Zu den Neuerungen im Datenschutzrecht der Europäischen Union

Datenschutzgrundverordnung, Richtlinie zum Datenschutz in der Strafverfolgung und Implikationen für die Schweiz

Astrid Epiney / Markus Kern

Dieser Beitrag wurde erstmals wie folgt veröffentlicht:
***Astrid Epiney/Markus Kern*, Zu den Neuerungen im Datenschutzrecht der Europäischen Union: Datenschutzgrundverordnung, Richtlinie zum Datenschutz in der Strafverfolgung und Implikationen für die Schweiz, in: Astrid Epiney/Daniela Nüesch (Hrsg.), Die Revision des Datenschutzes in Europa und die Schweiz / La révision de la protection des données en Europe et la Suisse, Zürich 2016, S. 39-76. Es ist möglich, dass diese publizierte Version – die allein zitierfähig ist – im Verhältnis zu diesem Manuskript geringfügige Modifikationen enthält.**

Inhaltsübersicht

A. Einleitung

Das Datenschutzrecht in der Europäischen Union hat sich in den letzten Jahren in verschiedener und durchaus bemerkenswerter Weise weiterentwickelt. Zahlreiche

dieser Entwicklungen beruhen auf wegweisenden Urteilen des Europäischen Gerichtshofs, der die datenschutzrechtlichen Vorgaben insbesondere der RL 95/46[1] ausgelegt hat.[2] Darüber hinaus wurde jüngst der rechtliche Rahmen des Datenschutzrechts in der EU als solcher – nach jahrelangen und, aufgrund divergierender Auffassungen zwischen den massgeblichen Akteuren, nicht immer einfachen Vorarbeiten – mit der Annahme der sog. Datenschutzgrundverordnung[3] sowie der Richtlinie zum Datenschutz in der Strafverfolgung[4] grundlegend modifiziert. Diese neuen Rechtsakte knüpfen zwar an die bestehenden Regelungen an, so dass insbesondere auch die bisherige, zur RL 95/46 ergangene Rechtsprechung im Wesentlichen nach wie vor relevant ist; jedoch sind sowohl in struktureller als auch in inhaltlicher Hinsicht durchaus bedeutende Weiterentwicklungen zu konstatieren, die auch Implikationen für und in der Schweiz entfalten.

Ziel des vorliegenden Beitrags ist es vor diesem Hintergrund, die wesentlichen Neuerungen im Unionsrecht zu erörtern, wobei zwischen der Datenschutzgrundverordnung (B.) und der Richtlinie zum Datenschutz in der Strafverfolgung (C.) zu unterscheiden ist. Auf dieser Grundlage ist nach den Implikationen für die Schweiz zu fragen (D.), bevor der Beitrag mit einer kurzen Schlussbemerkung schliesst (E.).

B. Zur Datenschutzgrundverordnung

Der Erlass bzw. die im Dezember 2015 erfolgte politische Einigung über eine Datenschutzgrundverordnung (DGVO) erfolgte nach einem rund vierjährigen Gesetzgebungsverfahren, innerhalb desselben diverse Stellungnahmen, Entwürfe und Vorschläge eingebracht wurden. Im Folgenden wird darauf verzichtet, die Entstehungsgeschichte und die im Laufe des Gesetzgebungsverfahrens zu Tage getretenen unterschiedlichen Ansichten darzustellen;[5] vielmehr erfolgt eine Konzentration

---

1 RL 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281, 31.

2 S. insbesondere EuGH, Rs. C-293/12, ECLI:EU:C:2014:238 (Digital Rights Ireland); EuGH, Rs. C-131/12, ECLI:EU:C:2014:317 (Google Spain und Google Inc.); EuGH, Rs. C-362/14, ECLI:EU:C:2015:650 (Schrems); EuGH, Rs. C-201/14, ECLI:EU:C:2015:638 (Bara u.a./Presdientele Caseri); EuGH, Rs. C-230/14, ECLI:EU:C:2015:639 (Weltimmo/Nemzeti).

3 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119, 1.

4 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. 2016 L 119, 89.

5 Vgl. insoweit den Überblick mit Fundstellen bei *David Vasella*, DSGVO: Stand und Fundstellen, digma 2016, 28 f.; s. auch die Hinweise bei *Rolf H. Weber*, EU-Datenschutz-Grundverordnung: Kernelemente und Ausstrahlungswirkung auf die Schweiz, Jusletter IT v. 24.9.2015, Rn. 3 ff. S. ansonsten zur Datenschutzgrundverordnung bzw. zu den jeweiligen Vorschlägen z.B. *Markus Kern*, Datenschutzrevision in der EU: Neuer Wein? Neue Schläuche?, digma 2013, 30 ff.; *Peter Blume*, The Public Sector and the Forthcoming EU Data Protection Regulation, EDPL 2015, 32 ff.; *Jan Philipp Albrecht*, Die EU-Datenschutzgrundverordnung rettet die informationelle Selbstbestimmung!, ZD 2013, 587 ff.;

auf die Analyse zentraler Neuerungen des nunmehr beschlossenen Rechtsakts, wobei ggf. (d.h. soweit sachdienlich) auf Aspekte der Entstehungsgeschichte hingewiesen wird.

Deutlich wird damit auch, dass im Folgenden keine Vollständigkeit angestrebt wird, sprengte dies doch angesichts der insgesamt 99 Artikel und des Umfangs von 88 Seiten der Verordnung im Amtsblatt (die RL 95/46 umfasst 20 Seiten) den Rahmen des vorliegenden Beitrags. So erfolgt eine Beschränkung auf einige, nach Ansicht der Autoren, zentrale Aspekte der Verordnung, wobei die diesbezügliche Auswahl in erster Linie einerseits auf der Bedeutung für die Grundstruktur bzw. Grundausrichtung der Verordnung und ihre Rechtswirkungen, andererseits auf besonders bedeutenden Modifikationen bzw. Weiterentwicklungen beruht.

Auf dieser Grundlage erschliessen sich die u.E. wichtigsten Inhalte bzw. Neuerungen der Verordnung – ausgehend von einem kurzen Hinweis auf die Rechtsgrundlage (I.) – durch zwei strukturell voneinander zu unterscheidenden Gesichtspunkte: die Wahl des Instruments der Verordnung (II.) sowie der Regelungsgehalt der Verordnung selbst, letzteres mit Akzent auf den u.E. besonders bedeutenden Neuerungen (III.).

I. Zur Rechtsgrundlage

Die Datenschutzgrundverordnung wurde auf Art. 16 Abs. 2 AEUV gestützt.[6] Nach dieser Bestimmung werden gemäss dem ordentlichen Gesetzgebungsverfahren Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowohl durch Organe und Einrichtungen der Union als auch durch die Mitgliedstaaten sowie über den freien Datenverkehr erlassen. Dabei darf die Datenverarbeitung durch die Mitgliedstaaten nur insoweit erfasst werden, als sie die Ausübung von Tätigkeiten betrifft, die in den Anwendungsbereich des Unionsrechts fallen. Weiter fällt auf, dass in dieser Bestimmung die Datenverarbeitung durch Private nicht erwähnt wird.

Auf den ersten Blick erscheint der Anwendungsbereich dieser Rechtsgrundlage somit durchaus beschränkt. Bei näherem Hinsehen wird jedoch klar, dass datenschutzrechtliche Fragen im Ergebnis auch für die Mitgliedstaaten umfassend geregelt werden dürfen: Denn der freie Datenverkehr darf – auch soweit die Mitgliedstaaten betroffen sind, wobei darüber hinaus auch durch Private erfolgende Datenverarbeitungen erfasst sind – umfassend geregelt werden. Da aber der freie Datenverkehr bzw. die grenzüberschreitende Datenübermittlung in engem Zusammen-

Alexander Roßnagel/Philipp Richter/Maxi Nebel, Besserer Internetdatenschutz für Europa, ZD 2013, 103 ff.; *Alexander Roßnagel/Maxi Nebel/Philipp Richter,* Was bleibt vom Europäischen Datenschutzrecht? Überlegungen zum Ratsentwurf der DS-GVO, ZD 2015, 453 ff.; *Winfried Veil*, DS-GVO: Risikobasierter Ansatz statt rigides Verbotsprinzip. Eine erste Bestandsaufnahme, ZD 2015, 347 ff.; *Eugen Ehmann* (Hrsg.), Der weitere Weg zur Datenschutzgrundverordnung. Näher am Erfolg, als viele glauben?, ZD 2015, 6 ff.; *Susanne Dehmel/Nils Hullen*, Auf dem Weg zu einem zukunftsfähigen Datenschutz in Europa?, ZD 2013, 147 ff.; *Sibylle Gierschmann*, Was „bringt" deutschen Unternehmen die DS-GVO? Mehr Pflichten, aber die Rechtsunsicherheit bleibt, ZD 2016, 51 ff.; *Tim Wybitul*, Was ändert sich mit dem neuen EU-Datenschutzrecht für Arbeitgeber und Betriebsräte, ZD 2016, 203 ff.

6 Allgemein zum primärrechtlichen Rahmen *Stephan Pötters*, Primärrechtliche Vorgaben für eine Reform des Datenschutzrechts, RDV 2015, 10 ff.

hang mit dem Datenschutzniveau in den involvierten Mitgliedstaaten steht, impliziert die Befugnis zur Regelung des freien Datenverkehrs auch eine umfassende Kompetenz zur Regelung des Datenschutzes in den Mitgliedstaaten, dies grundsätzlich unabhängig davon, ob – soweit die Datenverarbeitung durch die Mitgliedstaaten betroffen ist – der Anwendungsbereich des Unionsrechts eröffnet ist. Zwar könnte gegen diesen Ansatz eingewandt werden, der systematische Zusammenhang bzw. die Aufzählung der verschiedenen Konstellationen in Art. 16 Abs. 2 AEUV lege die Annahme nahe, dass bei Datenverarbeitungen durch mitgliedstaatliche Organe immer der Anwendungsbereich des Unionsrechts eröffnet sein muss, könnte diese Einschränkung doch ansonsten leerlaufen. Zu überzeugen vermag dies freilich nicht: Denn Art. 16 Abs. 2 AEUV stellt die Kompetenz der Union zur Regelung der Datenverarbeitung durch Organe der Union und durch die Mitgliedstaaten als eigenständige Fallgestaltungen neben die Kompetenz zur Regelung des freien Datenverkehrs, was dafür spricht, dass der freie Datenverkehr eine eigenständige „Kompetenzkategorie" darstellt und als solcher geregelt werden kann, unabhängig davon, ob von diesen Regelungen öffentliche Organe oder Private betroffen sind. Nur dieser Ansatz trägt auch der grossen Bedeutung des freien Datenverkehrs für den Binnenmarkt Rechnung, könnten doch ansonsten – also soweit die Datenverarbeitung durch mitgliedstaatliche Organe betroffen ist – bedeutende Unterschiede zwischen den Datenschutzniveaus in den Mitgliedstaaten fortbestehen, womit empfindliche Beschränkungen des freien Datenverkehrs einherzugehen drohen. Vieles spricht nämlich in diesem Zusammenhang dafür, die Befugnis zur Regelung des freien Datenverkehrs als Spezifizierung der allgemeinen Binnenmarktkompetenz (Art. 114 Abs. 1 AEUV) anzusehen, stellt doch die Gewährleistung des freien Datenverkehrs aufgrund der Betroffenheit der Grundfreiheiten einen Aspekt der Verwirklichung des Binnenmarktes dar.[7]

Illustriert wurde der Zusammenhang des freien Datenverkehrs mit dem Datenschutzniveau in den Mitgliedstaaten jüngst – wenn auch in Bezug auf das Verhältnis zu den Vereinigten Staaten – durch das Urteil des Gerichtshofs in Bezug auf die sog. *Safe Harbor*-Regelung:[8] Hier stand eine grenzüberschreitende Datenübermittlung in einen Drittstaat (die USA) zur Debatte, eine Datenverarbeitung, die nach der RL 95/46 (und auch der Datenschutzgrundverordnung) nur unter bestimmten Voraussetzungen zulässig ist, wobei der Frage nach dem Bestehen eines angemessenen Datenschutzniveaus eine zentrale Bedeutung zukommt. Ein solches angemessenes Datenschutzniveau sah der Gerichtshof in den USA nicht gegeben, dies trotz der sog. *Safe Harbor*-Entscheidung der Kommission:[9] Denn obwohl die RL 95/46 nicht im Einzelnen definiere, was als angemessenes

---

7 I.Erg. ebenso *Thorsten Kingreen*, in: Christian Calliess/Matthias Ruffert (Hrsg.), EUV/AEUV, Kommentar, 5. Aufl. (im Erscheinen), Art. 16 AEUV, Rn. 4, 7. S. auch *Lorin-Johannes Wagner*, Der Datenschutz in der Europäischen Union, 2015, 162, der in Bezug auf die Befugnis der Union, Regeln über den freien Datenverkehr zu erlassen, von einem „Auffangtatbestand" spricht.

8 EuGH, Rs. C-362/14, ECLI:EU:C:2015:650 (Schrems). Der Ausgangsfall betraf die Klage eines österreichischen Staatsbürgers gegen Facebook Ireland, mittels derer er die Übermittlung seiner Daten in die USA unterbinden lassen wollte.

9 In dieser Entscheidung (Entscheidung 2000/520 gemäss der RL 95/46 über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" gewährleisteten Schutzes, ABl. 2000 L 215, 7) stellte die Kommission fest, dass eine Datenübermittlung in die USA nach den Grundsätzen des sog. *Safe Harbor* (wonach diejenigen Organisationen in den USA, an welche die Daten übermittelt werden, sich zur Einhaltung einer Reihe von datenschutzrechtlichen Grundsätzen verpflichten) ein angemessenes Schutzniveau übermittelter personenbezogener

Schutzniveau zu gelten hat, ergebe sich doch aus dem Wortlaut und dem Sinn und Zweck der Vorschriften, dass es um eine Art „Garantie“ eines solchen Schutzes gehen müsse und dass auch im Falle der Übermittlung in einen Drittstaat ein hohes Schutzniveau zu gewährleisten sei, das zwar nicht identisch mit demjenigen der RL 95/46 sein müsse, jedoch einen gleichwertigen Schutz zu bieten habe. Jeder andere Ansatz verkenne die Zielsetzung der RL 95/46 und führe zu zahlreichen Umgehungsmöglichkeiten. Im Übrigen müsse es die Rechtsordnung des Drittstaates sein, die ein solches angemessenes Schutzniveau gewährleistet, wobei die Mittel im Vergleich zu denjenigen, die in der Union herangezogen werden, anders ausgestaltet sein können, was jedoch nichts daran ändere, dass sie in der Praxis im Hinblick auf die Gewährleistung eines gleichwertigen Schutzes wirksam sein müssten. Die Kommission sei vor diesem Hintergrund zur inhaltlichen Prüfung der einschlägigen Regeln in dem betreffenden Drittstaat sowie der zur Gewährleistung der Einhaltung dieser Regeln dienenden Praxis verpflichtet. Überdies sei in regelmässigen Abständen zu prüfen, ob die Feststellung der Angemessenheit des Schutzniveaus nach wie vor gerechtfertigt ist, wobei eine solche Prüfung jedenfalls dann vorzunehmen sei, wenn Anhaltspunkte bestehen, die daran Zweifel wecken könnten. Die gerichtliche Überprüfung sei angesichts der Bedeutung der in Frage stehenden Grundrechte im Fall der Übermittlung personenbezogener Daten in Drittstaaten strikt auszugestalten und der Wertungsspielraum der Kommission entsprechend beschränkt. Ausgehend von diesen Grundsätzen erklärte der Gerichtshof die Entscheidung der Kommission für ungültig, da in den USA kein angemessenes Schutzniveau gewährleistet sei. Hauptgrund für diesen Schluss – den der EuGH auf der Grundlage einer detaillierten Analyse des Konzepts des *Safe Harbor* entwickelte – war einerseits der Umstand, dass die Selbstzertifizierung (auf der das Konzept des *Safe Harbor* beruht und das vom EuGH grundsätzlich durchaus als zulässiges Konzept angesehen wird) nicht einhergehe mit in der innerstaatlichen Rechtsordnung vorgesehenen (staatlichen) Massnahmen, die die Einhaltung der datenschutzrechtlichen Grundsätze verlangen und gewährleisten. Andererseits könnten die grundsätzlich einzuhaltenden datenschutzrechtlichen Prinzipien allgemein eingeschränkt werden, sofern dies durch Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder der Durchführung von Gesetzen begründet ist, so dass diesen Erfordernissen zudem sehr generellen Charakters letztlich Vorrang vor den datenschutzrechtlichen Grundsätzen eingeräumt werde; Anhaltspunkte für Begrenzungen von Eingriffen in die Grundrechte der Betroffenen seien nicht zu erkennen, ganz abgesehen davon, dass kein wirksamer gerichtlicher Rechtsschutz gegen Eingriffe vorgesehen sei. Insgesamt gebe es daher weder präzise Regeln über die Zulässigkeit eines Eingriffs in Art. 7, 8 GRCh noch sei der Grundsatz der Verhältnismässigkeit gewahrt. Im Übrigen verletze eine Regelung, die es gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des Art. 7 GRCh. Darüber hinaus schränke die Entscheidung die Befugnisse der nationalen Kontrollstellen ein, da sie ihnen die Möglichkeit nimmt, Massnahmen zu ergreifen, um die Einhaltung der Vorgaben für die grenzüberschreitende Datenübermittlung für den Fall zu gewährleisten, dass eine Entscheidung der Kommission das Bestehen eines angemessenen Schutzniveaus festgestellt hatte.

Deutlich wird damit der Zusammenhang zwischen einem angemessenen Datenschutzniveau in einem Staat und der Zulässigkeit einer grenzüberschreitenden Datenübermittlung bzw. dem freien Datenverkehr, kann dieser doch letztlich nur unter der Voraussetzung gewährleistet werden, dass in den beteiligten Staaten ein angemessenes Datenschutzniveau garantiert ist, würden doch ansonsten die datenschutzrechtlichen Garantien unterlaufen. Dies gilt auch – wie gerade das erwähnte Urteil illustriert, waren hier doch die weitreichenden Befugnisse der für die nationale Sicherheit zuständigen Behörden mit ausschlaggebend – allgemein in Bezug auf datenschutzrechtliche Vorgaben für Verarbeitungen durch öffentliche Organe. Verallgemeinert man diesen Gedanken, so dienen datenschutzrechtliche Regelungen notwendigerweise immer auch dem Binnenmarkt, so dass sie grundsätzlich auch auf entsprechende Rechtsgrundlagen gestützt werden können.

Vor diesem Hintergrund überrascht es auch nicht, dass der EuGH bereits die RL 95/46 als sog. Vollharmonisierung ansieht, die in ihrem Anwendungsbereich den Schutzstandard abschliessend regelt, so dass auch eine Abweichung nach oben

Daten gewährleiste und die danach erfolgende grenzüberschreitende Datenübermittlung daher den Erfordernissen der RL 95/46 entspreche.

nicht zulässig ist.[10] Ebenso stellte er in verschiedenen Urteilen klar, dass die RL 95/46 auch in Bezug auf Sachverhalte, die als solche keinerlei grenzüberschreitenden Bezüge aufweisen, anwendbar ist und somit umfassend auch Vorgaben für das rein innerstaatliche Datenschutzrecht enthält, dies z.B. im Zusammenhang mit der Veröffentlichung des Jahreseinkommens von Angestellten der öffentlichen Verwaltung[11] oder die Verarbeitung öffentlicher Daten durch öffentliche Stellen für die Anwendung aufenthaltsrechtlicher Vorschriften und statistische Zwecke.[12]

II. Zum Instrument der Verordnung

Wie bereits die Bezeichnung erkennen lässt, handelt es sich bei dem neuen Rechtsakt nicht mehr um eine Richtlinie, sondern um eine Verordnung. Verordnungen entfalten nach Art. 288 AEUV unmittelbare Geltung in den Mitgliedstaaten, so dass die Bestimmungen der Verordnung als solche in den Mitgliedstaaten anzuwenden sind und somit keiner Umsetzung bedürfen. Dies impliziert auch, dass die Verordnung Behörden und Einzelne berechtigen und verpflichten kann.

Freilich ist damit nicht ausgeschlossen, dass gewisse Bestimmungen der Verordnung der mitgliedstaatlichen Durchführung bedürfen, können Verordnungen doch Vorgaben sehr unterschiedlicher Art enthalten, so – neben direkt anwendbaren Bestimmungen – auch solche, die es den Mitgliedstaaten aufgeben, bestimmte Massnahmen zu ergreifen.[13] Ein Beispiel in der Datenschutzgrundverordnung ist die in Art. 51 ff. DGVO enthaltene Verpflichtung der Mitgliedstaaten, eine oder mehrere unabhängige Aufsichtsbehörden vorzusehen, denen bestimmte Befugnisse zukommen müssen.

Der Hintergrund für die Wahl der Verordnung als Instrument (an Stelle der Richtlinie) ist nach den Erwägungsgründen der Verordnung[14] in erster Linie darin zu sehen, dass mit der Verordnung eine weitergehende Harmonisierung erreicht werden kann, da die mit der mitgliedstaatlichen Umsetzung notwendigerweise einhergehenden Spielräume zumindest teilweise wegfallen und damit eine grössere Rechtssicherheit erzielt werden kann. Insofern impliziert der Rückgriff auf eine Verordnung ein „gleichmässigeres" Datenschutzniveau in den Mitgliedstaaten, womit dieses auch insgesamt erhöht werden dürfte; gleichzeitig führt die weitergehende Harmonisierung auch zu einer Verringerung der Wettbewerbsverzerrungen.

Anzumerken bleibt in diesem Zusammenhang, dass das „Harmonisierungsdefizit" auf der Grundlage der RL 95/46 und damit die mitunter beachtlichen Unterschiede des Datenschutzniveaus in den Mitgliedstaaten nicht nur bzw. nicht massgeblich auf der Wahl der Richtlinie als Rechtsetzungsinstrument beruhen; vielmehr dürfte der Umstand, dass die Richtlinie selbst den Mitgliedstaaten in verschiedenen

---

10 EuGH, verb. Rs. C-468/10, C-469/10, ECLI:EU:C:2011:777 (ASNEF), Rn. 30; aus der Literatur, m.w.N., *Stephan Pötters*, Primärrechtliche Vorgaben für eine Reform des Datenschutzrechts, RDV 2015, 10 (11 f.).

11 EuGH, verb. Rs. C-465/00, C-138/01, C-139/01, ECLI:EU:C:2003:294 (Österreichischer Rundfunk).

12 EuGH, Rs. C-542/06, ECLI:EU:C:2008:724 (Huber).

13 Zur Zulässigkeit solcher Bestimmungen auch in Verordnungen z.B. EuGH, Rs. C-403/98, ECLI:EU:C:2001:6, Rn. 26 (Azienda Agricola Monte Arcosu).

14 S. insbesondere Erw. 9 f. DGVO.

Bereichen ausgesprochen weite (Umsetzungs-)Spielräume einräumt (insbesondere durch die teilweise sehr offenen Formulierungen sowie die in gewissen Bereichen weitgehenden Ausnahme- bzw. Abweichungsmöglichkeiten),[15] eine ungleich grössere Rolle spielen.

In diesem Sinn dürfte denn auch in Bezug auf die mit der neuen Verordnung einhergehenden Neuerungen die im Vergleich zur RL 95/46 wesentlich weniger weitgehenden Möglichkeiten der Mitgliedstaaten, abweichende Regelungen zu erlassen bzw. die grundsätzlich zu beachtenden Vorgaben zu relativieren, von grosser Bedeutung sein.

Grundsätzlich ergibt sich schon aus der Zielsetzung der Verordnung, (auch) den freien Datenverkehr sicherzustellen, dass ihre Vorgaben grundsätzlich abschliessend zu verstehen sind, so dass die Mitgliedstaaten auch keine strengeren Schutzmassnahmen ergreifen dürfen. Allerdings enthalten verschiedene Bestimmungen der Verordnung „Erlaubnisvorbehalte", wonach es den Mitgliedstaaten offen steht, in der betreffenden Frage und im vorgesehenen Ausmass ein erhöhtes Schutzniveau anzulegen.

Schliesslich sei noch auf einen weiteren, in der Regel wenig beachteten Aspekt in diesem Zusammenhang hingewiesen: Aufgrund des Vorrangs des Unionsrechts und der unmittelbaren Geltung der Verordnung kommt dieser Vorrang vor nationalem Recht – unter Einschluss bereichsspezifischer gesetzlicher Grundlagen und Vorgaben – zu; nationales Recht ist also in jeder Beziehung und soweit möglich so auszulegen, dass es mit der Datenschutzgrundverordnung in Einklang steht; andernfalls sind die nationalen Vorschriften nicht anzuwenden.

III. Aufbau und wesentliche Neuerungen

Die Datenschutzgrundverordnung wird einige, durchaus bedeutende und ins Gewicht fallende Neuerungen mit sich bringen, auf die nachfolgend der Akzent gelegt werden wird. Gleichzeitig ist bereits an dieser Stelle darauf hinzuweisen, dass die Verordnung in verschiedener Hinsicht – insbesondere soweit die Ziele und Grundsätze betroffen sind – an die RL 95/46 anknüpft und deren Vorgaben aufnimmt, wenn auch gelegentlich mit Präzisierungen.[16] Damit einher geht die auch in der Datenschutzgrundverordnung beibehaltene „Technikneutralität" der unionsrechtlichen Vorgaben, so dass auch auf der Grundlage der neuen Verordnung keine spezifisch technischen Fragen für bestimmte Datenverarbeitungen, die auf gewisse Techniken zurückgreifen, sondern vielmehr allgemein geltende datenschutzrechtliche Anforderungen formuliert werden, wenn auch einigen Vorgaben gerade im Internetzeitalter besondere Bedeutung zukommt.[17]

Im Einzelnen erschliessen sich die wesentlich Neuerungen der Datenschutzgrundverordnung durch folgende Aspekte: Anwendungsbereich (1.), Rechte der

---

15 Vgl. hierzu im Einzelnen bereits *Astrid Epiney/Bernhard Hofstötter/Annekathrin Meier/Sarah Theuerkauf*, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen. Zur rechtlichen Tragweite der europa- und völkerrechtlichen Vorgaben und ihren Implikationen für die Schweiz, 2007, 89 ff.

16 S. insoweit auch Erw. 9 DGVO.

17 Hierzu etwa *Gernot Sydow/Markus Kring*, Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug. Konkurrierende Leitbilder für den europäischen Rechtsrahmen, ZD 2014, 271 ff.

Betroffenen (2.), Pflichten der Datenverarbeiter (3.) sowie Durchsetzung und Sanktionen (4.).

Wie bereits erwähnt, geht es im Folgenden nicht darum, den Inhalt der Verordnung als solchen vollumfänglich zu erörtern, sondern es erfolgt eine Konzentration auf die u.E. besonders wichtigen Neuerungen. Die vollständige Tragweite der insgesamt 99 Artikel, die in 11 Kapitel gegliedert sind und einen Umfang von 88 Seiten aufweisen, lässt sich anhand ihres Aufbaus erahnen:

- Kap. I (Art. 1-4) enthält die allgemeinen Bestimmungen. Neben der Umschreibung von Gegenstand und Zielen und des (sachlichen und räumlichen) Anwendungsbereichs werden hier insbesondere zentrale Begriffe definiert. Auf diese Begriffsdefinitionen ist ggf. bei der Analyse der weiteren Vorgaben der Verordnung zurückzugreifen, hängt deren Tragweite doch häufig von der genauen Bedeutung der verwandten Begriffe ab.
- In Kap. II („Grundsätze", Art. 5-11) werden in weitgehender Anknüpfung an die RL 95/46 die zentralen Prinzipien der Datenverarbeitung (unter Einschluss der Voraussetzungen für die Rechtmässigkeit einer Datenverarbeitung und der weitergehenden Anforderungen an die Verarbeitung besonders sensibler Personendaten) formuliert.
- Die Rechte der Betroffenen (Art. 12-23) sind Gegenstand des Kap. III, ein Kapitel, das im Verhältnis zu den Vorgaben der RL 95/46 in verschiedener Hinsicht wesentliche Modifikationen bzw. Weiterentwicklungen erfahren hat.
- Der Verantwortlichkeit und der Auftragsverarbeitung (Art. 24-43) ist ein eigenes Kapitel (Kap. IV) gewidmet, das eher detaillierte und in weiten Teilen neue Anforderungen an die Datenverarbeiter stellt.
- Die in Kap. V (Art. 44-50) formulierten Vorgaben für die grenzüberschreitende Datenübermittlung knüpfen weitgehend an die bisherigen Vorschriften an, fallen jedoch in verschiedener Hinsicht präziser aus.
- Auch die in Kap. VI (Art. 51-59) niedergelegten Vorschriften betreffend die unabhängigen Aufsichtsbehörden sind zwar im Vergleich zur geltenden Regelung erheblich präziser und detaillierter (und damit auch klarer) gefasst, greifen jedoch im Wesentlichen das bestehende System auf.
- Kap. VII („Zusammenarbeit und Kohärenz", Art. 60-76) betrifft einerseits die Zusammenarbeit zwischen den Aufsichtsbehörden, insbesondere im Falle der (potentiellen) Betroffenheit und Zuständigkeit mehrerer Behörden für einen Sachverhalt, andererseits die Einrichtung des „Europäischen Datenschutzausschusses", der mit eigener Rechtspersönlichkeit als Einrichtung der Union ausgestaltet ist und sich aus Vertretern der Aufsichtsbehörden jedes Mitgliedstaats und des Europäischen Datenschutzbeauftragten zusammensetzt. Damit wird die sog. „Gruppe 29" erheblich aufgewertet.
- In Kap. VIII („Rechtsbehelfe, Haftung und Sanktionen", Art. 77-84) geht es um verschiedene Aspekte der Durchsetzung der datenschutzrechtlichen Vorgaben.
- Kap. IX (Art. 85-91) enthält spezifische Vorschriften für besondere Verarbeitungssituationen (z.B. im Beschäftigungskontext oder in Archiven).
- Schliesslich enthält Kap. X die Bestimmungen betreffend delegierte Rechtsakte und Durchführungsrechsakte (vgl. insoweit Art. 290 f. AEUV), während in Kap. XI die üblichen Schlussbestimmungen figurieren. Hervorzuheben ist hier, dass die Verordnung zwar am Tag ihrer Veröffentlichung in Kraft tritt, jedoch erst zwei Jahre danach tatsächlich gilt (Art. 99 DGVO).

1. Anwendungsbereich

Während der persönliche Anwendungsbereich – insbesondere in Bezug auf die Betroffenen – keine massgeblichen Modifikationen erfährt und auch in Bezug auf den sachlichen Anwendungsbereich an die bisherigen Regelungen angeknüpft wird,[18]

[18] So findet die Verordnung auf die Verarbeitung personenbezogener Daten Anwendung, wobei diese nach der Begriffsdefinition in Art. 4 Nr. 1 DGVO nur auf natürliche Personen bezogen

wird der räumliche Anwendungsbereich im Verhältnis zur bisherigen Regelung beträchtlich ausgedehnt. Im Einzelnen unterscheidet der hier einschlägige Art. 3 DGVO zwischen drei Konstellationen:

– Nach Art. 3 Abs. 1 DGVO findet die Verordnung auf die Verarbeitung personenenbezogener Daten Anwendung, soweit diese „im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt“,[19] wobei die Verarbeitung selbst nicht in der Union stattfinden muss. Entscheidender Anknüpfungspunkt ist somit einerseits die Niederlassung in der Union, die dann vorliegt, wenn der Datenverarbeiter oder der Auftragsverarbeiter über eine feste Einrichtung mit einer gewissen Stabilität in der Union verfügt.[20] Somit kommt es wohl nicht auf den juristischen „Hauptsitz“ an, wie sich im Gegenschluss aus der Begriffsdefinition der „Hauptniederlassung“ in Art. 4 Nr. 16 DGVO ergibt, geht diese Definition doch davon aus, dass es neben der Hauptniederlassung auch sonstige Niederlassungen geben muss. Andererseits muss die Verarbeitung aber im Rahmen dieser Niederlassung erfolgen. Hierbei ist es ausreichend, dass die Verarbeitung im Zusammenhang mit einer effektiven und tatsächlichen Tätigkeit der Niederlassung steht, wobei die Tätigkeit der Niederlassung nur geringfügig sein und auch der Zusammenhang eher lose ausfallen kann.

  Die eher geringen Anforderungen in diesem Zusammenhang können anhand von zwei Urteilen des EuGH zur RL 95/46 – die insoweit auch im Rahmen der Datenschutzgrundverordnung massgeblich sind, da bereits Art. 4 Abs. 1 lit. a RL 95/46 auf die Niederlassung im Hoheitsgebiet eines Mitgliedstaates sowie die Verarbeitung im „Rahmen der Tätigkeiten einer Niederlassung“ abstellt – illustriert werden:

  – In der Rs. C-131/12 (Google)[21] setzte sich der Gerichtshof im Einzelnen mit der Eröffnung des Anwendungsbereichs der RL 95/46 auseinander und bejahte diese in Bezug auf die Tätigkeit einer Suchmaschine: Eine solche Tätigkeit sei zunächst allgemein als Datenverarbeitung im Sinne der RL 95/46 anzusehen. Diese werde im konkreten Fall auch im Rahmen der Niederlassung von Google in Spanien ausgeübt, so dass der räumliche Anwendungsbereich der RL 95/46 betroffen sei. Denn durch die Tätigkeit der Suchmaschine solle die Niederlassung in dem betreffenden Mitgliedstaat für die Förderung des Verkaufs der angebotenen Werbeflächen der Suchmaschine sorgen, mit denen die Rentabilität der Dienstleistung der Suchmaschine gewährleistet werden solle, so dass die Tätigkeiten des Suchmaschinenbetreibers und die seiner Niederlassung in dem betreffenden Mitgliedstaat untrennbar miteinander verbunden seien. Da zusammen mit den Ergebnissen auf derselben Seite die mit den Suchbegriffen verknüpften Werbeanzeigen angezeigt werden, erfolge die in Rede stehende Verarbeitung personenbezogener Daten im Rahmen der Werbetätigkeit, die von der Niederlassung, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedstaats

---

werden. Zur Rechtslage auf der Grundlage der RL 95/46 *Epiney/Hofstötter/Meier/Theuerkauf*, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen (Fn. 15), 92 ff. Hinzuweisen ist jedoch darauf, dass der Begriff der „personenbezogenen Daten“ in der Verordnung im Vergleich zur RL 95/46 genauer definiert wird, vgl. hierzu *Weber*, Jusletter IT v. 24.9.2015 (Fn. 5), Rn. 19 ff., womit jedoch keine massgeblichen Modifikationen im Vergleich zur geltenden Rechtslage einhergehen.

19 Vgl. die Definitionen der Begriffe „Verantwortlicher“ und „Auftragsverarbeiter“ in Art. 4 Nr. 7, 8 DGVO.

20 Vgl. *Nicolas Passadelis/Simon Roth*, Weisser Rauch über Brüssel. Was Schweizer Unternehmen über die europäische Datenschutz-Grundverordnung wissen müssen, Jusletter v. 4.4.2016, Rn. 10.

21 EuGH, Rs. C-131/12, ECLI:EU:C:2014:317 (Google Spain und Google Inc.).

– im vorliegenden Fall in Spanien – besitzt, ausgeübt wird. Damit ist unerheblich, dass die eigentliche Datenverarbeitung in einem Drittland – hier den USA – erfolgte.

– Der Ausgangsfall der Rs. C-230/14 (Weltimmo)[22] betraf die Verhängung eines Bussgelds durch die ungarische Kontrollbehörde gegen eine in der Slowakei ansässige Gesellschaft wegen der Verletzung des ungarischen Informationsgesetzes, das Umsetzungsgesetz der RL 95/46. Der Gerichtshof hielt zunächst fest, dass in einer solchen Konstellation nach Art. 4 RL 95/46[23] (auch) das Datenschutzrecht eines anderen Mitgliedstaats (hier Ungarn) als dem, in dem der für die Verarbeitung Verantwortliche eingetragen oder ansässig ist (hier die Slowakei), angewandt werden kann, soweit der für die Verarbeitung Verantwortliche mittels einer festen Einrichtung im Hoheitsgebiet des zuerst genannten Mitgliedstaats eine effektive und tatsächliche Tätigkeit ausübt, in deren Rahmen eine Datenverarbeitung durchgeführt wird. Eine solche Tätigkeit könne im Betreiben von Websites bestehen, die der Vermittlung von Immobilien dienen, die sich in diesem Mitgliedstaat befinden, insbesondere, wenn diese Website hauptsächlich auf diesen Mitgliedstaat ausgerichtet ist. Zu berücksichtigen sei ferner, ob der Datenverantwortliche in dem betreffenden Mitgliedstaat über einen Vertreter verfügt, der die Forderungen aus dieser Tätigkeit einziehen und den Verantwortlichen in Verwaltungs- und Gerichtsverfahren vertreten soll. Die Staatsangehörigkeit der von der Datenverarbeitung Betroffenen sei hingegen irrelevant. Soweit die Befugnisse der nationalen Kontrollstelle betroffen sind, so sei diese zwar befugt, jedwede Beschwerde einer natürlichen Person unabhängig vom anwendbaren Recht zu prüfen; die Sanktionsmöglichkeiten stünden ihr jedoch nur soweit zu, wie auch das nationale Datenschutzrecht anwendbar ist. Andernfalls muss sie die zuständige Behörde benachrichtigen.
  Der Gerichtshof legt damit den räumlichen Anwendungsbereich der RL 95/46 (übrigens unter Bezugnahme auf die Zielsetzung der Richtlinie, einen umfassenden Persönlichkeitsschutz zu gewährleisten) weit aus und geht von einem „flexiblen" Konzept der Niederlassung aus, für deren Vorliegen es offenbar auf die konkreten Umstände des Einzelfalls ankommt. Ausschlaggebend dürfte letztlich sein, ob eine echte Geschäftstätigkeit in dem betreffenden Staat ausgeübt wird und in irgendeiner Form eine spezifische Vertretung vorgesehen ist. Deutlich wird damit auch, dass die Anforderungen hier eher gering angesetzt sind, was im Übrigen nichts daran ändert, dass das flexible Konzept des Gerichtshofs durchaus Abgrenzungsprobleme mit sich bringen dürfte. Jedenfalls ermöglicht es aber einen erleichterten Zugriff auf Unternehmen, die Datenverarbeitungen im bzw. über das Internet vornehmen, und insofern steht das Urteil in der logischen Folge des Urteils in der Rs. C-131/12 (*Google Spain und Google Inc.*). Hinzuweisen ist aber auch darauf, dass auf der Grundlage des Urteils davon auszugehen ist, dass zahlreiche Unternehmen neben dem Datenschutzrecht ihres Gesellschaftssitzes auch die Vorgaben zahlreicher weiterer Mitgliedstaaten zu beachten haben, in denen sie Niederlassungen im Sinne des Urteils betreiben. Dies wird sich jedoch mit dem Inkrafttreten der Datenschutzgrundverordnung ändern, da diese unmittelbar anwendbares Recht schafft; die Grundsätze des Gerichtshofs bleiben aber in Bezug auf ausserhalb der Union ansässige Unternehmen relevant.

– Die eigentliche Neuerung der Datenschutzgrundverordnung findet sich in Art. 3 Abs. 2 DGVO: Danach findet die Verordnung auch auf die Verarbeitung der Daten von Personen („betroffene Personen"), die sich in der Union befinden, Anwendung, wenn die Datenverarbeitung „im Zusammenhang damit steht", dass den Personen Waren oder Dienstleistungen in der Union angeboten werden (unabhängig von Zahlungsflüssen) oder dass ihr Verhalten in der Union beobachtet wird. Eine Niederlassung des Daten- oder des Auftragsverarbeiters in

---

22 EuGH, Rs. C-230/14, ECLI:EU:C:2015:639 (Weltimmo/Nemzeti).

23 Wonach die Mitgliedstaaten die Umsetzungsgesetzgebung auch auf diejenigen Datenverarbeitungen anwenden, die im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaates besitzt.

der Union ist in dieser Konstellation nicht notwendig.[24] Angestrebt wird damit ein umfassenderer Schutz der Persönlichkeitsrechte der sich im Hoheitsgebiet der Union bzw. ihrer Mitgliedstaaten aufhaltenden Personen vor potentiellen Eingriffen durch ausserhalb der Union niedergelassene Datenverarbeiter.

Diese neue Bestimmung bringt eine Ausdehnung des Anwendungsbereichs der Datenschutzgrundverordnung auf Personen und Sachverhalte mit sich, die vollumfänglich ausserhalb des Hoheitsgebiets der Union bzw. ihrer Mitgliedstaaten angesiedelt sind, so dass es insofern um Normen mit extraterritorialer Wirkung geht. Damit wird die Frage nach ihrer völkerrechtlichen Zulässigkeit aufgeworfen, die aber im Ergebnis zu bejahen ist: Zwar bezieht sich die staatliche Rechtsetzung typischerweise auf das eigene Hoheitsgebiet; jedoch steht das Völkerrecht nicht allgemein dem Erlass von Rechtsnormen mit (auch) extraterritorialer Wirkung entgegen, soweit ein hinreichender Bezug bzw. ein ausreichender Anknüpfungspunkt zum eigenen Hoheitsgebiet, zum eigenen Recht oder zu den eigenen Angehörigen besteht.[25] Diese Voraussetzung ist vorliegend zu bejahen, wird doch an das Anbieten von Dienstleistungen oder Waren oder das Beobachten von Personen, jeweils in der Union, abgestellt, und es werden im Anschluss daran lediglich Datenverarbeitungen, die im Zusammenhang mit diesen Aktivitäten stehen, vom Anwendungsbereich der Datenschutzgrundverordnung erfasst.

Die mit der neuen Bestimmung einhergehende beträchtliche Ausweitung des Anwendungsbereichs des europäischen Datenschutzrechts – die letztlich impliziert, dass zahlreiche Wirtschaftsteilnehmer und öffentliche Stellen in Drittstaaten die Vorgaben der Verordnung bei zahlreichen ihrer Datenverarbeitungen einhalten müssen – wirft jedoch auch einige Fragen auf, die im Wesentlichen auf zwei Ebenen anzusiedeln sind:

- Erstens ist zu erwarten, dass die Anwendung der Kriterien des Art. 3 Abs. 2 DGVO nicht immer einfach sein wird und sich hier durchaus Abgrenzungsprobleme ergeben werden.

  So fragt es sich, unter welchen Voraussetzungen davon ausgegangen werden kann, dass Waren oder Dienstleistungen in der Union angeboten werden: Sollte hierfür allein ein Angebot auf dem Internet ausreichend sein (das *per se* überall auf der Welt zugänglich ist), entfaltete die Datenschutzgrundverordnung eine allgemeine universelle Wirkung, was wohl kaum mit den erwähnten völkerrechtlichen Vorgaben in Einklang stünde, wäre dann der Anknüpfungspunkt zum Unionsgebiet, zu sich in diesem abspielenden Sachverhalten oder sich dort aufhaltenden Personen zu allgemein und vage.[26] Fordern wird man daher objektiv erkennbare und zielgerichtete Aktivitäten in diesem

---

24 Teilweise wird hier auch vom „Marktortprinzip“ gesprochen, vgl. *Benedikt Buchner*, Grundsätze und Rechtmässigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, 156.

25 Vgl. hierzu aus der völkerrechtlichen Literatur, m.w.N. insbesondere zur Rechtsprechung, z.B. *Walter Kälin/Astrid Epiney/Martina Caroni/Jörg Künzli*, Völkerrecht. Eine Einführung, 3. Aufl., 2010; *Andreas von Arnauld*, Völkerrecht, 2. Aufl., 2014, Rn. 342 ff.

26 S. insoweit auch EuGH, verb. Rs. C-585/08, C-144/09, ECLI:EU:C:2010:740, Rn. 75 (Pammer).

Sinn, etwa durch die Verwendung der entsprechenden Sprache oder von Werbung auf dem Gebiet der Union,[27] ohne dass es jedoch auf eine eigentliche „subjektive" Absicht ankäme.[28] Entscheidend wird hier eine Gesamtwürdigung der Umstände des Einzelfalls sein, womit aber auch gewisse Unklarheiten einhergehen können. Ebenso dürfte die Frage, ob eine Beobachtung betroffener Personen im Hoheitsgebiet der Union vorliegt, anhand aller Umstände des Einzelfalls zu beurteilen sein, wobei hier in aller Regel jedoch eine subjektive Absicht vorliegen wird, wenn auch nicht zwingend in Bezug auf eine ganz bestimmte Person.

Weiter könnte auch die Ermittlung, ob eine Datenverarbeitung „im Zusammenhang" mit den genannten Aktivitäten steht, schwierig sein: Wenn dabei auch klar ist, dass die Verarbeitung der Daten der betroffenen Personen erfasst sind, geht doch aus der Bestimmung nicht hervor, inwieweit hiermit im Zusammenhang stehende Verarbeitungen ebenfalls betroffen sind bzw. ab welchem Zeitpunkt die Daten wirklich bestimmte Personen oder identifizierbare Personen betreffen, eine Fragestellung, die etwa bei Videoüberwachungen eine Rolle spielen kann.[29]

- Zweitens wird die Rechtsdurchsetzung häufig problematisch sein, erlaubt es das Völkerrecht doch grundsätzlich nicht, entsprechende Massnahmen im Hoheitsgebiet anderer Staaten zu ergreifen, so dass man hier auf Massnahmen im eigenen Hoheitsgebiet beschränkt ist, die jedoch in aller Regel wenig effektiv sein werden, fehlt es doch an einer Niederlassung. Soweit öffentliche Stellen betroffen sind, kommen die völkerrechtlichen Immunitätsregeln zur Anwendung, die einer eigentlichen Rechtsdurchsetzung in aller Regel entgegenstehen werden.

– Schliesslich findet die Verordnung auch Anwendung – insoweit wiederum in Anknüpfung an die Rechtslage unter der RL 95/46 (vgl. deren Art. 4 Abs. 1 lit. b) – auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der auf der Grundlage der völkerrechtlichen Regeln dem Recht eines Mitgliedstaats unterliegt.

Nur am Rande sei in diesem Zusammenhang noch auf eine Problematik hingewiesen, die sich bereits auf der Grundlage der RL 95/46 stellt: Nach Art. 2 Abs. 2 DGVO findet die Datenschutzgrundverordnung u.a. keine Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen einer Tätigkeit erfolgt, die nicht in den Anwendungsbereich des Unionsrechts fällt (s. insoweit auch bereits Art. 3 Abs. 2 RL 95/46). Diese Formulierung wirft die Frage auf, unter welchen Voraussetzungen der „Anwendungsbereich des Unionsrechts" (nicht) betroffen ist. Jedenfalls kommt es hier nicht auf den grenzüberschreitenden Bezug an.[30] Aber auch darüber hinaus ist fraglich, ob überhaupt Konstellationen denkbar sind, in denen der Anwendungsbereich des Unionsrechts von vornherein nicht eröffnet ist, geht es doch bei der Verordnung auch um den freien

---

27 S. zu einzelnen, hier relevanten Elementen *Passadelis/Roth*, Jusletter v. 4.4.2016 (Fn. 20), Rn. 14.

28 S. insoweit auch Erw. 23 DGVO, wobei hier teilweise etwas missverständlich formuliert wird, so wenn auf ein „offensichtliches Beabsichtigen" Bezug genommen wird.

29 Zur Problematik im Zusammenhang mit „Big Data" *Astrid Epiney*, Big Data und Datenschutzrecht: Gibt es einen gesetzgeberischen Handlungsbedarf?, Jusletter IT v. 21.5.2015, Rn. 11 ff.

30 S. schon EuGH, Rs. C-101/01, ECLI:EU:2003:596 (Lindqvist); s. sodann EuGH, Rs. C-524/06, ECLI:EU:C:2008:724 (Huber); EuGH, verb. Rs. C-465/00, C-138/01, C-139/01, ECLI:EU:C:2003:294 (Österreichischer Rundfunk). Hierzu auch bereits oben B.I.

Verkehr personenbezogener Daten, so dass grundsätzlich einmal jede Datenverarbeitung (potentiell) betroffen ist.

2. Rechte der Betroffenen

Die Rechte der von einer Datenverarbeitung (potentiell) betroffenen Personen – worunter im Folgenden nicht nur die Rechte i.e.S. (also eigentliche Ansprüche der Betroffenen insbesondere gegenüber den Datenverarbeitenden), sondern auch solche Vorgaben verstanden werden, die auf andere Weise unmittelbar den Schutz der Persönlichkeitsrechte bestimmter Personen zum Gegenstand haben – werden in der Datenschutzgrundverordnung in verschiedener Hinsicht verstärkt bzw. ausgebaut. Von Bedeutung sind hier in erster Linie die neuen Anforderungen an Einwilligungserklärungen (a), die weitergehenden Transparenz- und Informationspflichten (b) sowie die neuen Ansprüche der Betroffenen (c).

a) Zur Einwilligung

Die Grundsätze der Datenverarbeitung (Art. 5 ff. DGVO) werden weitgehend in Anlehnung an die RL 95/46 formuliert, wenn auch einige stilistische Anpassungen und Präzisierungen zu verzeichnen sind, die jedoch in aller Regel keine ins Gewicht fallenden inhaltlichen Modifikationen mit sich bringen, auch wenn mitunter neue (aber nicht durchgehend überzeugende) Begriffe eingeführt werden.

So nimmt z.B. Art. 5 Abs. 1 lit. c DGVO auf den Begriff der „Datenminimierung" Bezug, der jedoch insofern wenig glücklich erscheint, als es letztlich um die Verhältnismässigkeit geht, die noch weitere Aspekte als diejenige der Datenminimierung (wie z.B. die Beschränkung der Zugangsberechtigten) erfasst.

Weiter ist auf Art. 6 Abs. 3 DGVO hinzuweisen, der spezifische Vorgaben für Art. 6 Abs. 2 lit. c und e DGVO formuliert, wobei die Bestimmung davon auszugehen scheint, dass in diesen Konstellationen eine gesetzliche Grundlage gefordert wird, ohne dass dies jedoch ausdrücklich klargestellt wird, was sich jedenfalls für Datenverarbeitungen durch öffentliche Organe aufgedrängt hätte.

Diverse Fragen wirft sodann Art. 6 Abs. 4 DGVO auf. Diese Bestimmung geht von der allgemeinen Zulässigkeit einer Verarbeitung von Personendaten auch zu anderen Zwecken als für diejenigen, für die sie erhoben wurden, aus, was letztlich wohl eine recht weitgehende Relativierung des Zweckbindungsgrundsatzes implizieren dürfte.[31]

Gewisse Modifikationen sind jedoch in Bezug auf die Anforderungen an die Einwilligung in eine Datenbearbeitung – wobei die Einwilligung eine der zentralen Rechtfertigungsgründe für eine Datenbearbeitung bleibt, dies trotz der mit dieser verbundenen Problematik, die dazu führt, dass es sich hier oft um eine Fiktion handelt[32] – zu verzeichnen:

---

31 Zum Problemkreis etwa *Maximilian von Grafenstein*, Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit, DuD 2015, 789 ff.

32 Zur grundsätzlichen Problematik der Einwilligung im Einzelnen sehr instruktiv *Spiros Simitis*, Entwicklung und Dilemmata des Datenschutzes, in: Astrid Epiney/Julia Hänni/Flavia Brülisauer (Hrsg.), Die Unabhängigkeit der Aufsichtsbehörden und weitere aktuelle Fragen des Datenschutzrechts, 2012, 1 (5 ff.); s. auch *Eleni Kosta*, Construing the Meaning of „Opt-Out" – An Analysis of the European, U.K. and German Data Protection Legislation, EDPL 2015, 16 ff.

- Zunächst wird die Begriffsdefinition in Art. 4 Nr. 11 DGVO im Vergleich zu Art. 2 lit. h RL 95/46 nicht nur etwas umformuliert und dadurch klarer gestaltet, sondern durch die Anforderung ergänzt, dass es sich um eine „eindeutige" Erklärung oder Handlung handeln muss. Damit werden aber auch in Zukunft konkludente Einwilligungen nicht ausgeschlossen, wenn auch die diesbezüglichen Anforderungen erhöht werden. Fraglich ist in diesem Zusammenhang, ob damit allgemein insbesondere im Rahmen von *online*-Geschäften das System des „*Opt-in*" verwirklicht werden soll.[33] Der Wortlaut des Art. 4 Nr. 11 DGVO („sonstige eindeutig bestätigende Handlung") ist unklar; jedoch dürfte vieles dafür sprechen, dass eine solche eindeutig bestätigende Handlung im Falle etwa der Nutzung von Internetseiten und der im Anschluss daran erfolgenden Datenverarbeitung durch den Betreiber nicht schon in der Nutzung liegen kann, so dass eine ausdrückliche Einwilligung durch das Anklicken des betreffenden Feldes notwendig ist. Für diesen Ansatz kann auch der Zusammenhang mit der ebenfalls in Art. 4 Nr. 11 DGVO erwähnten „Erklärung" angeführt werden, dürfte der Unionsgesetzgeber doch davon ausgegangen sein, dass die „sonstige bestätigende Handlung" eben mit einer Erklärung vergleichbar sein muss.
- Nach Art. 7 Abs. 1 DGVO trägt der für die Verarbeitung Verantwortliche die Beweislast für das Vorliegen einer Einwilligung.
- Art. 7 Abs. 2 DGVO enthält eher detaillierte Vorgaben in Bezug auf Form und Inhalt einer Einwilligung durch eine schriftliche Erklärung, wobei insbesondere eine klare und einfache Sprache gefordert wird.
- Die betroffene Person kann ihre Einwilligung jederzeit widerrufen, wobei der Widerruf so einfach wie die Einwilligung selbst sein muss: Art. 7 Abs. 3 DGVO.
- Sodann ist nach Art. 7 Abs. 4 DGVO bei der Beurteilung der Freiwilligkeit der Einwilligung zu berücksichtigen, ob die Erfüllung eines Vertrages von der Einwilligung in die Verarbeitung personenbezogener Daten abhängig gemacht wird, die für die Erfüllung des Vertrages gerade nicht erforderlich ist. Die Bestimmung impliziert im Gegenschluss, dass auch bei solchen Verbindungen die Freiwilligkeit durchaus gegeben sein kann.
- Art. 8 DGVO enthält spezifische Anforderungen an die Einwilligung von Kindern.[34]

Zwar führen diese Bestimmungen insgesamt einerseits zu einer Präzisierung gewisser, an die Einwilligung zu stellender Anforderungen sowie zu einer Stärkung der Rechte und der Stellung der Betroffenen. Andererseits folgt auch die Datenschutzgrundverordnung insofern dem „traditionellen" Ansatz bei der Einwilligung, als diese nach wie vor einen allgemeinen Rechtfertigungsgrund darstellt, dessen Anwendungsbereich nicht wirklich eingeschränkt wird. Hieran ändert auch Art. 7 Abs. 4 DGVO nichts, geht es doch nur um eine Berücksichtigungspflicht. Verzichtet wurde insbesondere darauf, die Einwilligung als Rechtfertigungsgrund in gewissen Fallgestaltungen – z.B. bei einem erheblichen „Machtgefälle" zwischen Da-

[33] So offenbar *Weber*, Jusletter IT v. 24.9.2015 (Fn. 5), Rn. 30, dies allerdings auf der Grundlage des leicht anders formulierten Entwurfs der Verordnung.

[34] Spezifisch zu diesem Problemkreis *Peter Gola/Sebastian Schulz*, DS-GVO – Neue Vorgaben für den Datenschutz bei Kindern? Überlegungen zur einwilligungsbasierten Verarbeitung von personenbezogenen Daten Minderjähriger, ZD 2013, 475 ff.

tenverarbeiter und Betroffenen – auszuschliessen. Hinzuweisen ist allerdings darauf, dass es Art. 88 DGVO den Mitgliedstaaten erlaubt, „spezifischere Vorschriften" zur Gewährleistung des Persönlichkeitsschutzes im Beschäftigungskontext zu erlassen, was wohl auch die Formulierung erhöhter Anforderungen an die Einwilligung oder gar den Ausschluss der Einwilligung als Rechtfertigungsmöglichkeit einschliesst.[35]

b) Informations- und Transparenzpflichten

Die Informations- und Transparenzpflichten werden in der Datenschutzgrundverordnung wesentlich ausgebaut, was angesichts der in diesem Zusammenhang häufig herrschenden Intransparenz sehr zu begrüssen ist: So werden die zu übermittelnden Informationen in Art. 13 Abs. 1 und 2 sowie 14 Abs. 1 und 2 DGVO in sehr detaillierter Weise umschrieben, wobei – insofern wie bereits in Art. 10 und 11 RL 95/46 – zwischen der Informationspflicht bei der Erhebung von personenbezogenen Daten bei den Betroffenen und bei der Erhebung in anderer Weise unterschieden wird. Sollen die Daten zu einem anderen Zweck verarbeitet werden als den, für den sie erhoben wurden, hat eine erneute Information zu erfolgen (Art. 13 Abs. 3 und 14 Abs. 4 DGVO), eine Bestimmung, welche die Relativierung des Zweckbindungsgrundsatzes bestätigt.

c) Ansprüche der Betroffenen

Die Datenschutzgrundverordnung verankert zwei neue Rechte der betroffenen Personen:

– Art. 17 DGVO kodifiziert das sog. „Recht auf Vergessenwerden", das offenbar synonym mit dem „Recht auf Löschung" verstanden wird. In der Sache umfasst dieser Anspruch das Recht der betroffenen Person, von dem Verantwortlichen zu verlangen, dass sie betreffende Daten unverzüglich gelöscht werden, dies falls die Rechtmässigkeit der Datenverarbeitung nicht mehr gegeben ist, wobei die entsprechenden Konstellationen in Art. 17 Abs. 1 DGVO im Einzelnen aufgeführt werden. Art. 17 Abs. 3 DGVO enthält einige Ausnahmetatbestände (u.a. die Erforderlichkeit der entsprechenden Daten im Hinblick auf das Recht auf freie Meinungsäusserung und Information), bei deren Anwendung wohl jeweils eine Interessenabwägung vorzunehmen ist. Gerade die Reichweite der Einschränkungen dürfte im Einzelnen durchaus Fragen aufwerfen und wird wohl erst im Zuge der Entwicklung der Rechtsprechung verlässlich konkretisiert werden können.
  Im Ergebnis sollte die Tragweite dieses „neuen" Rechts nicht überschätzt werden: Art. 12 lit. b RL 95/46 sieht bereits ein Recht der Betroffenen vor, vom Datenverantwortlichen eine Löschung der sie betreffenden Daten zu verlangen, woraus der EuGH umfassende Rechte abgeleitet hat (ohne jedoch den Begriff „Recht auf Vergessenwerden" zu verwenden).[36]

---

35 Hierzu, wenn auch nicht ganz klar, *Tim Wybitul/Stephan Pötters*, Der neue Datenschutz am Arbeitsplatz, RDV 2016, 10 (13).

36 Zur Problematik eines „Rechts auf Vergessen" instruktiv auch *Gabriele Buchholtz*, Das „Recht auf Vergessen" im Internet. Vorschläge für ein neues Schutzkonzept, ZD 2015, 570

Erinnert sei hier an das Urteil in der Rs. C-131/12,[37] in dem der Gerichtshof u.a.[38] zur rechtlichen Tragweite der Art. 12 lit. b und Art. 14 Abs. 1 lit. a RL 95/46 Stellung nahm: Diese Bestimmungen seien so auszulegen, dass ein von der Datenbearbeitung durch die Suchmaschine Betroffener (dessen Personendaten also im Rahmen der Suche angezeigt werden) verlangen kann, dass der Suchmaschinenbetreiber prüft, ob die betroffene Person ein Recht darauf hat, dass ihr Name nicht mehr durch die Ergebnisliste erfasst wird, zumindest nicht in Bezug auf bestimmte personenbezogene Informationen. Irrelevant sei dabei, ob dem Betroffenen durch die Anzeige ein Schaden entsteht. Art. 7 und 8 GRCh räumten den Betroffenen ein Recht ein, dass bestimmte, sie betreffende Informationen nicht mehr auf der Ergebnisliste angezeigt werden, so dass diese Rechte grundsätzlich sowohl gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers als auch dem Interesse der breiten Öffentlichkeit am Zugang zu solchen Informationen überwögen, letzteres unter dem Vorbehalt, dass nicht besondere Gründe (z.B. die Rolle der Person im öffentlichen Leben) ein anderes Abwägungsergebnis nahelegen. Auf dieser Grundlage und in Anbetracht des Umstandes, dass Suchmaschinen einen besonders leichten Zugang zu den relevanten Informationen ermöglichen, sei der Suchmaschinenbetreiber verpflichtet, bei Vorliegen der skizzierten Voraussetzungen die Ergebnisliste entsprechend zu verändern, dies auch soweit die Information noch auf den entsprechenden Internetseiten zu finden ist und diese Veröffentlichung rechtmässig ist.

Hervorzuheben ist allerdings, dass Art. 17 DGVO im Vergleich zur RL 95/46 eine wesentlich detailliertere Regelung enthält. Wenig glücklich erscheint jedoch der Begriff des „Rechts auf Vergessenwerden", da er suggeriert, die Betroffenen hätten nicht nur ein Recht auf Löschung, sondern ein darüber hinausgehendes Recht, dass bestimmte sie betreffende Daten in Vergessenheit geraten. Ein solcher Anspruch kann aber weder gegenüber einzelnen Personen und offenkundig auch nicht auf dem *World Wide Web* gewährt werden, so dass es nach der hier vertretenen Ansicht weiser gewesen wäre, bereits den insofern irreführenden Begriff zu vermeiden.

– Nach Art. 20 DGVO hat die betroffene Person das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem „strukturierten, gängigen und maschinenlesbaren Format" zu erhalten und ohne Behinderung durch den „ersten" Verantwortlichen einem anderen Verantwortlichen zu übermitteln, soweit die Verarbeitung auf bestimmten Rechtfertigungsgründen (insbesondere einer Einwilligung oder einem Vertrag) beruht und die Verarbeitung mittels automatisierter Verfahren erfolgt. Dieses neue Recht stärkt ganz erheblich die Kontrolle der Betroffenen über die eigenen Daten, woran auch gewisse Einschränkungen (Anwendbarkeit nur in bestimmten Konstellationen, notwendige Aussonderung der Daten Dritter) nichts ändert.

3. Pflichten der Datenverarbeiter

Bedeutende Neuerungen enthält die Verordnung in Bezug auf die Verpflichtungen der Verantwortlichen und Auftragsverarbeiter, die in Kap. IV der Verordnung (Art. 24 ff.) figurieren und in verschiedener Hinsicht ausgebaut und um neue Instrumente bzw. Pflichten erweitert wurden. Von Bedeutung erscheinen hier in erster Linie

ff.; s. auch *Anika D. Luch/Sönke E. Schulz/Florian Kuhlmann*, Ein Recht auf Vergessenwerden als Ausprägung einer selbstbestimmten digitalen Persönlichkeit, EuR 2014, 698 ff.

37 EuGH, Rs. C-131/12, ECLI:EU:C:2014:317 (Google Spain und Google Inc.).

38 Zu den Aussagen des Gerichtshofs zum Anwendungsbereich der RL 95/46 bereits oben B.III.1.

folgende Aspekte: *Privacy by design* und *Privacy by default* (a), Aufzeichnungspflichten (b), sicherheitsbezogene Massnahmen (c), Datenschutz-Folgeabschätzung (d) und die Pflicht, unter gewissen Voraussetzungen, einen Datenschutzbeauftragten zu bestellen (e).

Daneben enthält die Verordnung noch neue detaillierte Vorgaben für die Konstellation, dass es gemeinsame Verantwortliche für eine Datenverarbeitung gibt, für die Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern (die grundsätzlich zwingend zu bestellen sind) und die Auftragsverarbeitung (Art. 26-29); insbesondere der zuletzt genannte Aspekt dürfte von grosser Bedeutung sein.[39]

Eigene Vorschriften werden auch im Hinblick auf die Förderung von Verhaltensregeln und die Zertifizierung formuliert (Art. 40-43 DGVO), wobei es hier jedoch im Wesentlichen um Förderpflichten unterschiedlicher Reichweite geht.[40]

Schliesslich ist allgemein darauf hinzuweisen, dass die Datenschutzgrundverordnung in der Regel davon ausgeht, dass die Beweispflicht für die Einhaltung der datenschutzrechtlichen Vorgaben beim Verantwortlichen liegt (vgl. insbesondere Art. 5 Abs. 2 und 24 DGVO), was häufig mit dem Begriff der sog. *Accountability* umschrieben wird.

a) Privacy by design und Privacy by default

Art. 25 DGVO verankert die Grundsätze des Datenschutzes durch Technikgestaltung (*privacy by design*) und der datenschutzrechtlichen Voreinstellungen (*privacy by default*):

– Danach haben die Verantwortlichen einerseits frühzeitig geeignete technische und organisatorische Massnahmen zu treffen, um die Datenschutzgrundsätze wirksam umzusetzen und die notwendigen Garantien für den Schutz der Betroffenen gewährleisten zu können. M.a.W. ist bereits bei der technischen Gestaltung und Entwicklung der für die Datenverarbeitung verwendeten Technologien auf eine wirksame Umsetzung der datenschutzrechtlichen Vorgaben zu achten. Dieser Ansatz geht insofern über die „traditionellen" datenschutzrechtlichen Instrumente und Vorgaben hinaus, als er Verpflichtungen bereits zu einem Zeitpunkt formuliert, zu dem es noch gar keine Verarbeitung personenbezogener Daten stattfindet.[41] Damit wird auch die Frage aufgeworfen, wie weit diese Verpflichtung geht: So dürfte sie zwar jedenfalls dann zum Zuge kommen, wenn zum Zeitpunkt der Entwicklung der jeweiligen Technik die Verarbeitung personenbezogener Daten vorgesehen und beabsichtigt ist. Nicht klar hingegen ist, ob sie auch dann zum Tragen kommt, wenn es noch unklar ist, ob die jeweilige Technik auch die Verarbeitung personenbezogener Daten betrifft. U.E. spricht vieles dafür, dass Art. 25 Abs. 1 DGVO immer schon dann zur Anwendung gelangt, wenn aufgrund der Umstände des Einzelfalls damit gerechnet werden muss, dass personenbezogene Daten verarbeitet werden bzw. der Verarbeiter dies nicht ausschliesst.

---

39 Vgl. zu diesen Regelungen *Passadelis/Roth,* Jusletter v. 4.4.2016 (Fn. 20), Rn. 46 ff.; *Thomas Petri,* Auftragsdatenverarbeitung – heute und morgen. Reformüberlegungen zur Neuordnung des Europäischen Datenschutzrechts, ZD 2015, 305 ff.

40 Spezifisch zur Zertifizierung *Sebastian Kraska,* Datenschutz-Zertifizierung in der EU-Datenschutzgrundverordnung, ZD 2016, 153 f.

41 *Passadelis/Roth,* Jusletter v. 4.4.2016 (Fn. 20), Rn. 45.

– Andererseits sind Voreinstellungen so vorzunehmen, dass Personendaten nur soweit verarbeitet werden, wie dies für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist; insbesondere ist sicherzustellen, dass personenbezogene Daten durch Voreinstellungen nicht (ohne Eingreifen der Betroffenen) einer unbestimmten Zahl von Personen zugänglich gemacht werden.

b) Aufzeichnungspflichten

Art. 30 DGVO verpflichtet die für eine Verarbeitung Verantwortlichen (bzw. seine Vertreter), ein Verzeichnis aller in ihrer Zuständigkeit liegenden Verarbeitungstätigkeiten zu führen. Überdies präzisiert die Bestimmung mit einem bemerkenswerten Detaillierungsgrad die in dieses Verzeichnis – das der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen ist (während eine Anmeldepflicht für bestimmte Datenverarbeitungen nicht vorgesehen ist) – aufzunehmenden Angaben.

c) Sicherheitsbezogene Massnahmen

Art. 32 DGVO formuliert diverse Vorgaben in Bezug auf die Sicherheit personenbezogener Daten, wobei bemerkenswert ist, dass gewisse, zumindest in allgemeiner Form umschriebene Massnahmen in jedem Fall vorgeschrieben werden (Art. 32 Abs. 1 DGVO), während ansonsten in Bezug auf das anzulegende Schutzniveau auf Verhältnismässigkeitsgesichtspunkte verwiesen wird (Art. 32 Abs. 2 DGVO).

Von grosser Bedeutung dürften die neu verankerten Melde- und Benachrichtigungspflichten sein:

– Nach Art. 33 DGVO hat der Verantwortliche im Fall einer Verletzung der datenschutzrechtlichen Vorgaben der zuständigen Aufsichtsbehörde diese unverzüglich und möglichst binnen 72 Stunden zu melden (Art. 33 Abs. 1 DGVO), wobei Art. 33 Abs. 3 DGVO die der Meldung beizufügenden Informationen aufzählt. Allerdings steht die Meldepflicht unter dem Vorbehalt, dass aufgrund der Verletzung der datenschutzrechtlichen Vorschriften voraussichtlich ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht. M.a.W. darf eine Meldung dann unterbleiben, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Diese Einschränkung besticht nicht durch ihre Klarheit: Denn grundsätzlich stellt jede Nichtbeachtung der datenschutzrechtlichen Vorgaben – jedenfalls soweit die materiell-rechtlichen Pflichten betroffen sind – eine Verletzung der Persönlichkeitsrechte der Betroffenen dar, so dass es letztlich nur darum gehen kann, ob diese Verletzung der Persönlichkeitsrechte darüber hinaus ein Risiko für andere Rechte und Freiheiten der Betroffenen darstellt, die ungerechtfertigt eingeschränkt werden könnten. In jedem Fall weist diese Bestimmung eine eher geringe normative Dichte auf, und dem Verantwortlichen – der diese Frage letztlich jedenfalls zunächst zu beurteilen hat – dürfte hier ein gewisser Spielraum zukommen. Dies führt aber auch zu einer beachtlichen Rechtsunsicherheit, wird es doch für den Verantwortlichen nicht immer klar sein, ob jetzt eine Meldepflicht besteht oder nicht. Jedenfalls aber entfällt eine Meldepflicht nur dann, wenn ein Risiko voraussichtlich nicht besteht, nicht schon dann, wenn unklar ist, ob ein Risiko besteht. Dies führt dazu, dass im

Zweifel dann doch eine Meldung erfolgen sollte, schon weil innerhalb der kurzen Frist von 72 Stunden entsprechende Abklärungen häufig nicht getroffen werden können.

– Art. 34 DGVO ergänzt die erwähnte Meldepflicht durch eine Pflicht zur Benachrichtigung der betroffenen Person, dies soweit die Verletzung der datenschutzrechtlichen Vorgaben ein „hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen" zur Folge hat. Hier reicht also nicht ein Risiko, sondern dieses muss zudem „hoch" sein und erst noch die „persönlichen" (und nicht „irgendwelche") Rechte und Freiheiten betreffen. Erkennbar ist somit eine Abstufung, wobei auch hier ins Gewicht fallende normative Unschärfen zu verzeichnen sind. Zudem sieht Art. 34 Abs. 3 DGVO noch ein Entfallen der Benachrichtigungspflicht in gewissen Konstellationen vor, wobei insbesondere Art. 34 Abs. 3 lit. a DGVO Fragen aufwirft, lässt diese Bestimmung die Benachrichtigungspflicht bereits dann entfallen, wenn der Verantwortliche geeignete Sicherheitsvorkehrungen getroffen hat, ändern diese doch nichts daran, dass es u.U. trotzdem zu einem hohen Risiko für die persönlichen Rechte der Betroffenen gekommen ist.

d) Datenschutz-Folgeabschätzung (Data Protection Impact Assessment)

Art. 35 DGVO überträgt die Idee der Umweltverträglichkeitsprüfung auf den Datenschutz: So hat der Verantwortliche immer dann, wenn eine Verarbeitung aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, vorgängig eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchzuführen. Art. 35 Abs. 3 DGVO nennt diejenigen Konstellationen, in denen in jedem Fall eine solche Prüfung durchzuführen ist (z.B. systematische umfangreiche Überwachung öffentlicher Bereiche), und Art. 35 Abs. 7 DGVO sind nähere Angaben zum Mindestinhalt einer solchen Datenschutz-Folgeabschätzung zu entnehmen.

Ergibt die Datenschutz-Folgeabschätzung, dass die Verarbeitung ein hohes Risiko (wobei auch hier auf die Unschärfe dieses Begriffs hinzuweisen ist) für die Betroffenen impliziert, sind Konsultationen mit der Aufsichtsbehörde durchzuführen, es sei denn, der Verantwortliche trifft Massnahmen zur Eindämmung des Risikos (Art. 36 Abs. 1 DGVO). Das Konsultationsverfahren ist in Art. 36 DGVO im Einzelnen geregelt und kann in Empfehlungen der Aufsichtsbehörde münden, die zudem ihre Befugnisse nach Art. 58 DGVO ausüben kann.

e) Datenschutzbeauftragter

Gemäss Art. 37 DGVO sind gewisse Datenverarbeiter verpflichtet, einen Datenschutzbeauftragten zu benennen (wobei Konzerne oder Behörden auch gemeinsame Beauftragte vorsehen dürfen). Allerdings besteht diese Pflicht allgemein nur für Behörden oder sonstige öffentliche Stellen (mit Ausnahme der Judikative); hingegen muss sich bei Privaten die „Kerntätigkeit" des Verantwortlichen gerade auf eine Datenverarbeitung beziehen, die zudem entweder ein gewisses Ausmass bzw. einen gewissen Umfang aufgrund einer umfangreichen, regelmässigen und systematischen Überwachung aufweisen oder besonders schützenswerte Personendaten betreffen muss.

Die Bezugnahme auf die „Kerntätigkeit“ legt es nahe, dass der eigentliche Unternehmenszweck in der Datenverarbeitung bestehen muss, m.a.W., dass diese als solche gerade Teil der unternehmerischen Tätigkeit darstellt. Hingegen ziehen die in allen Unternehmen durchgeführten Datenverarbeitungen im Personal- oder Finanzwesen oder die regelmässig anzutreffende Verarbeitung personenbezogener Daten zu Werbezwecken keine Pflicht zur Bestellung eines Datenschutzbeauftragen nach sich, dies auch, falls es sich um umfangreiche, risikobehaftete oder sonstwie für die Persönlichkeitsrechte ins Gewicht fallende Verarbeitungen handelt oder handeln kann. Immerhin steht es den Mitgliedstaaten nach wie vor frei, über die Mindestvorgaben der Datenschutzgrundverordnung hinaus eine Pflicht zur Bestellung eines Datenschutzbeauftragten vorzusehen (Art. 37 Abs. 4 DGVO).

4. Durchsetzung und Sanktionen

Die Regelungen der Datenschutzgrundverordnung betreffend Durchsetzung und Sanktionen knüpfen zwar an das bereits durch die RL 95/46 vorgesehene System an, dies insbesondere soweit die zentrale Rolle der unabhängigen Aufsichtsbehörden betroffen ist. Jedoch werden die entsprechenden Vorgaben weit präziser gefasst und die Aufgaben und Kompetenzen der Aufsichtsbehörden mitunter erheblich ausgeweitet.

Insbesondere werden die Untersuchungs- und Abhilfebefugnisse (letztere umfassen etwa das Recht, Verantwortlichen Anweisungen zu erteilen, aber auch das Recht, eine Verarbeitung zu verbieten) detailliert aufgeführt, präzisiert und im Ergebnis beträchtlich ausgeweitet (Art. 58 DGVO). Weiter werden die Sanktionsbefugnisse ebenfalls detailliert ausgeführt, vereinheitlicht und erheblich ausgebaut; sie umfassen insbesondere die Befugnis zur Verhängung von (hohen) Geldbussen (Art. 83 DGVO).[42]

Darüber hinaus werden auch die zivilrechtlichen Ansprüche der Betroffenen im Falle von (möglichen) Verletzungen der datenschutzrechtlichen Vorgaben gestärkt. So haben sie nicht nur einen Anspruch auf Beschwerde vor der Aufsichtsbehörde und mitgliedstaatlichen Gerichten (Art. 77 und 79 DGVO), sondern können sich auch von Organisationen oder Vereinigungen vertreten lassen, deren statutarische Ziele sich auf den Schutz der Rechte und Freiheiten von Personen im Zusammenhang mit ihren personenbezogenen Daten beziehen (Art. 80 DGVO). Weiter werden die Vorgaben betreffend die Haftung und das Recht auf Schadensersatz präzisiert, und es wird – im Falle eines Verstosses gegen die Verordnung – eine Gefährdungshaftung vorgesehen (Art. 82 DGVO).[43]

Schliesslich ist in diesem Zusammenhang auf Kap. VII („Zusammenarbeit und Kohärenz“) hinzuweisen, in dem einerseits die Zusammenarbeit zwischen den na-

---

42 Spezifisch zu diesem Aspekt *Sebastian Faust/Jan Spittka/Tim Wybitul*, Milliardenbussgelder nach der DS-GVO. Ein Überblick über die neuen Sanktionen bei Verstössen gegen den Datenschutz, ZD 2016, 120 ff.; s. auch *Daniel Ashkar*, Durchsetzung und Sanktionierung des Datenschutzrechts nach den Entwürfen der Datenschutz-Grundverordnung, DuD 2015, 796 ff.

43 Vgl. im Einzelnen zur Neuregelung der Schadensersatzansprüche im Vergleich zur aktuellen Rechtslage *Peter Gola/Carlo Piltz*, Die Datenschutz-Haftung nach geltendem und zukünftigem Recht – ein vergleichender Ausblick auf Art. 77 DS-GVO, RDV 2015, 279 ff.

tionalen Aufsichtsbehörden (insbesondere im Fall mehrerer betroffener Aufsichtsbehörden) geregelt wird, dies im Hinblick auf die Sicherstellung einer gewissen Kohärenz der Anwendung und Auslegung der datenschutzrechtlichen Vorgaben (Art. 60 ff. DGVO).[44] Andererseits wird neu der „Europäische Datenschutzausschuss" geschaffen (Art. 68 DGVO), der die sog. „Gruppe 29" ersetzen wird. Der Ausschuss – zusammengesetzt aus den Leitern der Aufsichtsbehörden der Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten – wird als Einrichtung mit eigener Rechtspersönlichkeit vorgesehen. Ihm kommen zahlreiche, in Art. 70 DGVO detailliert aufgeführte[45], Befugnisse zu, unter Einschluss der Überwachung und Sicherstellung der ordnungsgemässen Anwendung der Verordnung sowie der Erarbeitung von Leitlinien und Empfehlungen.

C. Die Richtlinie zum Datenschutz in der Strafverfolgung

I. Allgemeines

Die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (im Folgenden: Richtlinie zum Datenschutz in der Strafverfolgung; Richtlinie) hat – gewissermassen als kleines Geschwister der Datenschutzgrundverordnung – deren hürdenreichen Gesetzgebungsprozess mitgemacht: Obgleich im EU-Parlament 673 Änderungsanträge bezüglich der Richtlinie eingereicht worden waren, war ihre Erarbeitung in der Summe wesentlich weniger umstritten als jene der Datenschutzgrundverordnung, hing doch eine grosse Anzahl der Änderungsanträge mit jenen in Bezug auf die Verordnung zusammen. Der Grund hierfür ist wohl ein dreifacher: Erstens hatte ein beträchtlicher Teil des Zündstoffes, der noch in einem ersten, im November 2011 bekanntgewordenen Entwurf des Rechtsaktes enthalten war, keinen Eingang in den Kommissionentwurf vom 25. Januar 2016 erhalten; zweitens war der Rahmenbeschluss 2008/977 als Vorläufererlass wesentlich jüngeren Datums als die RL 95/46 und somit der Aktualisierungsbedarf geringer und schliesslich dürfte auch eine Rolle gespielt haben, dass die Grundverordnung die hauptsächliche Aufmerksamkeit von Politik und Kommentatoren auf sich zog und sich die Richtlinie somit wohl gewissermassen in ihrem Fahrwasser entwickeln konnte. Wie die Verordnung 2016/679 stützt sich die Richtlinie auf Art. 16 Abs. 2 AEUV.[46] Die obgenannten Fragen in Bezug auf die Datenbearbeitung durch Private stellen sich vorliegend jedoch in weit geringerem

[44] Spezifisch zu diesem Aspekt *Alexander M. Nguyen*, Die zukünftige Datenschutzaufsicht in Europa. Anregungen für den Trilog zu Kap. VI bis VII der DS-GVO, ZD 2015, 265 ff.

[45] So umfasst die diesbezügliche Aufzählung in Art. 70 Abs. 1 DGVO die Buchstaben a-y.

[46] Vgl. hierzu auch oben S. B.I.

Masse, da der Regelungsgegenstand schwergewichtig die Datenbearbeitung durch behördliche Akteure umfasst.[47]
Während der Vorgängererlass – wie bereits erwähnt – als Rahmenbeschluss ausgestaltet war, wurde – insbesondere auch, da das Instrument des Rahmenbeschlusses mit dem Vertrag von Lissabon gar nicht mehr existiert – das Regelungsinstrument der Richtlinie gewählt. Rahmenbeschlüsse dienten im Bereich der polizeilichen und justiziellen Zusammenarbeit (dritte Säule), mit dem Ziel der Förderung der Zusammenarbeit, „zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten".[48] Ebenso wie Richtlinien waren Rahmenbeschlüsse für die Mitgliedstaaten hinsichtlich des zu erreichenden Ziels verbindlich, überliessen diesen jedoch die Wahl der Form und der Mittel.[49] Im Unterschied zu diesen waren Rahmenbeschlüsse jedoch „nicht unmittelbar wirksam", sondern es handelte sich vielmehr um ein intergouvernementales, nach völkerrechtlichen Grundsätzen zu beurteilendes Instrument.[50] Damit konnte auch gerechtfertigt werden, dass Rahmenbeschlüsse allein durch den Rat beschlossen wurden und gegenüber dem Europäischen Parlament lediglich eine Anhörungspflicht bestand.[51] Mit der völkerrechtsnahen Natur der Rechtsakte im Zusammenhang stehend waren Rahmenbeschlüsse nur in beschränktem Umfang der Zuständigkeit des EuGH unterstellt, da Kompetenzen zur Vorabentscheidung lediglich insoweit bestanden, als die Mitgliedstaaten die entsprechende Zuständigkeit des Gerichtshofes ausdrücklich anerkannt hatten.[52] Demzufolge bedeutet die Verwendung der Richtlinienform vorliegend eine weitergehende Einbindung des Regelungsgegenstandes in das Unionsrecht, eine grundsätzlich grössere Verbindlichkeit gegenüber den Mitgliedstaaten und eine vollständige Erfassung der geregelten Sachfragen durch die Zuständigkeiten des EuGH. Für die Richtlinienform entschied sich die EU-Kommission mit der Begründung, dass diese am besten geeignet sei, eine materielle Harmonisierung zu erreichen und „gleichzeitig den Mitgliedstaaten bei der Umsetzung der Grundsätze, der Durchführung der Vorschriften und der Anwendung der Ausnahmebestimmungen auf nationaler Ebene den notwendigen Spielraum zu geben".[53] Insbesondere aber dürfte eine weitergehende oder gar vollständige Harmonisierung dieses Regelungsbereichs im Rahmen einer Verordnung unter den Mitgliedstaaten kaum konsensfähig gewesen sein. Angestrebt wurde vielmehr eine Mindestharmonisierung, womit den Mitgliedstaaten ein datenschutzrechtlicher Mindeststandard vorgegeben wird, für den jedoch Abweichungsmöglichkeiten zugunsten des mitgliedstaatlichen

47 Zur Ausweitung des subjektiven Anwendungsbereichs auf Private, denen öffentliche Gewalt und hoheitliche Befugnisse übertragen wurden, vgl. Art. 2 Abs. 1 i.V.m. Art. 3 Ziff. 7 lit. b VO 2016/680 sowie gerade unten.

48 Art. 34 Abs. 2 UAbs. 1 Satz 2 lit. b EUV (in der Fassung des Vertrages von Nizza).

49 Formulierung von Art. 34 Abs. 2 UAbs. 1 Satz 2 lit. b Satz 2 EUV, übereinstimmend mit Art. 249 Abs. 3 EUV (Fassung des Vertrages von Nizza) bzw. Art. 288 Abs. 3 AEUV.

50 Vgl. statt vieler *Rudolf Streinz*, Europarecht, 8. Aufl., 2008 Heidelberg u.a., 170 f.

51 Art. 34 Abs. 2 sowie Art. 39 Abs. 1 EUV (Fassung des Vertrages von Nizza).

52 Art. 35 Abs. 2 – 4 EUV (Fassung des Vertrages von Nizza).

53 Begründung zum Vorschlag vom 25.1.2012 für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM(2012) 10 endgültig, 6 (im Folgenden: Begründung Vorschlag Richtlinie)

Rechts vorgesehen sind, und über den die Mitgliedstaaten gegebenenfalls auch hinausgehen können (Art. 1 Abs. 3).[54]
Inhaltlich verfolgt die Richtlinie 2016/690 eine doppelte Zielsetzung: Zum einen bezweckt sie den Schutz natürlicher Personen bei der Verarbeitung von Daten im Bereich der Strafverfolgung, der Strafvollstreckung und der Abwehr von Gefahren für die öffentliche Sicherheit und damit zusammenhängend der Schutz der Grundrechte und Grundfreiheiten der betroffenen Personen (Art. 1 Abs. 1 und Abs. 2 lit. a). Zum anderen soll der Austausch personenbezogener Daten in diesen Bereichen zwischen den zuständigen Behörden innerhalb der EU ermöglicht werden.[55] Mit diesem doppelten Schutz- und Zirkulationsziel, welches gleichzeitig das Spannungsfeld des Regelungsgegenstandes umreisst, entspricht die Ausrichtung der Richtlinie auch der Zielstruktur der Datenschutzgrundverordnung, der das doppelte Ziel von Schutz bei der Datenverarbeitung und Gewährleistung des freien Datenverkehrs zugrunde liegt (Art. 1 Abs. 2 und 3 DGVO).[56]
Der Anwendungsbereich des Rahmenbeschlusses hatte sich in sachlicher Hinsicht auf die Verarbeitung von Daten zum Zweck der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen beschränkt; dabei musste die Verarbeitung in einer Übermittlung zwischen den Mitgliedstaaten oder einer Übermittlung zwischen Mitgliedstaaten und europäischen Behörden oder Informationssystemen bestehen (Art. 1 Abs. 2 Rahmenbeschluss 2008/977/JI). Erfasst war somit lediglich die Bereitstellung oder Übermittlung im zwischenstaatlichen Kontext, nicht hingegen die rein innerstaatliche Datenverarbeitung.[57] Die Richtlinie erweitert bzw. präzisiert den Anwendungsbereich nun in dreifacher Hinsicht:

- Erstens erstreckt sich der Anwendungsbereich der Richtlinie nunmehr auf jegliche Verarbeitung personenbezogener Daten durch die zuständigen Behörden zu den Zwecken der Richtlinie (Art. 2 Abs. 1); erfasst sind somit auch *rein innerstaatliche* und nicht lediglich grenzüberschreitende Vorgänge.
- Zweitens wurden die einschlägigen Verarbeitungszwecke der Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten oder der Vollstreckung strafrechtlicher Sanktionen (so übereinstimmend Art. 1 Abs. 2 Rahmenbeschluss 2008/977 und Art. 1 Abs. 1 RL 2016/680) ergänzt um die Gewährleistung „des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“. Hiermit werden folglich auch präventive und repressive Massnahmen im Rahmen des *polizeilichen Handelns* in den Anwendungsbereich der Richtlinie einbezogen, was dem Bestreben der Mit-

54 Vgl. dazu gerade unten.
55 Damit ist die Zielausrichtung spezifischer gefasst als noch im Rahmenbeschluss, der neben den Schutzzielen „ein hohes Maß an öffentlicher Sicherheit“ zu gewährleisten suchte: Art. 1 Abs. 1 Rahmenbeschluss 2008/977/JI; vgl. hierzu *Eva Maria Belser/Astrid Epiney/Bernhard Waldmann*, Datenschutzrecht, Bern 2011, 221 f.
56 *Belser/Epiney/Waldmann*, Datenschutzrecht (Fn. 55), 222 f.
57 *Belser/Epiney/Waldmann*, Datenschutzrecht (Fn. 55), 223.

gliedstaaten entspricht, den gesamten Polizeibereich der Richtlinie zu unterstellen.[58] Erfasst wird damit unter anderem auch die Tätigkeit der Polizei an Sportveranstaltungen oder bei Demonstrationen.[59]

- Drittens wurde der Anwendungsbereich in persönlicher Hinsicht von eigentlichen Behörden in den genannten Bereichen auf Stellen oder Einrichtungen ausgeweitet, denen gestützt auf nationales Recht die Ausübung öffentlicher Gewalt oder hoheitliche Befugnisse für die Zwecke der Richtlinie übertragen wurden (Art. 2 Abs. 1 i.V.m. Art. 3 Ziff. 7 lit. b).[60] Damit gelangt der Regelungsrahmen der Richtlinie auch auf *private Akteure*, welche mit justiziellen oder polizeilichen Aufgaben betraut wurden, zur Anwendung.

Aufgrund des gemäss Art. 2 Abs. 2 lit. d DGVO als *lex generalis—lex specialis* Verhältnis angelegten Zusammenspiels zwischen Datenschutzgrundverordnung und Richtlinie reduziert sich der Anwendungsbereich der DGVO um diese Ausweitungen des Anwendungsbereichs der Richtlinie. Aus mitgliedstaatlicher Perspektive dürfte dieser Umstand aufgrund der grösseren Regelungsspielräume im Anwendungsbereich der Richtlinie zu begrüssen sein, umgekehrt bringt diese Entwicklung jedoch vor dem Hintergrund der Vollharmonisierung der Grundverordnung im Gegenzug auch ein weniger einheitliches unionsrechtliches Schutzniveau mit sich. Relativiert wird diese Feststellung immerhin durch die Tatsache, dass auch im Regelungsbereich der Richtlinie im Grundsatz die Garantien der Grundrechtscharta zur Anwendung gelangen und somit jedenfalls ein grundrechtlicher Minimalstandard angesetzt wird.[61]
Inhaltlich gesehen ist das Verhältnis zwischen Richtlinie und Verordnung durch zahlreiche Parallelitäten der Begrifflichkeiten, Konzepte und Instrumente gekennzeichnet. Die inhaltlichen Übereinstimmungen wurden im Zuge des Gesetzgebungsprozesses im Vergleich zum Kommissionsentwurf eher noch etwas verstärkt, so beispielsweise mit der Verankerung des Instruments der Datenschutz-Folgeabschätzung auch im Anwendungsbereich der Richtlinie (Art. 27).[62] Gleichzeitig bestehen zwischen den beiden Regelungsinstrumenten jedoch auch beträchtliche Unterschiede und Divergenzen, zumeist im Sinne grösserer mitgliedstaatlicher Gestaltungsspielräume der Richtlinie im Vergleich zur Datenschutzgrundverordnung.

---

58 Entwurf der Begründung des Rates vom 8. April 2016 betreffend Standpunkt des Rates in erster Lesung im Hinblick auf den Erlass einer Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, 5418/1/16, 5 (im Folgenden Entwurf Begründung Rat). Bemerkenswert ist immerhin, dass diese Zweckausweitung in der Bezeichnung des Erlasses keinen Niederschlag gefunden hat.

59 Entwurf Begründung Rat (Fn. 58), 5.

60 Entwurf Begründung Rat (Fn. 58), 5.

61 Von der Anwendbarkeit der Charta ist aufgrund der vorliegenden „Durchführung des Unionsrechts“ gemäss Art. 51 Abs. 1 Charta jedenfalls im Grundsatz auszugehen. Inwieweit diese Voraussetzung auch bei der Wahrnehmung von Regelungsspielräumen oder Ausnahmeklauseln durch die Mitgliedstaaten gegeben ist, lässt sich an dieser Stelle nicht abschliessend beantworten. Im Resultat dürfte jedoch vieles dafür sprechen, auch in diesen Konstellationen die Schutzgarantien der Grundrechtecharta zur Anwendung zu bringen, um damit ein einheitliches grundrechtliches Schutzniveaus zu gewährleisten.

62 Vgl. dazu oben B.III.3.d).

Dennoch ist nicht zu verkennen, dass die strukturelle, konzeptuelle und begriffliche Verschränkung der beiden Instrumente jedenfalls dazu führen dürfte, dass die Grundverordnung gewissermassen als naheliegender Vergleichsstandard für die Richtlinie herangezogen und diese folglich am – relativ weitgehenden – Schutzniveau der Grundverordnung gemessen werden wird.

II. Aufbau und wesentliche Neuerungen

Im vorliegenden Rahmen kann es nicht darum gehen, eine abschliessende Erörterung der Regelungsinhalte der Richtlinie und der im Vergleich zum Rahmenbeschluss 2008/977/JI erfolgten Änderungen vorzunehmen. Vielmehr sollen im Folgenden der Aufbau der Richtlinie übersichtsartig dargestellt und die wichtigsten Neuerung kurz skizziert werden.

In der Darstellungsform des Amtsblattes hat sich der Umfang der Richtlinie im Vergleich zum Rahmenbeschluss 2008/977JI etwa verdoppelt (43 statt 20 Seiten; 64 statt 30 Artikel; 107 statt 48 Erwägungsgründe). Begrüssenswerterweise ging mit dieser Erweiterung der Regelungssubstanz auch eine Umschichtung der Regelungsinhalte innerhalb des Erlasses sowie eine bessere Strukturierung einher, welche die Zugänglichkeit des Rechtsaktes verbessern, wobei auch in der Strukturierung eine Anlehnung an die Datenschutzgrundverordnung erfolgte:

- Kap. I (Art. 1-3) enthält die allgemeinen Bestimmungen. Hierbei erfolgt neben der Festschreibung von Gegenstand und Zielen auch die Fixierung des Anwendungsbereiches und eine Festlegung der Begrifflichkeiten, die weitestgehend mit den im vorliegenden Sachzusammenhang massgeblichen Definitionen der Datenschutzgrundverordnung übereinstimmen. Eigen ist der Richtlinie der Begriff der „zuständigen Behörde“ als einer staatlichen Stelle im Bereich der Strafverfolgung oder einer anderen, vom Staat mit entsprechenden Aufgaben betrauten Stelle oder Einrichtung (Art. 3 Ziff. 7) sowie die Einengung des Begriffs des „Verantwortlichen“ auf (im obgenannten, weiten Sinne) behördliche Akteure (Art. 3 Ziff. 8).
- In Kap. II (Art. 4-11) werden die Grundsätze der Datenverarbeitung festgehalten. Zentral ist dabei neben dem Grundsatz der Rechtmässigkeit und der Richtigkeit, den Anforderungen an ein angemessenes Sicherheitsniveau und die Dauer der Speicherung insbesondere das Zweckbindungsgebot (Art. 4 Abs. 1 Bst. b und c), von dem unter Voraussetzung einer entsprechenden gesetzlichen Grundlage und unter Einhaltung des Verhältnismässigkeitsprinzips ggf. abgewichen werden kann (Art. 4 Abs. 2). Überdies verankert die Richtlinie verschiedene Datenkategorien, unter anderem im Hinblick auf unterschiedliche Kategorien betroffener Personen (Straftatverdächtige; Straftäter; Opfer; andere Parteien – Art. 6), auf eine Unterscheidung zwischen faktenbasierten Daten und persönlichen Einschätzungen (Art. 7 Abs. 1) sowie bezüglich besonders sensiblen Personendaten.
- In Kap. III (Art. 12-18) werden die Rechte der Betroffenen geregelt, wobei sich die Richtlinie inhaltlich eng an den Weiterentwicklungen der RL 95/46 durch die Datenschutzgrundverordnung orientiert. Namentlich regelt die Richtlinie die generellen Modalitäten der Information (Art. 12), statuiert eine grundsätzliche Informationspflicht gegenüber der betroffenen Personen (Art. 13) sowie ein Auskunftsrecht (Art. 14), allerdings jeweils mit relativ weitgehenden Einschränkungsmöglichkeiten (Art. 13 Abs. 3 und 4 bzw. Art. 15), und verankert ein Recht auf Berichtigung und Löschung (Art. 16). Die Wahrnehmung dieser Rechte kann auch über die Aufsichtsbehörde erfolgen, welche die betroffene Person zumindest darüber zu unterrichten hat, dass alle erforderlichen Prüfungen durchgeführt wurden (Art. 17). In Bezug auf Daten in gerichtlichen Entscheidungen sowie für Dokumente im Rahmen strafrechtlicher Ermittlungen steht den Mitgliedstaaten die Möglichkeit offen, eine Regelung im nationalen Strafprozessrecht vorzusehen (Art. 18).

- Kap. IV (Art. 19-34) enthält in den Abschnitten „Allgemeine Pflichten“, „Sicherheit personenbezogener Daten“ und „Datenschutzbeauftragter“ Vorgaben bezüglich Verantwortlichen und Auftragsverarbeitern. Dabei werden die generellen Pflichten des Verantwortlichen (Art. 19), Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 20), das Vorgehen bei mehreren Verantwortlichen (Art. 21) und bei Auftragsverarbeitung (Art. 21 f.) sowie die Zusammenarbeit mit der Aufsichtsbehörde (Art. 26 und 28) geregelt. Eine interessante Weiterentwicklung des bisherigen Rechts bilden die Vorschriften zum Verzeichnis der Verarbeitungstätigkeiten und zur Protokollierung (Art. 24 f.). Im Zuge der Beratungen des Entwurfes aufgenommen wurde auch eine an die Datenschutzgrundverordnung angelehnte Regelung zur Datenschutz-Folgeabschätzung (Art. 27). Im Gegensatz zur DGVO nicht vorgesehen ist hingegen eine Grundlage für den Einsatz zertifizierter Technologien. Bezüglich der Sicherheit personenbezogener Daten statuiert die Richtlinie die Grundsätze und verankert Meldungs- und Benachrichtigungspflichten für den Fall sogenannter „Daten-Pannen“ (Art. 29 ff.). Schliesslich stehen die Verantwortlichen künftig grundsätzlich in der Pflicht, einen Datenschutzverantwortlichen zu benennen, der frühzeitig in alle Fragen im Zusammenhang mit dem Schutz personenbezogener Daten einzubeziehen ist (Art. 32 ff.).
- Die in Kap. V (Art. 35-40) niedergelegten und im Vergleich zum Rahmenbeschluss 2008/977/JI weit ausgebauten Vorschriften schaffen einen umfangreichen Regelungsrahmen für die Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen (Art. 35 ff.).
- Kap. VI (Art. 41-49) regelt in den Abschnitten „Unabhängigkeit“ und „Zuständigkeit, Aufgaben und Befugnisse“ die Errichtung und Ausgestaltung der Aufsichtsbehörde, namentlich deren Unabhängigkeit (Art. 42), die Anforderungen an die Mitglieder (Art. 43), die Errichtung (Art. 44), die Zuständigkeit (Art. 45), die Aufgaben und Befugnisse (Art. 46 und 47), die Meldung von Verstössen (Art. 48) sowie den Tätigkeitsbericht (Art. 49). In Bezug auf die institutionelle Ausgestaltung orientiert sich die Richtlinie fast vollständig an der Regelung in der Verordnung 2016/679. Im Hinblick auf die Kompetenzen hingegen bleiben die Anforderungen hinter jener der Verordnung zurück, indem die Untersuchungsbefugnisse beispielsweise weniger ausführlich und damit vager geregelt sind, die beispielhafte Aufzählung der Abhilfebefugnisse knapper ausfällt und keine Genehmigungsbefugnisse gewährt werden. Im Vergleich zum Rahmenbeschluss (Art. 25 Abs. 2 Rahmenbeschluss 2008/977/JI) erfolgt soweit ersichtlich keine massgebliche Änderung des Kompetenzumfangs, obgleich die Befugnisse unter der neuen Regelung wesentlich spezifischer ausformuliert werden, so dass jedenfalls ein Zugewinn an Rechtssicherheit resultieren dürfte.
- Kap. VII (Art. 50 f.) enthält Vorschriften zur Zusammenarbeit, einerseits im Bereich der gegenseitigen Amtshilfe (Art. 50) und andererseits in Bezug auf den Europäischen Datenschutzausschuss (Art. 51). Im Gegensatz zur Datenschutzgrundverordnung nicht vorgesehen ist hingegen ein Kohärenzverfahren mit entsprechender Koordinationsrolle des Datenschutzausschusses und der Europäischen Kommission.
- Kap. VIII (Art. 52-57) formuliert die Rechte auf Beschwerde bei einer Aufsichtsbehörde, wobei unter anderem eine Pflicht der Aufsichtsbehörde statuiert wird, betroffenen Personen auf Ersuchen weitere Unterstützung zu gewähren (Art. 52). Sodann ist betroffenen Personen ein wirksamer Rechtsbehelf gegen sie betreffende Entscheidungen der Aufsichtsbehörden zu gewähren (Art. 53) und ein wirksamer Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter vorzusehen (Art. 54). Neu verankert wird auch das Verbandsklagerecht, wonach eine Organisation mit entsprechenden Satzungszielen im öffentlichen Interesse mit der Einreichung einer Beschwerde im Namen der betroffenen Person betraut werden kann (Art. 55). Die Richtlinie sieht ein Recht auf Schadenersatz vor, belässt aber die Bestimmung des Schadenersatzes und – im Gegensatz zur Datenschutzgrundverordnung – auch der anwendbaren Sanktionen bei Verstössen gegen die Richtlinie abgesehen von den Grundsätzen der Wirksamkeit, Verhältnismässigkeit und Abschreckung, den Mitgliedstaaten.

- Kap. IX (Art. 58) regelt das Ausschussverfahren für Durchführungsrechtsakte der Kommission (vgl. Art. 290 f. AEUV), das in der Richtlinie lediglich bei der Beurteilung der Angemessenheit des Schutzniveaus für die Übermittlung von Daten an Drittstaaten und internationale Organisationen (Art. 36 Abs. 3 bis 5) sowie für die Formulierung von Verfahren und Form der Amtshilfe (Art. 50 Abs. 8) vorgesehen ist.
- Schliesslich enthält Kap. X (Art. 59-63) die Schlussbestimmungen mit einer Umsetzungsfrist bis zum 6. Mai 2018 – wobei für automatisierte Verarbeitungssysteme ein Aufschub bis zum 6. Mai 2023 oder spätestens zum 6. Mai 2026 vorgesehen werden kann. Der Rahmenbeschluss 2008/977/JI wird demzufolge auf den 6. Mai 2018 aufgehoben (Art. 59). Im Verhältnis zu bereits geschlossenen völkerrechtlichen Abkommen bestimmt die Richtlinie, dass die vor dem Inkrafttreten geschlossenen Abkommen in Kraft bleiben, bis sie geändert, ersetzt oder gekündigt werden, sofern sie Unionsrecht nicht verletzen (Art. 61). Die weiteren Unionsrechtsakte bezüglich Datenschutz im Bereich Strafverfolgung, Strafvollstreckung sowie Schutz und Abwehr von Gefahren für die öffentliche Sicherheit, insbesondere die gegenüber den Organen und Einrichtungen der EU zur Anwendung gelangende Verordnung 45/2001, sind von der Kommission innerhalb von drei Jahren zu überprüfen, wobei insbesondere angestrebt wird, ein einheitliches Vorgehen beim Schutz personenbezogener Daten zu schaffen (Art. 62 Abs. 6 i.V.m. Art. 60).

III. Ausgewählte Aspekte

1. Zweckbindung

Nach den Vorschriften des Rahmenbeschlusses mussten Daten „zu festgelegten, eindeutigen und rechtmäßigen Zwecken“ erhoben werden und durften nur zu dem Zweck verwendet werden, zu dem sie erhoben worden sind (Art. 1 Abs. 1 Rahmenbeschluss 2008/977/JI). Vom damit statuierten Zweckbindungsprinzip durfte abgewichen werden, wenn (a) die „Verarbeitung mit den Zwecken, zu denen die Daten erhoben worden sind, nicht unvereinbar ist“, (b) eine ausreichende rechtliche Grundlage besteht und (c) die Verarbeitung zu einem anderen Zweck notwendig und verhältnismässig ist (Art. 2 Uabs. 2 Rahmenbeschluss). Wie nun aber ein alternativer Zweck mit den Erhebungszwecken „nicht unvereinbar“ sein kann, blieb dabei fraglich. Somit wies die Ausnahmeklausel letztlich eine untaugliche Formulierung auf.[63] Dies hat letztlich wohl dazu geführt, dass dem entsprechenden Kriterium die Anwendung weitgehend versagt wurde. Im Hinblick auf die Reform der Datenschutzregelungen stellte die Kommission gestützt auf die Feststellung, dass der Zweckbindungsgrundsatz zu vielen Ausnahmen zugänglich sei, eine entsprechende Anpassung in Aussicht.[64] Demzufolge lag dem Vorschlag der EU-Kommission ein relativ striktes Verständnis des Zweckbindungsgrundsatzes zugrunde, wonach eine mit den Erhebungszwecken nicht zu vereinbarende Weiterverarbeitung grundsätzlich untersagt war und die Verarbeitung mit Hinblick auf die Zwecke angemessen, sachlich relevant und nicht exzessiv zu sein hatte.[65] Letzt-

63 Vgl. dazu etwa die Kritik bei *Belser/Epiney/Waldmann*, Datenschutzrecht (Fn. 55), 225 f.

64 Mitteilung der Kommission vom 4.11.2010, Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM(2010) 609 endgültig, 15.

65 Art. 4 Bst. b und c Vorschlag für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der

lich „Gesetz“ geworden ist jedoch eine Ausnahmeklausel, die sich an der Konzeption des Rahmenbeschlusses orientiert, wonach eine Verarbeitung zu einem anderen Zweck erlaubt ist, sofern erstens dem Unionsrecht oder dem Recht des Mitgliedstaaten eine entsprechend Rechtsgrundlage zu entnehmen ist und zweitens den Grundsätzen der Erforderlichkeit und der Verhältnismässigkeit ausreichend Rechnung getragen wird. Diese auf Forderung des Rates ausgeweitete Klausel scheint insofern nicht unproblematisch, als sie keine klaren Anhaltspunkte bietet, wie die Ausnahmen vom Grundsatz der Zweckbindung zu begrenzen sind und dessen Ausformulierung somit weitgehend in das Ermessen der Mitgliedstaaten stellt.[66]

2. Datenkategorien

Ein weiteres Desideratum der EU-Kommission im Hinblick auf die Reform des Datenschutzrechtes bestand in einer weitergehenden Differenzierung nach unterschiedlichen Kategorien von Daten: Nach sachlicher Richtigkeit und Zuverlässigkeit, nach der Faktenbasiertheit sowie nach den betroffenen Personen.[67] Dieser von der EU-Kommission bereits beim Erlass des Rahmenbeschlusses verfolgte Ansatz[68] fand Niederschlag in der Richtlinie, wonach „so weit wie möglich“ zwischen verschiedenen Kategorien betroffener Personen (Strafverdächtige, Straftäter, Opfer, andere Parteien) zu unterscheiden ist (Art. 6)[69], eine Differenzierung vorgenommen werden muss zwischen faktenbasierten Daten und auf persönlichen Einschätzungen beruhenden Daten (Art. 7 Abs. 1) und bei der Datenübermittlung gegebenenfalls zusätzliche Informationen bereitzustellen sind, um eine Einschätzung der Richtigkeit, Zuverlässigkeit und Vollständigkeit der Daten zu ermöglichen (Art. 7 Abs. 2). Insbesondere eine Kategorisierung anhand der beiden letztgenannten Kriterien erscheint insofern grundsätzlich stimmig, als sie datenverarbeitenden Personen bei der Bewertung von Informationsgehalt und Richtigkeit hilfreich sein können. Immerhin lässt sich die Frage aufwerfen, ob sich die Differenzierung nach Faktenbasiertheit bzw. persönlicher Einschätzung nicht bereits aus der Vorgabe der Datenrichtigkeit ergibt, wäre doch ein Datum, das fälschlicherweise vorgibt oder

Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM(2012) 10 endgültig (im Folgenden: Vorschlag Richtlinie).

66 Vgl. auch die entsprechende Kritik in: Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Datenschutzrechtliche Kernpunkte für die Trilogverhandlungen der Datenschutz-Richtlinie im Bereich Justiz und Inneres, Empfehlungen vom 29.10.2015, 4 (abrufbar unter <https://www.datenschutz.hessen.de/entschliessungen.htm>).

67 Mitteilung Kommission (Fn. 64), 15; vgl. auch bereits Grundsatz 3.2 Empfehlung R (87) 15 des Ministerkomitees des Europarates an die Mitgliedstaaten zur Regelung der Benutzung personenbezogener Daten durch die Polizei vom 17. September 1987.

68 Vgl. Art. 4 Abs. 1 Bst. d und Art. 4 Abs. 3 Entwurf Rahmenbeschluss, KOM(2005) 475 endgültig.

69 Eine entsprechende Unterscheidung wurde bereits im Hinblick auf den Erlass des Rahmenbeschlusses vorgebracht (Art. 4 Abs. 3 Entwurf, KOM(2005) 475 endgültig) und findet sich auch in Artikel 14 Europol-Beschluss 2009/371/JI sowie Artikel 15 Eurojust-Beschluss 2009/426/JI.

den Eindruck erweckt, auf Fakten zu basieren, wohl zugleich als unrichtig zu qualifizieren.[70] Im Übrigen dürfte sich die Faktenbasiertheit oftmals aus den Umständen ergeben. Die Differenzierung nach betroffenen Personen scheint insoweit zielführend, als etwa das öffentliche Interesse an der Speicherung der Daten und umgekehrt das Interesse auf Löschung je nach Personenkategorie unterschiedlich gross sein dürfte. Eine Verknüpfung mit entsprechenden Pflichten in der Verarbeitung der Daten ist der Richtlinie jedoch nicht zu entnehmen (jedenfalls soweit sie sich nicht ohnehin bereits aus dem Verhältnismässigkeitsprinzip ergibt). Insofern ist nicht ersichtlich, welchem konkreten Zweck die Differenzierungsvorgabe von Art. 6 dienen sollte.

3. Verzeichnisführung und Protokollierung

Eine Neuerung im Vergleich zum Rahmenbeschluss und eine (weitgehende) Parallelität zur Datenschutzgrundverordnung stellt die Pflicht von Verantwortlichen und Auftragsverarbeitern dar, ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Hierzu sind die Kategorien von Verarbeitungstätigkeiten in einem Verzeichnis zu führen (im Unterschied zur Führung eines Verzeichnisses bezüglich der einzelnen Verarbeitungstätigkeiten gemäss Art. 30 Abs. 1 und 2 DGVO), wobei die Richtlinie im Einzelnen spezifiziert, welche Angaben das Verzeichnis enthalten muss (Art. 24 Abs. 1 und 2). Die Pflichten der Richtlinie sind dabei insofern strenger ausgestaltet als jene der Verordnung, als keine Ausnahmeklausel für „kleine" Datenverarbeiter vorgesehen ist (so Art. 30 Abs. 5 DGVO). Dieser Ausgestaltung dürfte die – zutreffende – Wertung innewohnen, dass Datenverarbeitung im Bereich von Justiz und Polizei generell ein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, eine Voraussetzung, gemäss der auch nach der Grundverordnung von der Ausnahme der Verzeichnisführungspflicht abzuweichen ist.

Über die Vorgaben der Grundverordnung und die vormaligen Pflichten des Rahmenbeschlusses hinausgehend sieht die Richtlinie eine Pflicht zur Dokumentierung bestimmter automatisierter Verarbeitungsvorgänge vor: Buch zu führen ist mindestens über die Erhebung, Veränderung, Abfrage, Offenlegung einschliesslich Übermittlung, Kombination und Löschung der Daten. Die Dokumentierung der Abfragen und Offenlegungen soll es insbesondere ermöglichen, Informationen zu gewinnen, wer, wann, mit welcher Begründung Daten abgefragt oder offengelegt hat und wer sie empfangen hat (Art. 25 Abs. 1). Der Rahmenbeschluss hatte dagegen lediglich die Protokollierung der Übermittlung vorgeschrieben (Art. 10 Abs. 1 Rahmenbeschluss 2008/977/JI). Übernommen wurde hingegen die enge Zweckbindung der Protokolle, wonach diese lediglich zur Überprüfung der Rechtmässigkeit, der Sicherstellung der Integrität und Sicherheit sowie neu für Eigenüberwachung und Strafverfahren verwendet werden dürfen (25 Abs. 2). Diese Protokollierungspflicht könnte durchaus ein geeignetes Instrument darstellen, um ausufernde Verarbeitungsaktivitäten und insbesondere unnötige Weitergaben der bearbeiteten Daten im Zaum zu halten, da die Möglichkeit einer späteren Kontrolle einen eher zurückhal-

[70] Abgesehen davon dürfte jedenfalls eine trennschafte Unterscheidung zwischen Fakten und Einschätzungen im Grundsatz ohnehin grossen Schwierigkeiten unterworfen sein, basieren doch auch Fakten stets auf einer Einschätzung und einer Wahrnehmung.

tenden Umgang mit den Daten bewirken dürfte. Der Ausbau der Protokollierungspflicht ist somit als eine begrüssenswerte Weiterentwicklung des Rechtsrahmens im Datenschutz bezüglich Polizei- und Jusitzdaten zu betrachten und es stellt sich die Frage, ob analoge Pflichten mit zunehmenden technischen Möglichkeiten, welche solche Protokollierungen künftig einfacher machen dürften, nicht auch in anderen Bereichen, etwa im Umgang mit sensiblen Daten oder in der Handhabung besonders grosser Datenvolumen, verankert werden sollten. Weniger unmittelbar ersichtlich ist hingegen der Nutzen der Verzeichnisführungspflicht, insbesondere soweit sich diese nicht auf einzelne Datenverarbeitungen, sondern lediglich auf deren Kategorien bezieht. Hierbei ist in der Umsetzung darauf zu achten, dass sich die damit einhergehende administrative Bürde und der Nutzen der Pflicht die Waage halten.

4. Übermittlung in Drittländer und an internationale Organisationen

Eine wesentlich umfassendere Regelung als noch unter dem Rahmenbeschluss findet künftig die Übermittlung von Daten in Drittländer oder an internationale Organisationen, wobei sich das neue Regime in seinem grundsätzlichen Aufbau an jenes der Datenschutzgrundverordnung anlehnt. Ausgeweitet wird zunächst der Anwendungsbereich der Regelung, der sich auf sämtliche Datenübermittlungen an Drittländer erstreckt, während sich das Regime des Rahmenbeschlusses lediglich auf Daten bezog, welche die nationalen Behörden von den Behörden anderer Mitgliedstaaten erhalten haben.[71]

- Zur Übermittlung erforderlich ist zunächst das Vorliegen von *drei allgemeinen Voraussetzungen* (Art. 35 Abs. 1):
  - Die Übermittlung muss zur Erreichung der Richtlinienzwecke *erforderlich* sein (Art. 35 Abs. 1 lit. a);
  - beim Empfänger muss es sich grundsätzlich um eine im Sinne der Richtlinie *zuständige Behörde* handeln (Art. 35 Abs. 1 lit. b). Eine direkte Übermittlung an andere Empfänger ist lediglich unter restriktiven Bedingungen zulässig, namentlich wenn die Übermittlung an die zuständige Behörde etwa aufgrund der zeitlichen Dringlichkeit als wirkungslos betrachtet wird, die Übermittlung zur Zweckerreichung unbedingt erforderlich ist und die Grundrechte und Grundfreiheiten der betroffenen Person in der Abwägung nicht überwiegen (Art. 39);
  - es muss eine *Genehmigung* des betreffenden Mitgliedstaats vorliegen, wenn Daten übermittelt werden sollen, die ursprünglich auch aus einem anderen Mitgliedsstaat stammen. Vorbehalten sind Fälle unmittelbarer und ernsthafter Gefahr für die öffentliche Sicherheit (Art. 35 Abs. 1 lit. c und Abs. 2).
- Überdies muss ein *Erlaubnistatbestand* gegeben sein (Art. 35 Abs. 1 lit. d sowie Art. 36 ff.):
  - Mit dem *Angemessenheitsbeschluss* bestätigt die Kommission im Rahmen eines Durchführungsrechtsakts, dass ein Drittland bzw. eine internationale Organisation ein angemessenes Schutzniveau bietet, wobei der

[71] Art. 13 Abs. 1 Rahmenbeschluss 2008/977/JI.

Richtlinie Vorgaben zu den hierfür heranzuziehenden Kriterien (Rechtsstaatlichkeit, Achtung der Menschenrechte und Grundfreiheiten etc.) zu entnehmen sind (Art. 36).

- *Geeignete Garantien* können als Grundlage für eine Übermittlung herangezogen werden, wenn sie entweder in einem rechtsverbindlichen Instrument verankert sind oder der Verantwortliche gestützt auf eine umfassende Abwägung zum Schluss gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten vorliegen (Art. 37). Vom Gebrauch letzterer Option ist die Aufsichtsbehörde in Kenntnis zu setzten und er ist zu dokumentieren. Diese Möglichkeit zur Selbsteinschätzung erscheint nicht unproblematisch, da es zu verhindern gilt, dass auf diesem Wege der geschaffene Schutzrahmen unterminiert wird und die Übermittlung letztlich weitestgehend dem Ermessen des Verantwortlichen überlassen bleibt.[72]
- Schliesslich kann sich die Übermittlungserlaubnis gestützt auf die vorgesehenen *Ausnahmebestimmungen* ergeben, wenn die Übermittlung erforderlich ist, um lebenswichtige Interessen einer Person zu schützen, rechtlich geschützte berechtigte Interessen der betroffenen Person zu wahren, eine unmittelbare oder ernsthafte Gefahr für die öffentliche Sicherheit abzuwenden oder im Einzelfall die Zwecke der Richtlinie zu erreichen oder Rechtsansprüche im Zusammenhang mit diesen Zwecken geltend zu machen oder auszuüben (Art. 38 Abs. 1). Sehr weit gefasst sind dabei die beiden letztgenannten Gründe, da den Übermittlungen definitionsgemäss die Erreichung dieser Zwecke zu Grunde liegen dürfte und die Zweckausrichtung überdies ohnehin eine allgemeine Voraussetzung der Übermittlung darstellt (Art. 36 Abs. 1 lit. a). Somit durchbricht diese Option einerseits die Systematik der Voraussetzungen und spannt andererseits und insbesondere die Übermittlungsmöglichkeiten überaus weit.[73] Daran vermag auch die Vorgabe nichts zu ändern, dass Übermittlungen in diesen Konstellationen erstens nur im Einzelfall stattfinden dürfen (Art. 38 Abs. 1 lit. d und e) und zweitens das öffentliche Interesse an einer Übermittlung gegen die grundrechtlichen und grundfreiheitlichen Positionen der betroffenen Person abgewogen werden müssen (Art. 38 Abs. 2).

Überblickt man den hiermit geschaffenen Regelungsrahmen, so wird der erste Eindruck einer vergleichsweise restriktiven Ausformung der Übermittlungsvoraussetzungen dadurch relativiert, dass im Rahmen der Erlaubnistatbestände vergleichsweise weitgefasste Ausnahmeklauseln bestehen, so dass das anwendbare Schutzniveau letztlich massgeblich davon abhängen dürfte, wie diese Klauseln in der Praxis gehandhabt werden.

---

72 Kritisch – allerdings noch unter Bezugnahme auf den Kommissionsvorschlag – auch *Matthias Bäcker/Gerrit Hornung*, EU-Richtlinie für die Datenverarbeitung bei Polizei und Justiz in Europa, ZD 4/2012, 151.

73 Vgl. auch die entsprechende kritische Würdigung des Kommissionsvorschlages bei *Bäcker/Hornung*, ZD 4/2012 (Fn. 73), 151.

5. Rolle der EU-Kommission

Die frühere Ansiedlung des Regelungsgegenstandes der Richtlinie in der dritten Säule der Europäischen Union scheint mit Blick auf die Ausformulierung der Vorschriften der Richtlinie einerseits in den weitergehenden Regelungsspielräumen der Mitgliedstaaten in diesem Bereich auf, welche bereits aufgrund des gewählten Regelungsinstruments der Richtlinien ersichtlich wird. Andererseits zeigt sich das geringere Mass der „Unionisierung" auch an der weniger ausgebauten Rolle der EU-Kommission bei der Konkretisierung und Umsetzung des Rechtsrahmens in diesem Sachbereich: Im Unterschied zur Datenschutzgrundverordnung kennt die Richtlinie etwa die Instrumente der Verhaltensregeln und der Zertifizierung nicht, bei deren Erarbeitung der Kommission gewisse Befugnisse zukommen,[74] sodann sieht die Richtlinie kein Kohärenzverfahren vor, welches der Kommission (und insbesondere auch dem Ausschuss) Einflussmöglichkeiten im Rahmen der Zusammenarbeit im europäischen Behördengefüge einräumen würde[75] und schliesslich bestehen nach der Richtlinie auch geringere Möglichkeiten zum Erlass von delegierten Rechtsakten und Durchführungsrechtsakten.[76] Somit folgt die Rollenzuteilung der Organe und Einrichtungen (Kommission und Zusammenarbeitsgremium Ausschuss) in diesem Bereich der zurückhaltenderen Ausformung der materiellrechtlichen Vorgaben im Vergleich zur Datenschutzgrundverordnung.

IV. Würdigung

Im Gegensatz zur Datenschutzgrundverordnung wird mit dem Erlass der Richtlinie keine Vollharmonisierung vollzogen, sondern den Mitgliedstaaten verbleiben weiterhin beträchtliche Regelungsspielräume: Zum einen steht es ihnen ausdrücklich frei, im Regelungsbereich des Rechtsaktes Garantien vorzusehen, die strenger sind als die Garantien der Richtlinie (Art. 1 Abs. 3). Das Unionsrecht statuiert in diesem Bereich demzufolge lediglich einen Mindeststandard für den Schutz personenbezogener Daten. Zum anderen enthält die Richtlinie eine Reihe von Ausnahmetatbeständen mit Abweichungsmöglichkeiten von einem diesfalls lediglich dispositiv geltenden Schutzniveau. Solche Abweichungen sind zunächst möglich, wenn (1.) die Richtlinie die Möglichkeit vorsieht, bestimmte Sachbereiche entweder direkt oder durch entsprechende Begriffsdefinitionen von ihrem *Anwendungsbereich* auszunehmen, beispielsweise indem die Betroffenenrechte bezüglich Daten in gerichtlichen Entscheidungen oder in Dokumenten strafrechtlicher Ermittlungen dem mitgliedstaatlichen Recht unterstellt werden können (Art. 18) oder durch Definition der mit hoheitlichen Befugnissen betrauten Stellen und Einrichtungen (Art. 3 Ziff. 7 lit. b). Sodann sieht die Richtlinie (2.) *Einschränkungsmöglichkeiten* von eingeräumten Rechten vor, etwa wenn die behördliche Informati-

74 Art. 40 f. VO 679/2016.

75 Vgl. Art. 63 ff. VO 679/2016, wobei anzumerken bleibt, dass die Kompetenzen der Kommission, insbesondere zu Gunsten der Befugnisse des Ausschusses, im Vergleich zum ursprünglichen Kommissionsvorschlag massgebliche Beschränkungen erfahren haben.

76 Vgl. Art. 92 i.V.m. Art. 12 Abs. 8 und Art. 43 Abs. 8 VO 679/2016 sowie Art. 40 Abs. 9, 43 Abs. 9, 45 Abs. 3 u. 5, Art. 47 Abs. 3, Art. 61 Abs. 9 und Art. 67 VO 679/2016.

onspflicht, das Auskunftsrecht der betroffenen Personen oder das Recht auf Berichtigung, Löschung oder die Einschränkung der Bearbeitung gesetzlich eingeschränkt werden können (Art. 13 Abs. 3, Art. 15 Abs. 1 bzw. Art. 16 Abs. 4). Überdies kann das Recht der Mitgliedstaaten (3.) die *Handlungsmöglichkeiten* der Verantwortlichen unterschiedlich weit bemessen und damit die Grenzen der Datenverarbeitung enger oder weiter ziehen, zum Beispiel in der Ausgestaltung der anderweitigen Verarbeitungszwecke im nationalen Recht, indem Datenverarbeitung auch ausserhalb der Richtlinienzwecke ermöglicht wird (Art. 4 Abs. 2) oder indem für die Bearbeitung besonderer Kategorien personenbezogener Daten eine mitgliedstaatliche Rechtsgrundlage vorgesehen wird (Art. 10 lit. a. Diese divergierenden mitgliedstaatlichen Handlungsgrundlagen haben im Resultat auch unterschiedlich bemessene Standards der Rechtmässigkeit zur Folge (Art. 8 Abs. 1). Schliesslich erlaubt es die Richtlinie (4.), die darin vorgesehenen *behördlichen Befugnisse* teilweise durch mitgliedstaatliches Recht im Einzelnen auszuformen, wenn die justizielle Tätigkeit von Gerichten vom Zuständigkeitsbereich der Aufsichtsbehörde ausgenommen werden kann (Art. 45 Abs. 2). Aus diesen Abweichungsmöglichkeiten vom Standard der Richtlinie ergibt sich das Bild, dass im Zusammenspiel zwischen Unionsrecht und mitgliedstaatlichem Recht kein einheitlicher Schutzstandard resultiert.

Ebenfalls keine Einheitlichkeit erreicht die Richtlinie in Bezug auf die unterschiedlichen Datenschutzregelungen der Europäischen Union, nachdem einerseits das generelle Regelungsregime der Datenschutzgrundverordnung weiterhin abweicht vom Regelungsrahmen im Bereich Justiz und Polizei und hierzu etwa in Bezug auf das Schengener Informationssystem, das Visa-Informationssystem, das Zollinformationssystem, Eurojust, Europol, dem Vertrag von Prüm entstammende Regeln, den Rahmenbeschluss 2006/960 über den Austausch von Informationen zwischen Strafverfolgungsbehörden oder die neue Richtlinie über Verwendung von Fluggastdaten zur Strafverfolgung weiterhin abweichende Regelungsregime bestehen.[77] Folglich wurde das von der Kommission ursprünglich ins Auge gefasste Ziel verfehlt, die Bereiche der polizeilichen und justiziellen Zusammenarbeit in Strafsachen in den Anwendungsbereich der allgemeinen Datenschutzbestimmungen einzubeziehen sowie die sektorspezifischen Vorschriften in diesem Bereich zu ersetzen.[78]

Ein direkter und präziser Vergleich des Schutzniveaus von Grundverordnung und Richtlinie lässt sich aufgrund der teilweise unterschiedlichen Strukturierung und Ausgestaltung der Garantien, dem ungleichen Harmonisierungsgrad und den divergierenden Regelungen verschiedener Instrumente und Befugnisse kaum übergreifend ziehen. So sieht die Richtlinie etwa mit der Protokollierungspflicht (Art. 25) zusätzliche Schutzkautelen vor[79] und kennt geringere Beschränkungsmöglichkeiten des Rechts auf Löschung[80], umgekehrt enthält die Richtlinie hingegen zum Beispiel Einschränkungsmöglichkeiten des Auskunftsrechts (Art. 15), wie sie in

77 Für einen Überblick der unterschiedlichen Regelungsrahmen vgl. *Belser/Epiney/Waldmann*, Datenschutzrecht (Fn. 55), 222 f.

78 Mitteilung der Kommission vom 4.11.2010, Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM(2010) 609 endgültig, 16.

79 Art. 25 RL 2016/680.

80 Vgl. Art. 16 Abs. 4 RL 2016/680 mit Art. 17 Abs. 4 VO 2016/679.

der Grundverordnung nicht vorgesehen sind. Insbesondere aber erlauben die obgenannten zahlreichen Abweichungsmöglichkeiten vom unionsrechtlichen Standard kaum eine umfassende Einschätzung des Datenschutzniveaus der Richtlinie, hängt dieses doch massgeblich vom mitgliedstaatlichen Recht ab. Gerade vor dem Hintergrund dieser Abweichungsmöglichkeiten lässt immerhin festhalten, dass dem Unionsrecht selbst in diesem Bereich weder besonders strenge noch einheitliche Datenschutzvorgaben zu entnehmen sind. Die Ausweitung des Anwendungsbereichs der Richtlinie im Vergleich zum Rahmenerlass hat nun zur Konsequenz, dass in weiteren Sachbereichen dieses uneinheitliche und eher lose Schutzregime der Richtlinie statt der harmonisierte allgemeine Regelungsrahmen der Grundverordnung zur Anwendung gelangt.

D. Zu den Implikationen für die Schweiz

Die Schweiz ist über die sog. Schengen- und Dublinassoziierung[81] auch an datenschutzrechtliche Vorgaben des EU-Rechts gebunden,[82] soweit diese in den Anhängen der Abkommen entsprechend vermerkt sind, womit die entsprechenden Rechtsakte Teil des sog. Schengen- und Dublin-Besitzstands sind, wobei hier in Bezug auf die genaue Reichweite dieser Einbindung der Schweiz in den unionsrechtlichen Besitzstand nach wie vor noch einiges streitig ist.[83] Die RL 95/46 figuriert in den

---

81 Abkommen zwischen der Schweizerischen Eidgenossenschaft, der Europäischen Union und der Europäischen Gemeinschaft über die Assoziierung dieses Staates bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands, SR 0.362.31; Abkommen zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Gemeinschaft über die Kriterien und Verfahren zur Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat oder in der Schweiz gestellten Asylantrags, SR 0.142.392.68.

82 Vgl. schon *Astrid Epiney*, Datenschutz und „Bilaterale II", SJZ 2006, 121 ff.; *Epiney/Hofstötter/Meier/Theuerkauf*, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen (Fn. 15), 263 ff.; *Simone Füzesséry Minelli/Stephan C. Brunner*, La protection des données et les Accords Schengen/Dublin, in: Christine Kaddous/Monique Jametti Greiner (Hrsg.), Bilaterale Abkommen II Schweiz – EU und andere neue Abkommen, 2006, 426 (428 ff.); s. auch *Markus Schefer/Sandra Stämpfli*, Die Grundlagen des Datenschutzes im Rahmen von Schengen, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Schengen in der Praxis. Erfahrungen und Ausblicke, 2009, 135 ff.; *Stephan C. Brunner*, Datenschutz im Rahmen von Schengen. Die neuen Rechtsgrundlagen in der Schweiz, in: Stephan Breitenmoser/Sabine Gless/Otto Lagodny (Hrsg.), Schengen in der Praxis. Erfahrungen und Ausblicke, 2009, 189 ff.

83 Dies in erster Linie bezüglich der genauen Reichweite der Bindungswirkung der RL 95/46 für die Schweiz (lediglich für die von der Schengen-/Dublin-Assoziierung erfasste Bereiche oder allgemeine Verbindlichkeit, ähnlich wie für einen EU-Mitgliedstaat), vgl. für die zuletzt genannte Ansicht *Epiney*, SJZ 2006 (Fn. 83), 121 (122 ff.); *Epiney/Hofstötter/Meier/Theuerkauf*, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen (Fn. 15), 263 ff.; *Carmen Langhanke*, Datenschutz in der Schweiz. Reichweite der europarechtlichen Vorgaben, ZD 2014, 621 ff.; a.A. *Stephan C. Brunner*, Zur Umsetzung von „Schengen" und „Dublin" im Bereich des Datenschutzes: Drei Thesen, in: Astrid Epiney/Patrick Hobi (Hrsg.), Die Revision des Datenschutzgesetzes / La révision de la Loi fédérale sur la protection des données, 2009, 139 (140 ff.); *Beat Rudin/Bruno Baeriswyl*, „Schengen" und der Datenschutz in den Kantonen: Anforderungen – Beurteilung – Handlungsbedarf, in: Astrid

Anhängen beider Abkommen, während der Rahmenbeschluss 2008/977/JI nur in den Anhang des Schengener Abkommens aufgenommen wurde.[84] Da die erwähnten Assoziierungsabkommen in den „Übernahmemechanismen" auch eine grundsätzliche Übernahme der Weiterentwicklungen des Schengen- und Dublin-Besitzstands vorsehen, könnte man auf den ersten Blick annehmen, die Schweiz werde im Zuge der Anwendung dieser Mechanismen[85] nach der Übernahme der neuen Rechtsakte in die Anhänge der genannten Abkommen im Ergebnis auch die Vorgaben der Datenschutzgrundverordnung und der Richtlinie zum Datenschutz bei der Strafverfolgung zu beachten haben.

Dieser Schluss gilt jedoch nur für die Richtlinie, nicht jedoch für die Datenschutzgrundverordnung: Die Richtline sieht in Erwägung 102 vor, dass es sich hierbei um eine Weiterentwicklung des Schengen-Besitzstandes handelt, womit das Instrument in den Anhang des Abkommens aufzunehmen und die Schweiz in den entsprechenden unionsrechtlichen Besitzstand einzubeziehen ist. Interessanterweise fehlt hingegen in Bezug auf die Datenschutzgrundverordnung jeglicher Hinweis darauf, dass sie Teil des Schengen-Besitzstandes ist bzw. sein soll, was insofern überrascht, als dies bei der RL 95/46 – die ja durch die Datenschutzgrundverordnung aufgehoben wird – der Fall ist. Ein Erklärungsansatz hierfür wäre, dass der Unionsgesetzgeber aufgrund der Ausweitung des Anwendungsbereiches der Richtlinie im Vergleich zum Rahmenbeschluss davon ausgegangen sein könnte, dass die Anwendungsfälle im Bereich von „Schengen" und „Dublin" nunmehr vollständig durch die Richtline abgedeckt werden. Bei näherer Betrachtung sollte jedoch die Ablösung der in den Abkommen genannten RL 95/46 durch die Datenschutzgrundverordnung sowie der Umstand, dass sich im Rahmen von „Schengen" und „Dublin" zahlreiche datenschutzrechtliche Fragen stellen im Gegensatz zur Ansicht des Unionsgesetzgebers dafür sprechen, dass auch die Verordnung als Teil des Schengen-Besitzstandes hätte angesehen werden müssen. Die Frage, ob ein Rechtsakt Teil des Schengen-Besitzstandes ist oder nicht, ist im Übrigen durchaus eine Rechtsfrage, die Gegenstand der gerichtlichen Überprüfung durch den EuGH ist bzw. sein kann. Allerdings unterliegt es einigen Zweifeln, ob es zu einem entsprechenden Verfahren kommen wird: Eine Nichtigkeitsklage (Art. 263 AEUV) wäre hier zwar grundsätzlich denkbar; es ist jedoch zu bezweifeln, dass einer der privilegiert Klagebefugten klagen wird. Darüber hinaus kann die Gültigkeit eines Rechtsakts auch im Rahmen des Art. 267 AEUV (Vorabentscheidungsverfahren) geprüft werden; hierfür müsste jedoch gerade diese Frage für die Entscheidung einer bei einem mitgliedstaatlichen Gericht anhängigen Streitsache relevant sein, was theoretisch möglich ist, sich aber wohl kaum in absehbarer Zeit realisieren dürfte (wenn dies auch nicht ausgeschlossen ist). Vor diesem Hintergrund bleibt es in Bezug auf die Schweiz dabei, dass für diese nach wie vor die RL 95/46 massgeblich sein wird, während in den EU-Mitgliedstaaten die Datenschutzgrundverordnung

Epiney/Sarah Theuerkauf (Hrsg.), Datenschutz in Europa und die Schweiz / La protection des données en Europe et la Suisse, 2006, 169 (175 f.).

84 Notenaustausch vom 14. Januar 2009 zwischen der Schweiz und der Europäischen Union betreffend die Übernahme des Rahmenbeschlusses 2008/977/JI vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, SR 0.362.380.041.

85 Vgl. im Einzelnen zu diesen *Astrid Epiney/Beate Metz/Benedikt Pirker*, Zur Parallelität der Rechtsentwicklung in der EU und in der Schweiz, 2012, 140 ff.

gilt, ein Ergebnis, das in einem gewissen Spannungsverhältnis zur Zielsetzung der Schengen- und Dublinassoziierung, im Verhältnis zur Schweiz in den betroffenen Bereichen eine möglichst parallele Rechtslage sicherzustellen, steht.

Dieser Befund ändert jedoch nichts daran, dass die Datenschutzgrundverordnung und die Rechtsprechung des EuGH, die zu dieser zweifellos ergehen wird, für die Schweiz von Bedeutung sind, wobei in erster Linie auf drei Aspekte hinzuweisen ist:

- Erstens knüpft die Verordnung – trotz aller Neuerungen – in zahlreichen Bereichen an bereits in der RL 95/46 enthaltene Regelungen an. Soweit also z.B. Rechtsprechung des EuGH zu solchen übernommenen oder ggf. auch präzisierten Regelungen ergeht, kann diese durchaus auch für die Auslegung der RL 95/46 und damit für die Schweiz von Bedeutung sein. Im Einzelfall sind hier aber schwierige Abgrenzungsfragen zu gewärtigen.
- Zweitens sind in der Schweiz tätige Unternehmen aufgrund des weiten Anwendungsbereichs der Datenschutzgrundverordnung insofern betroffen, als sie sich bei Vorliegen der skizzierten Voraussetzungen an die Vorgaben der Verordnung zu halten haben.
- Schliesslich ist es auch darüber hinaus sinnvoll, in diesem Bereich die unionsrechtlichen Entwicklungen zumindest zur Kenntnis zu nehmen und in die Betrachtungen einzubeziehen, zumal gewisse Aspekte auch im Rahmen der laufenden Revision der Datenschutzkonvention des Europarates – die nach ihren erklärten Zielsetzungen inhaltlich mit den Entwicklungen auf EU-Ebene abgestimmt werden soll[86] – relevant sein dürften. Hier könnte es gar zu einer Art „Harmonisierung" der in der Union einerseits und in der Schweiz andererseits geltenden rechtlichen Vorgaben aufgrund des Abschlusses eines sowohl für die Union als auch für die Schweiz verbindlichen völkerrechtlichen Vertrages kommen, dies soweit davon auszugehen ist, dass das Unionsrecht im Ergebnis und zumindest in weiten Teilen insbesondere durch die Datenschutzgrundverordnung die Vorgaben der revidierten Datenschutzkonvention des Europarates umsetzen will. Denn diesfalls wären im Ergebnis auch die Datenschutzgrundverordnung (bzw. Teile derselben) sowie die zu ihr ergehende Rechtsprechung für die Schweiz relevant, stellt doch die Praxis der Vertragsparteien ein bei der Auslegung eines völkerrechtlichen Vertrages zu berücksichtigendes Element dar (vgl. Art. 31 Abs. 3 lit. b VRK).[87]

Überblickt man nun das mit der neuen Datenschutzordnung in der EU für die Schweiz zur Anwendung gelangende Recht, zeigt sich eine geradezu paradox anmutende Situation: Während die sachlich im Bereich Justiz und Polizei angesiedelte Richtlinie, die aufgrund ihrer Souveränitätsnähe zurückhaltend und nur teilweise harmonisiert ausgestaltet wurde, durch die Schweiz als Teil des Schengen-

86 Vgl. hierzu, m.w.N., *Cécile de Terwangne*, La modernisation de la Convention 108 du Conseil de l'Europe, in: Astrid Epiney/Tobias Fasnacht (Hrsg.), Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes und Implikationen für die Schweiz/Le développement du droit européen en matière de protection des données et ses implications pour la Suisse, 2012, 23 ff. sowie den Beitrag von *Jean-Philippe Walter* (in diesem Band).

87 S. hierzu, im Zusammenhang mit der sog. Aarhus-Konvention, *Astrid Epiney*, Rechtsprechung des EuGH zur Aarhus-Konvention und Implikationen für die Schweiz. Zugleich ein Beitrag zu den Vorgaben der Aarhus-Konvention in Bezug auf das Verbandsbeschwerderecht, AJP 2011, 1505 (1511 f.).

Besitzstandes umgesetzt werden muss, wäre die Datenschutzgrundverordnung, die insbesondere auch mit Blick auf das Funktionieren des Binnenmarktes erlassen wurde, somit hauptsächlich eine marktorientierte Ausrichtung aufweist und wohl als „souveränitätsferner" zu bezeichnen ist, nicht ins nationale Recht zu übernehmen.

E. Schluss

Das (noch) geltende Datenschutzrecht der Europäischen Union stammt überwiegend aus einer Zeit, die sich namentlich in Bezug auf die technologischen Möglichkeiten der Datenverarbeitung von der heutigen weitgehend unterscheidet. Themen wie *big data*, das *internet of things*, soziale Netzwerke oder mobile Internetapplikationen haben damals in dieser Form noch nicht existiert und stellen heute beträchtliche Herausforderungen für den Datenschutz dar. Dementsprechend war es höchste Zeit, den Rechtsrahmen dieses dynamischen Regelungsgegenstandes neu zu fassen und weitergehend mit den Lebensrealitäten in Einklang zu bringen. Insbesondere die Datenschutzgrundverordnung mit ihren teilweise innovativen Ansätzen (*privacy by design*, *privacy by default*, Datenschutzfolgeabschätzung, Zertifizierungslösungen etc.) lässt sich nun durchaus als wichtigen Schritt in diese Richtung qualifizieren, wenn auch zu konzedieren ist, dass diese Instrumente hiermit erst im Grundsatz angelegt sind und zunächst noch im Einzelnen ausgeformt und dann insbesondere stimmig umgesetzt werden müssen. Für Wirksamkeit und Tragweite noch bedeutsamer als die Ausgestaltung der einzelnen Instrumente dürfte hingegen die Ausweitung des Anwendungsbereiches der Datenschutzgrundverordnung und die Verwirklichung einer tatsächlichen Vollharmonisierung sein, da dies die Chance birgt, einerseits durch Vereinheitlichung der Regeln das Funktionieren des Binnenmarktes zu vereinfachen und andererseits und insbesondere als ein mit einem gewichtigen Markt verbundener einheitlicher Datenschutzraum gegenüber Drittstaaten aufzutreten.

Gerade vor dem Hintergrund, dass in den in jüngerer Zeit ergangenen Urteilen des EuGH im Datenschutzbereich (*Google Spain* und *Google Inc.*, *Digital Rights Ireland*, *Schrems* etc.) grundrechtliche Erwägungen eine bedeutende Rolle gespielt haben, stellt sich die Frage des künftigen Zusammenspiels zwischen dem sekundärrechtlichen und dem primär- bzw. grundrechtlichen Datenschutz innerhalb der Europäischen Union. Hierzu ist zunächst festzuhalten, dass die Vollharmonisierung der Datenschutzgrundverordnung die Anwendung nationaler Grundrechte und ein darauf allenfalls basierender höherer Schutzstandard ausschliesst, während im Anwendungsbereich der Richtlinie je nach Konstellation die Grundrechte der Charta und die mitgliedstaatlichen Grundrechtsgarantien zur Anwendung kommen können. Nachdem die Zurückdrängung der nationalen Grundrechte mit Blick auf die Reform teilweise kritisiert worden waren, erscheint es nicht gänzlich abwegig, die genannten Urteile des EuGH als Zeichen dafür zu werten, dass der Gerichtshof bestrebt ist, inskünftig gestützt auf die Charta einen umfassenden Grundrechtsschutz zu gewährleisten und seine Rolle als „Verfassungsgericht" der Europäischen Union in ambitionierter Art und Weise wahrzunehmen. Die Ausfüllung dieser Rolle durch den Gerichtshof lässt sich darüber hinausgehend möglicherweise sogar als genereller Lackmustest für diese Funktion betrachten, woran sich somit letztlich

zeigen könnte, ob und inwieweit der EuGH gewillt ist, seine Rolle als jene eines Grundrechtswächters zu verstehen.

Mit der Datenschutzreform bedauerlicherweise nicht gelungen, ist eine Beseitigung der rechtlichen Fragmentierung des Datenschutzes auf Unionsebene: Nicht nur gelten weiterhin separate Regeln für die Organe und Einrichtungen der EU (Verordnung 45/2001), sondern es konnte auch weder eine Integration des Regelungsrahmens für Justiz und Polizei in den allgemeinen Datenschutzrahmen noch eine Vereinheitlichung der zahlreichen sektoriellen Regelungsregime (Schengener-Informationssystem, Europol, Eurojust etc.) erreicht werden. Es ist demzufolge nicht gelungen, den datenschutzrechtlichen Flickenteppich in Europa massgeblich zu vereinfachen.

Die eigentliche Herausforderung für den geschaffenen Rechtsrahmen besteht jedoch in seiner Umsetzung. Gelingt es mit den nun verabschiedeten Rechtsgrundlagen, die beträchtliche Kluft zwischen den datenschutzrechtlichen Aspirationen und der Lebensrealität zu vermindern, so wäre das wohl wichtigste Ziel bereits erreicht. Hierzu stellt ein angepasster und stimmiger rechtlicher Rahmen zwar eine zentrale, aber keine hinreichende Bedingung dar. Erforderlich ist darüber hinaus vielmehr die konkrete Umsetzung, Anwendung und Verfeinerung der geschaffenen Schutzinstrumente, ihre stetige Weiterentwicklung und Anpassung an die gesellschaftlichen Realitäten sowie insbesondere der Wille und das Bestreben sowohl der Behörden als auch der betroffenen Personen, die Einhaltung der geschaffenen rechtlichen Vorgaben konsequent einzufordern.

C. Abkürzungen

ABl.	Amtsblatt der Europäischen Union (bis 1.2.2002: Amtsblatt der Europäischen Gemeinschaften)
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
AJP	Aktuelle Juristische Praxis
Art.	Artikel
Aufl.	Auflage
BBl	Bundesblatt (Schweiz)
BGE	Amtliche Sammlung der Entscheidungen des Schweizerischen Bundesgerichts
bzw.	beziehungsweise
d.h.	das heisst
DuD	Datenschutz und Datensicherheit
DSGV	Datenschutzgrundverordnung (RL 2016/679)
EDPL	European Data Protection Law Review
Erw.	Erwägung
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Gemeinschaften
EUV	Vertrag über die Europäische Union
f./ff.	folgende
Fn.	Fussnote
ggf.	gegebenenfalls
GRCh	Grundrechtecharta der Europäischen Union
Hrsg.	Herausgeber
i.e.S.	im engeren Sinne
i.Erg.	im Ergebnis
i.V.m.	in Verbindung mit
lit.	Litera
m.a.W.	mit anderen Worten
m.w.N.	mit weiteren Nachweisen
Nr.	Nummer
RDV	Recht der Datenverarbeitung
RL	Richtlinie
Rn.	Randnummer
Rs.	Rechtssache
Rspr.	Rechtsprechung
SJZ	Schweizerische Juristen-Zeitung
SR	Systematische Sammlung des Bundesrechts
Uabs.	Unterabsatz
U.K.	United Kingdom
v.	vom/von
VO	Verordnung
VRK	Wiener Übereinkommen über das Recht der Verträge (SR 0.111)
ZD	Zeitschrift für Datenschutz