Aufl., München 2014, zitiert: Bearbeiter in Sachs, GG

Schaar, Peter, Privacy by Design in Identity, in the Information Society, Quelle: www.bfdi.bund.de/SharedDocs/Publikationen/EN/0610EUPrivacyByDesign.pdf?__blob=publicationFile, (Abrufdatum 10.08.2014)

Schaffland, Hans-Jürgen/Wiltfang, Noeme, Bundesdatenschutzgesetz, Loseblattsammlung, Stand Juni 2014, zitiert: Schaffland/Wiltfang, BDSG

Schild, Hans-Hermann/Ronellenfitsch, Michael/Arlt, Ute/Dembowski, Barbara/Müller, Ulrike/Piendl, Robert/Rydzy, Wilhelm/Schriever-Steinberg, Angelika/Topp, Cornelia/Wehrmann, Rüdiger/Wellbrock, Rita, Praxis der Kommunalverwaltung, Bd. B16, zitiert: Schild/Ronellenfitsch/Arlt/Dembowski/Müller/Piendl/Rydzy/Schriever-Steinberg/Topp/Wehrmann/Wellbrock, Praxis der Kommunalverwaltung

Schmahl, Stefanie, Grundrechtsschutz im Dreieck von EU, EMRK und nationalem Verfassungsrecht, in EuR 2008 Heft Beiheft 1, S. 7

Schmidt-Bleibtreu, Bruno/Klein, Franz/Hofmann, Hans/Henneke, Hans-Günter, GG Kommentar zum Grundgesetz, 13. Aufl., Köln 2014, zitiert: Bearbeiter in Schmidt-Bleibtreu/Klein, GG

Schmitz, Thomas, Die Grundrechtecharta als Teil der Verfassung der Europäischen Union, in EuR 2004, S. 691

Schoch, Friedrich/Schneider, Jens-Peter/Bier, Wolfgang, Verwaltungsgerichtsordnung, 33. Ergänzungslieferung, Juni 2017 München, zitiert: Bearbeiter in Schoch/Schneider/Bier, VwGO

Schwarz, Otfried/Wockenfoth, Kurt, Zollrecht, Loseblattsammlung, Stand: 79. Ergänzungslieferung, 02/2016, zitiert: Schwarz/Wockenfoth, Zollrecht

Schwarze, Jürgen, EU-Kommentar, Baden-Baden 2012, zitiert Bearbeiter in Schwarze, EU

Simitis, Spiros, Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden 2014, zitiert: Bearbeiter in Simitis, BDSG

Sodan, Helge, Grundgesetz Beckscher Kompakt-Kommentar, 4. Aufl. München 2018, zitiert: Bearbeiter in Sodan, Grundgesetz Beckscher Kompakt-Kommentar

Spindler, Gerald/Schuster, Fabian, Recht der elektronischen Medien, § 4 BDSG, 3. Aufl. 2015, zitiert: Spindler/Schuster, Recht der elektronischen Medien

Steiner, Udo, Der beliehene Unternehmer, in JuS 1969, S. 69

Stern, Klaus, Der allgemeine Privatsphärenschutz durch das Grundgesetz und seine Parallelen im internationalen und europäischen Recht in: Festschrift für Georg Ress, 2005, S. 1259

Stern, Klaus, Postreform zwischen Privatisierung und Infrastrukturgewährleistung, in DVBL 1997, S. 309

Stober, Rolf/Moelle, Henning/Müller-Dehn, Christian, Postgesetz in Stern, Postrecht der Bundesrepublik, Loseblattsammlung, Stand März 2000, zitiert: Stober/Moelle/Müller-Dehn, in Stern Postrecht

Streinz, Rudolf, EUV/AEUV, 2. Aufl., 2012 München, zitiert: Bearbeiter in Streinz, EUV

Taeger, Jürgen/Gabel, Detlev, Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG, 2. Aufl. 2013 Frankfurt am Main, zitiert: Bearbeiter in Taeger/Gabel, BDSG

Tettinger, Peter, Das aktuelle Deutsche Postrecht, in NVwZ 2000, S. 633

Tettinger, Peter/Stern, Klaus, Kölner Gemeinschaftskommentar zur Europäischen Grundrechte-Charta, 2006 München, zitiert: Bearbeiter in Tettinger/Stern, Europäische Grundrechtecharta

Vranes, Erich, Lex Superior, Lex Specialis, Lex Posterior – Zur Rechtsnatur der „Konfliktlösungsregeln", in ZaöRV 2005, S. 391

WCO, Safe framework of standards to secure an facilitate global trade, June 2007

Weerth, Carsten, Europäische Rechtsquellen des Zollrechts, in AW-Prax 2002, S. 102.

WIK – Consult, Study on the External Dimension oft he EU Postal Acquis

Witte, Markus, Risikomanagement im Zollrecht – rechtliches Neuland oder bekanntes Terrain?, S. 41ff.

Witte, Peter, Der neue Zollkodex der EU, in AW-Prax 2012, S. 125

Witte, Peter, Zollkodex 2005 Teil 1, in AW-Prax 2005, S. 236

Witte, Peter, Zollkodex 2005 Teil 2, in AW-Prax 2005, S. 284

Witte, Peter, Zollkodex, 6. Aufl. München 2013, zitert, Bearbeiter in Witte, ZK

Witte, Peter/Wolffgang, Hans-Michael, Lehrbuch des Europäischen Zollrechts, 8. Aufl., 2016

Wronka, Georg, Datenschutzrechtliche Aspekte beim Postversand, in RDV 2011, S. 123

Grundlagen und Grenzen der Risikoanalyse zum Zwecke der allgemeinen Gefahrenabwehr innerhalb der postalischen Lieferkette

Zbigniew Adam Strzoda

Angesichts terroristischer Bedrohungen ist der offene Lebensstil freiheitlich demokratischer Gesellschaften zunehmenden Sicherheitsrisiken ausgesetzt. Um das Merkmal einer offenen Gesellschaft zu wahren, bedarf es einer Austarierung von Freiheit und Sicherheit. Lebensader unserer modernen Industrie- und Informationsgesellschaft ist der Fluss von Waren und Informationen rund um den Globus. An dieser Stelle ist die Gesellschaft besonders verwundbar und gleichzeitig auf Offenheit besonders angewiesen. Fraglich erscheint daher, inwieweit unsere Kommunikations- und Transportsysteme auf diese neuen Gefahren vorbereitet sind. Die Auswertung von Informationen zwecks Risikoanalyse soll helfen, der Flut an Informationen Herr zu werden, und durch gezielte weitergehende Untersuchungen Sicherheit gewährleisten. Ob und inwieweit die betroffenen Rechtsgebiete darauf vorbereitet sind und wie Lösungen grundrechtskonform ausgestaltet werden können und müssen, ist Teil dieser Arbeit.

25,80 €
ISBN 978-3-8405-0191-3