

Die Datenschutzgrundverordnung: Grundsätze und ausgewählte Aspekte

Astrid Epiney / Nula Frei

Dieser Beitrag wurde erstmals wie folgt veröffentlicht:

Astrid Epiney/Nula Frei, Die Datenschutzgrundverordnung: Grundsätze und ausgewählte Aspekte, in: Astrid Epiney/Sophia Rovelli (Hrsg.), Datenschutzgrundverordnung (DSGVO): Tragweite und erste Erfahrungen / Le Règlement général sur la protection des données (RGDP): portée et premières expériences, Zürich 2020, 1-38.

Es ist möglich, dass diese publizierte Version – die allein zitierfähig ist – im Verhältnis zu diesem Manuskript geringfügige Modifikationen enthält.

Inhaltsübersicht

- A. Einleitung
- B. Zum primärrechtlichen Rahmen: Art. 7, 8 GRCh
- C. Zu den Implikationen für die Schweiz
- D. Zur Datenschutzgrundverordnung
 - I. Zur Rechtsgrundlage
 - II. Zum Instrument der Verordnung
 - III. Aufbau und wesentliche Neuerungen
- E. Schluss

A. Einleitung

Die 2016 erlassene und seit 2018 massgebliche sog. Datenschutzgrundverordnung (VO 2016/679),¹ welche die aus dem Jahr 1995 stammende Datenschutzrichtlinie

¹ VO 2016/679 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, 8. Die Literatur zur Datenschutzgrundverordnung ist mittlerweile kaum noch überschaubar. Hinzuweisen ist darüber hinaus insbesondere auf die (bereits sehr zahlreichen) Kommentare zur Datenschutzgrundverordnung. S. insbesondere *Eugen Ehmann/Martin Selmayr* (Hrsg.), *Datenschutz-Grundverordnung*, München 2018; *Sibylle Gierschmann/Katharina Schlender/Rainer Stentzel/Winfried Veil* (Hrsg.), *Datenschutz-Grundverordnung*, Köln 2018; *Peter Gola* (Hrsg.), *Datenschutz-Grundverordnung VO (EU) 2016/679*, München 2018; *Jürgen Kühling/Benedikt Buchner* (Hrsg.), *Datenschutz-Grundver-*

RL 95/46² ablöste, führte zu einer grundlegenden Revision der für die Mitgliedstaaten der Union massgeblichen datenschutzrechtlichen Vorgaben, und entfaltet darüber hinaus auch Wirkungen für Drittstaaten. Die VO 2016/679 knüpft zwar an die bestehenden Regelungen an, so dass insbesondere auch die bisherige, zur RL 95/46 ergangene Rechtsprechung³ 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, ausgehend von der Bedeutung der Art. 7, 8 GRCh, die anhand der diesbezüglichen Rechtsprechung des EuGH illustriert werden soll (B.), sowie den Implikationen der VO 2016/679 für die Schweiz (C.) einen Überblick über die wesentlichen, mit der VO 2016/679 einhergehenden Neuerungen zu geben, dies unter Hervorhebung einiger ausgewählter Aspekte (D.). Der Beitrag schliesst mit einer kurzen Schlussbemerkung (E.).⁴

B. Zum primärrechtlichen Rahmen: Art. 7, 8 GRCh

In der Union wird der Persönlichkeitsschutz der Betroffenen (nunmehr) in Art. 7, 8 GRCh geregelt: Während Art. 7 GRCh das Recht auf Achtung des Privat- und Familienlebens verankert und insoweit Art. 8 EMRK entspricht, enthält Art. 8

ordnung und Bundesdatenschutzgesetz, München 2018; *Boris Paal/Daniel Pauly* (Hrsg.), *Datenschutz-Grundverordnung/Bundesdatenschutzgesetz*, München 2018; *Kai-Uwe Plath* (Hrsg.), *DSGVO/BDSG*, Köln 2018; *Rolf Schwartmann/Andreas Jaspers/Gregor Thüsing/Dieter Kugelmann* (Hrsg.), *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz*, Heidelberg 2018; *Gernot Sydow* (Hrsg.), *Europäische Datenschutzgrundverordnung*, Baden-Baden 2018.

² RL 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281, 31.

³ S. insbesondere EuGH, Rs. C-518/07 (Kommission/Deutschland), ECLI:EU:C:2010:125; EuGH, Rs. C-614/10 (Kommission/Österreich), ECLI:EU:C:2012:631; EuGH, Rs. C-288/12 (Kommission/Ungarn), ECLI:EU:C:2014:237; EuGH, Rs. C-212/13 (Rynes), ECLI:EU:C:2014:2428; EuGH, Rs. C-293/12 (Digital Rights Ireland), ECLI:EU:C:2014:238; EuGH, Rs. C-131/12 (Google Spain und Google Inc.), ECLI:EU:C:2014:317; EuGH, Rs. C-362/14 (Schrems), ECLI:EU:C:2015:650; EuGH, Rs. C-201/14 (Bara), ECLI:EU:C:2015:638; EuGH, Rs. C-230/14 (Weltimmo), ECLI:EU:C:2015:639; EuGH, Rs. C-191/15 (Verein für Konsumenteninformation/Amazon), ECLI:EU:C:2016:612; EuGH, Rs. C-582/14 (Breyer), ECLI:EU:C:2016:779; EuGH, verb. Rs. C-203/15, C-658/15 (Tele2 Sverige), ECLI:EU:C:2016:970; EuGH, Rs. C-398/15 (Manni), ECLI:EU:C:2017:197; EuGH, Rs. C-13/16 (Rigas satiksme), ECLI:EU:C:2017:336; EuGH, Rs. C-434/16 (Nowak), ECLI:EU:C:2017:994; EuGH, Rs. C-210/16 (Wirtschaftsakademie), ECLI:EU:C:2018:388; EuGH, Rs. C-25/17 (Zeugen Jehovas), ECLI:EU:C:2018:551.

⁴ Dabei greifen die nachfolgenden Ausführungen teilweise auf bereits durchgeführte Untersuchungen zurück, vgl. insbesondere *Astrid Epiney*, *Europäisches Daten- und Persönlichkeitsschutzrecht im Spiegel der Rechtsprechung des EuGH*, FS für Christoph Vedder, Baden-Baden 2017, 89 ff.; *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*, Zürich 2016, 39 ff.

GRCh das Recht auf Schutz personenbezogener Daten. Der Gerichtshof prüft beide Bestimmungen in der Regel zusammen, und seine bisherige Rechtsprechung illustriert die Bedeutung dieser Grundrechte – die bei der Auslegung des Sekundärrechts zu beachten sind – trefflich, wie anhand von folgenden Urteilen, welche staatliche Überwachungsmaßnahmen betreffen, aufgezeigt werden kann.

- In dem von der Grossen Kammer gefällten Urteil in der Rs. C-293/12 (Digital Rights Ireland)⁵ erklärte der EuGH die sog. Vorratsdatenspeicherungs-Richtlinie⁶ für ungültig: Die Richtlinie – die die Mitgliedstaaten dazu verpflichtet, dafür zu sorgen, dass die Anbieter von elektronischen Kommunikationsdiensten die Verkehrs- und Standortdaten (nicht die Inhalte) der erfassten Kommunikation während mindestens sechs und höchstens 24 Monaten „auf Vorrat“ zu speichern haben – greife in den Schutzbereich der Art. 7, 8 GRCh ein, erlaube die Gesamtheit der zu speichernden personenbezogenen Daten doch sehr genaue Rückschlüsse auf das Privatleben der Betroffenen. Allerdings sei der Wesensgehalt dieser Grundrechte nicht angetastet, da die Richtlinie nicht die Kenntnisaufnahme des Inhalts der Kommunikation gestatte und geeignete Massnahmen zum Schutz der Daten gegen zufällige oder unrechtmässige Verluste oder Modifikationen zu ergreifen seien. Der Eingriff – den der Gerichtshof als schwer bezeichnet, gehe es doch um eine stetige Überwachung – könne zwar grundsätzlich durch das Anliegen der Bekämpfung schwerer Kriminalität und damit der öffentlichen Sicherheit gerechtfertigt werden. Jedoch verneinte der Gerichtshof aufgrund einer detaillierten Prüfung die Erforderlichkeit; die Geeignetheit wurde hingegen unproblematisch bejaht, wobei der Gerichtshof hervorhob, hieran ändere auch der Umstand nichts, dass es manche elektronische Kommunikationsweisen gebe, die nicht in den Anwendungsbereich der Richtlinie fallen, da diese jedenfalls einen Beitrag zur Verfolgung des angestrebten Ziels zu leisten vermöge. Bei seiner Prüfung ging der EuGH aufgrund der besonderen Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung des Privatlebens sowie des Ausmasses und der Schwere des mit der RL 2006/24 verbundenen Eingriffs in diese Grundrechte davon aus, dass der Gestaltungsspielraum des Unionsgesetzgebers eingeschränkt sei, so dass die Richtlinie einer strikten Kontrolle unterliege. Unter Rückgriff auf die einschlägige Rechtsprechung des EGMR betonte der Gerichtshof sodann, dass ein solch schwerwiegender Eingriff in die Rechte der Art. 7, 8 GRCh präzise Regeln für die Tragweite und die Anwendung der fraglichen Massnahme vorsehen und Mindestanforderungen aufstellen müsse, so dass die Betroffenen über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen, Anforderungen, die im Rahmen automatisierter Verarbeitungen umso bedeutender seien. Diese Vorgaben erfülle die RL 2006/24 nicht, da sich ihr Anwendungsbereich generell auf alle Personen und alle elektronischen Kommunikationsmittel sowie sämtliche Verkehrsdaten erstreckte, ohne dass irgendeine Differenzierung, Einschränkung oder

⁵ EuGH, Rs. C-293/12 (Digital Rights Ireland), ECLI:EU:C:2014:238.

⁶ RL 2006/24/EG über die Vorratsspeicherung von Daten, ABl. 2006 L 105/54.

Ausnahme in Abhängigkeit von dem Ziel der Kriminalitätsbekämpfung vorgesehen sei. Auch sehe die Richtlinie kein objektives Kriterium vor, das den Zugang der zuständigen nationalen Behörden zu den Daten einschränke, und sie enthalte auch sonst keine materiell- oder verfahrensrechtlichen Voraussetzungen für den Zugang dieser Behörden zu den Daten. Sodann dürfe die Speicherfrist zwischen sechs und 24 Monaten liegen, ohne dass objektive Kriterien formuliert werden, die eine Differenzierung etwa in Abhängigkeit von den Datenkategorien zu gewährleisten vermögen. Schliesslich seien auch die Vorgaben in Bezug auf die Datensicherheit nicht hinreichend klar und präzise, zumal sie nicht im Unionsgebiet zu speichern seien, was jedoch aufgrund der Überwachung auf der Grundlage des Unionsrechts notwendig sei.

Das Urteil überzeugt im Ergebnis und in der Begründung; bemerkenswert ist insbesondere die sehr differenzierte und argumentativ ausführliche Verhältnismässigkeitsprüfung. Gewünscht hätte man sich jedoch – auch wenn man dem Gerichtshof hier ebenfalls zustimmen mag – eine etwas ausführlichere Stellungnahme zu der Frage, auf welche Weise denn methodisch ermittelt werden soll, unter welchen Voraussetzungen der „Wesensgehalt“ eines Grundrechts angetastet ist, was nach Art. 52 Abs. 1 GRCh keinesfalls zulässig ist. Man wird aus den insofern etwas ergebnisorientierten Formulierungen des Gerichtshofs schliessen können, dass die durch das jeweilige Grundrecht eingeräumten Rechte jedenfalls nicht vollumfänglich „ausgehebelt“ werden dürfen; aber auch auf dieser Grundlage bleiben selbstverständlich beachtliche Unschärfen, wenn auch Vieles dafür spricht, dass jedenfalls in den Fällen, in denen in Bezug auf einen nicht näher eingegrenzten Personenkreis auf Kommunikationsinhalte zurückgegriffen werden kann, der Kerngehalt berührt ist.⁷ Ebenfalls auslegungsbedürftig sind Aussage und Begründung in Bezug auf die Feststellung, die Grundrechtskonformität der Richtlinie unterliege einer strikten gerichtlichen Kontrolle, so dass der ansonsten häufig eingeräumte Gestaltungsspielraum des Gesetzgebers entsprechend eingeschränkt ist: Zwar vermag diese Aussage im Ergebnis im konkreten Fall durchaus zu überzeugen; fraglich ist jedoch, unter welchen Voraussetzungen denn jeweils eine solche strikte Kontrolle durchzuführen ist. Der Gerichtshof stellt hier auf die Bedeutung der in Frage stehenden Grundrechte sowie die Schwere des Eingriffs ab; aufgeworfen wird damit die Frage, ob diese Kriterien kumulativ zu verstehen sind (wofür die Formulierung des Gerichtshofs sprechen dürfte), wobei aber die besondere Bedeutung eines Grundrechts wohl auch für sich allein ein Kriterium für eine zumindest etwas strengere Prüfung darstellen könnte. Daran anschliessend fragt es sich, welche Grundrechte denn von besonderer Bedeutung sind; vieles könnte hier dafür sprechen, an ihren Bezug zur in Art. 1 GRC garantierten Menschenwürde anzuknüpfen. Schliesslich ist darauf hinzuweisen, dass der Gerichtshof, wenn er an mehreren Stellen die fehlende Präzision gewisser Regelungen moniert, offenbar davon ausgeht, dass die Richtlinie selbst bereits so ausgestaltet sein muss, dass sie den Anforderungen an die Schranken für den Grundrechtseingriff entspricht; es soll also nicht genügen, dass sie es den Mitgliedstaaten nicht verwehrt, die Richtlinie so umzusetzen,

⁷ In diesem Sinne dann auch die nachfolgende Rechtsprechung; vgl. EuGH, Rs. C-362/14 (Schrems), ECLI:EU:C:2015:650.

dass die EU-Grundrechte – die bei der Umsetzung von Richtlinien unbestritten-erweise zu beachten sind – nicht verletzt werden. Dieser Ansatz steht in einem gewissen Gegensatz zu anderen Urteilen des Gerichtshofs, in denen er darauf hinweist, ein Verstoss gegen die EU-Grundrechte könne deshalb nicht festgestellt werden, weil der Sekundärrechtsakt einen Gestaltungsspielraum lasse und die Mitgliedstaaten diesen dann eben so zu nutzen hätten, dass die EU-Grundrechte beachtet werden;⁸ es war schon immer unklar, warum dann nicht gleich das Sekundärrecht so formuliert werden muss, zumal derartige Spielräume eine gewisse Rechtsunsicherheit mit sich bringen und es nicht klar ist, warum Gestaltungsspielräume so ausgestaltet werden, dass eine Verletzung von Grundrechten möglich ist. Insofern ist der in dem angezeigten Urteil vertretene Ansatz sehr zu begrüßen, wobei zu hoffen ist, dass er sich nicht nur auf die Fälle „strikt“ Kontrolle durch den Gerichtshof beschränkt.

- Auch in der Rs. C-203/15 (Tele2 Sverige)⁹ ging es um die Vorratsdatenspeicherung, dies jedoch in Bezug auf eine mitgliedstaatliche Vorschrift. Im Anschluss an sein Urteil in der Rs. C-293/12 hielt der Gerichtshof fest, es stehe nicht mit Art. 15 Abs. 1 RL 2002/58 (Datenschutzrichtlinie im Bereich der elektronischen Kommunikation¹⁰) in Einklang, zum Zweck der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorzusehen. Denn eine solche Massnahme genüge nicht den Anforderungen der Verhältnismässigkeit, wobei der Gerichtshof auf seine Erwägungen in der Rs. C-293/12 zur RL 2006/24 zurückgreift (da die in Frage stehende nationale Regelung im Wesentlichen derjenigen entspreche, die in der RL 2006/24 verankert war); letztlich war somit auch hier die „Pauschalität“ der Pflicht zur Vorratsdatenspeicherung entscheidend. Ebenso wenig sei es mit Art. 15 Abs. 1 RL 2002/58 vereinbar, wenn der Zugang der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten nicht ausschliesslich auf die Zwecke der Bekämpfung schwerer Straftaten beschränkt wird, der Zugang keiner vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird und nicht gewährleistet ist, dass die betreffenden Daten im Gebiet der Union auf Vorrat zu speichern sind. Dabei seien bei der Regelung des Zugangs der zuständigen nationalen Behörden zu den auf Vorrat gespeicherten Daten nicht nur die in Art. 15 Abs. 1 RL 2002/58 genannten Zwecke zu beachten, sondern es seien auch materiell- und verfahrensrechtliche Voraussetzungen bezüglich dieses Zugangs zu regeln, womit ein allgemeiner Zugang gerade nicht in Einklang stehe.

Der Gerichtshof legt Art. 15 Abs. 1 RL 2002/58 im Lichte der Art. 7, 8, 52 I GRCh aus und nimmt eine ausführliche Prüfung der Grundrechtskonformität der in Frage stehenden nationalen Massnahmen vor. Dabei hebt er auch hervor, dass eine Pflicht zur Vorratsdatenspeicherung zur Bekämpfung schwerer Straftaten zulässig sein könne, wenn sie hinsichtlich der Kategorien der zu speichernden Daten, der erfassten elektronischen Kommunikationsmittel, der betroffenen Personen und der vorgesehenen Dauer der Vorratsdatenspeicherung auf das absolut

⁸ Vgl. EuGH, Rs. C-540/03 (Parlament/Rat), ECLI:EU:C:2006:429.

⁹ EuGH, verb. Rs. C-203/15, C-658/15 (Tele2 Sverige), ECLI:EU:C:2016:970.

¹⁰ ABl. 2002 L 201, 37.

Notwendige beschränkt ist; dabei wird durchaus ein gewisser Spielraum eingeräumt, so wenn auf die Objektivität der Kriterien (die auch ein bestimmtes geographisches Gebiet betreffen können) hingewiesen wird.

- In der Rs. C-362/14 (Schrems)¹¹ hielt der Gerichtshof insbesondere fest, auch im Falle der Übermittlung von Daten in einen Drittstaat sei ein hohes Schutzniveau zu gewährleisten, das zwar nicht identisch mit demjenigen der RL 95/46 sein müsse, jedoch einen gleichwertigen Schutz bieten müsse. Jeder andere Ansatz verkenne die Zielsetzung der RL 95/46 und führe zu zahlreichen Umgehungsmöglichkeiten. Im Übrigen müsse es – wie sich aus dem Wortlaut der RL 95/46 ergebe – 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 könnten, 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 sei, 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 entsprechende *Safe Harbor*-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, Art. 8 GRC noch sei der Grundsatz der Verhältnismässigkeit gewahrt, und im Übrigen verletze eine

¹¹ EuGH, Rs. C-362/14 (Schrems), ECLI:EU:C:2015:650.

Regelung, die es gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des Art. 7 GRC.

Der Gerichtshof geht damit in überzeugender Weise davon aus, dass die jeweilige innerstaatliche Rechtsordnung das angemessene Schutzniveau gewährleisten muss, an das übrigens eher hohe Anforderungen gestellt werden. Das Erfordernis der effektiven Einhaltung auch in der Praxis dürfte im Übrigen nicht immer einfach zu erfüllen sein; man wird hier wohl auf gewisse Plausibilitätserwägungen zurückgreifen dürfen. Sodann impliziert der Ansatz des Gerichtshofs, dass eine Regelung, die es Behörden generell gestattet, auf die Inhalte elektronischer Kommunikation zurückzugreifen, den Wesensgehalt des Art. 7 GRC beeinträchtigt, die Unzulässigkeit solcher Vorschriften, so dass der entsprechende Grundrechtseingriff damit auch nicht rechtfertigungsfähig ist.¹²

- In der Rs. C-207/16 (Ministerio Fiscal)¹³ betonte der Gerichtshof im Zusammenhang mit der Auslegung des eine Beschränkung der Persönlichkeitsrechte ermöglichenden Art. 15 Abs. 1 RL 2002/58 (Datenschutzrichtlinie im Bereich der elektronischen Kommunikation), die Verpflichtung, öffentlichen Stellen Zugang zu Daten zu gewähren, anhand derer die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt wurden (wie Name, Vorname und ggf. Adresse der Karteninhaber), stelle zwar einen Eingriff in Art. 7, 8 GRCh dar; dieser lediglich der Ermittlung der Identität dienende Eingriff wiege aber nicht so schwer, dass er nur zur Bekämpfung schwerer Kriminalität zulässig wäre. Im Umkehrschluss – was der Gerichtshof auch ausdrücklich betont – können schwere Eingriffe nur durch die Bekämpfung schwerer Kriminalität gerechtfertigt werden, wobei in Bezug auf die Telekommunikation ein solcher schwerer Eingriff jedenfalls dann vorliege, wenn die Daten Schlüsse auf das Privatleben der Betroffenen erlauben, was wohl bei einem «umfassenden» Zugang zu Daten im Zusammenhang mit dem Mobiltelefon (neben Kommunikationsinhalten vermutlich auch schon die Ortung) zu bejahen ist.
- In dem auf Antrag des Europäischen Parlaments erstellten Gutachten 1/15¹⁴ ging es um das geplante Abkommen zwischen Kanada und der EU über die Übermittlung und Verarbeitung von Fluggastdatensätzen. Der Schwerpunkt des Gutachtens – das daneben noch einige, hier nicht näher zu erörternde

¹² Inzwischen hat die Union mit den Vereinigten Staaten ein neues Abkommen ausgehandelt, das Datenübermittlungen in die USA erlaubt (sog. „Privacy Shield“), vgl. hierzu *Kai von Lewinski*, Privacy Shield – Notdeich nach dem Pearl Harbor für die transatlantischen Datentransfers, EuR 2016, 405 ff.; *Stefan Weiss*, Nach dem Ende von Safe Harbor: Das EU-U.S.-Privacy Shield, RDV 2016, 135 ff, wobei fraglich ist, ob dieses einer wohl zu erwartenden gerichtlichen Überprüfung durch den EuGH standhalten wird, sind die vom Gerichtshof formulierten Anforderungen doch sehr streng ausgestaltet (was übrigens nicht mit Blick auf eine angebliche Extraterritorialität kritisiert werden kann, geht es doch um eine Datenverarbeitung in der Union, nämlich die Übermittlung in Drittstaaten).

¹³ EuGH, Rs. C-207/16 (Ministerio Fiscal), ECLI:EU:C:2018:788.

¹⁴ Gutachten 1/15 vom 26.7.2017, ECLI:EU:C:2017:592 (Große Kammer). Zu diesem Gutachten z.B. *Elspeth Guild/Elif Mednos Kuskonmaz*, EU Exclusive Jurisdiction on Surveillance Related to Terrorism and Serious Transnational Crime: Case Review on Opinion 1/15, ELR 2018, 583 ff.; *Olivia Tambou*, Opinion 1/15 on the EU-Canada Passenger Name Record (PNR) Agreement: PNR Agreements Need to Be Compatible with EU Fundamental Rights, European Foreign Affairs Review 2018, 187 ff.

Fragen der Zulässigkeit des Antrags sowie der Rechtsgrundlage thematisierte – lag auf der Vereinbarkeit des geplanten Abkommens mit Art. 7, 8 und 21 GRCh. Die in dem Abkommen vorgesehene Übermittlung von Fluggastdatensätzen (die recht umfangreiche Informationen über die Fluggäste beinhalten) an die zuständige kanadische Behörde sowie deren Speicherung und Verwendung (unter Einschluss der Weiterleitung an andere Behörden in Kanada, in der EU oder in Drittstaaten) stelle einen Eingriff in Art. 7, 8 GRCh dar. Dieser könne grundsätzlich gerechtfertigt werden, dies allerdings nicht durch die Einwilligung der Fluggäste (hätten diese ihre Daten doch lediglich mit Blick auf die Abwicklung ihrer Flugreise bekanntgegeben), sondern durch das Abkommen selbst, das eine gesetzliche Grundlage im Sinne der Art. 8 II und 52 I GRCh darstelle. Auch würden im Allgemeinwohl liegende Ziele verfolgt, denn die vorgesehene Datenverarbeitung diene der öffentlichen Sicherheit (Bekämpfung terroristischer Aktivitäten und schwerer grenzüberschreitender Kriminalität). Der Wesensgehalt der Art. 7, 8 GRCh sei nicht betroffen, da nur gewisse Aspekte des Privatlebens erfasst würden und die Datenverarbeitung nur zur bestimmten, im Abkommen umschriebenen Zwecken erfolgen dürfe und zudem Regelungen zur Sicherheit, Vertraulichkeit und Integrität der Daten vorgesehen seien. Allerdings lasse es das geplante Abkommen auch zu, dass sensible Daten (die im Abkommen definiert sind und z.B. die rassische oder ethnische Herkunft, die Religion oder das Sexualleben erfassen) übermittelt und verwendet werden. Eine Massnahme, die auf der Annahme beruht, dass eines dieser sensiblen Merkmale unabhängig vom konkreten Verhalten des Betroffenen für das Ziel des Schutzes der öffentlichen Sicherheit relevant sein könnte, verstosse jedoch gegen Art. 7, 8, 21 GRCh (andere Rechtfertigungsgründe seien vorliegend nicht ersichtlich). Daher sei insoweit ein Verstoß gegen die genannten Vorgaben der GRCh anzunehmen. Weiter sei der Umfang der zu übermittelnden Daten teilweise nicht hinreichend bestimmt. Schliesslich formuliert der Gerichtshof eine Reihe von Voraussetzungen, denen das Abkommen Rechnung tragen müsse, damit die Übermittlung von Fluggastdatensätzen mit Art. 7, 8 GRCh vereinbar sei, so u.a. in Bezug auf die Präzision der zu übermittelnden Daten, die automatisierte Verarbeitung, die verfahrensrechtlichen Gewährleistungen, die Speicherung der Daten nach der Ausreise (die nur bei Anhaltspunkten, dass von den Betroffenen eine Gefahr ausgeht, zulässig sei), die Weitergabe an Empfänger in Drittstaaten (hinreichendes Datenschutzniveau), die Information der Betroffenen und der Einbezug einer unabhängigen Kontrollstelle.

Insgesamt nimmt der EuGH in seiner Rechtsprechung zu Art. 7, 8 GRCh eine sehr detaillierte Grundrechtsprüfung vor und prüft im Einzelnen insbesondere die Verhältnismässigkeit, dies mit einer hohen Prüfungsdichte, wobei er zahlreiche, eher detaillierte Vorgaben für den Unionsgesetzgeber formuliert. Versucht man aus der Gesamtheit der in diesem Beitrag besprochenen jüngeren Urteile des Gerichtshofs ein kurzes Fazit zu ziehen bzw. über die jeweils konkret aufgeworfenen Fragen hinausgehende Grundsätze zu formulieren, so scheinen folgende Aspekte von besonderer Bedeutung zu sein:

- Grundsätzlich wird im Rahmen der Prüfung der Vereinbarkeit von Unionsrechtsakten mit Art. 7, 8 GRC eine sehr hohe Kontrolldichte angelegt. Dem Gestaltungsspielraum des Unionsgesetzgebers werden auf diese Weise entsprechend enge Grenzen gesteckt.
- Der Gerichtshof wendet die allgemeinen datenschutzrechtlichen Grundsätze sowie die grundrechtlichen Vorgaben konsequent auch auf Fallgestaltungen an, bei denen dies auf gewisse Schwierigkeiten stösst (wie im Rahmen der Datenverarbeitung im Internet) und macht sie auf diese Weise auch für eher neue Fragestellungen fruchtbar. Dass es hier mitunter in der Rechtsdurchsetzung zu Problemen kommen kann, ist nicht zu verkennen, jedoch *per se* kein Grund, das Recht nicht anzuwenden; im Gegenteil: Möglicherweise ist das Schutzbedürfnis der Betroffenen hier gerade besonders gross.
- Von besonderer Bedeutung ist auch der in der gesamten Rechtsprechung zum Ausdruck kommende sehr hohe Stellenwert, der dem Grundrechtsschutz eingeräumt wird. Dies impliziert auch, dass der grundrechtlich garantierte Persönlichkeitsschutz der Verfolgung durchaus legitimer öffentlicher oder privater Interessen Grenzen setzt, so dass diese „nicht um jeden Preis“ verfolgt werden dürfen. Insofern wohnt den Grundrechten ein gewisser „Absolutheitsanspruch“ inne, was übrigens nicht nur für die Gewährleistung des Kerngehalts der Grundrechte, sondern auch für die übrigen Anforderungen gilt.
- Die Bestimmung des Kerngehalts der Art. 7, 8 GRCh im Zusammenhang mit der Verarbeitung von Personendaten ist noch nicht abschliessend geklärt. Die Rechtsprechung legt den Schluss nahe, dass jedenfalls in den Fällen, in denen in Bezug auf einen nicht näher eingegrenzten Personenkreis auf Kommunikationsinhalte zurückgegriffen werden kann, der Kerngehalt berührt ist. Auch dürfte der Wesensgehalt der Art. 7, 8 GRCh immer dann betroffen sein, wenn umfassend (fast) alle Aspekte des Privatlebens betroffen sind und die Nutzung ohne eine präzise Umschreibung des Zwecks erfolgen darf. Sodann dürfte im Ergebnis ebenfalls der Kerngehalt der Art. 7, 8 GRCh i.V.m. Art. 21 GRCh betroffen sein, wenn es um die Verarbeitung besonders sensibler Daten (wie z.B. Rasse oder Religion) geht und die Annahme zugrunde gelegt wird, dass ein solches Merkmal unabhängig von konkreten Anhaltspunkten im Verhalten des Betroffenen für die öffentliche Sicherheit relevant sein könnte.
- Gleichzeitig ist nicht zu verkennen, dass auch die datenschutz- bzw. grundrechtlichen Vorgaben eine Verfolgung wichtiger (insbesondere öffentlicher) Interessen keineswegs verunmöglichen. Nur sind in diesem Zusammenhang eben die anhand der Rechtsprechung des EuGH erörterten Vorgaben bzw. Schranken zu beachten. Freilich schränken diese die Gestaltungsfreiheit des Gesetzgebers ein und führen möglicherweise zu einer gewissen „Ineffizienz“. Diese ist aber der Preis für ein rechtsstaatliches System, dessen Grundprinzipien auch und gerade bei der Verfolgung bedeutender öffentlicher Interessen Sorge zu tragen ist.

Es lohnt sich u.E., diese Zusammenhänge immer wieder in Erinnerung zu rufen: Denn mitunter schlägt im Zuge emotionaler Diskussionen aufgrund bestimmter aktueller Ereignisse das Pendel in der politischen und manchmal auch rechtlichen

Diskussion über Sinn und Unsinn von Datenschutz ohne nähere Reflexion der einschlägigen Rechtsprinzipien – die immerhin ein Kernelement jeden rechtsstaatlichen Gemeinwesens bilden – in die eine oder andere Richtung aus.

C. Zu den Implikationen für die Schweiz

Die Schweiz ist über die sog. Schengen- und Dublinassoziiierung¹⁵ auch an datenschutzrechtliche Vorgaben des EU-Rechts gebunden,¹⁶ dies soweit diese Teil des sog. Schengen- und Dublin-Besitzstands und in den Anhängen der Abkommen entsprechend vermerkt sind, wobei hier in Bezug auf die genaue Reichweite dieser Einbindung der Schweiz in den unionsrechtlichen Besitzstand nach wie vor noch einiges streitig ist.¹⁷ Sowohl die RL 95/46 als auch der Rahmenbeschluss 2008/977 figurieren in den Anhängen. 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 Mechanismen¹⁸ nach der Übernahme der neuen Rechtsakte in die Anhänge der genannten

¹⁵ 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.

¹⁶ 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.

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

¹⁸ 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.

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 zum Datenschutz in der Strafverfolgung (RL 2016/680)¹⁹, nicht jedoch die Datenschutzgrundverordnung: Interessanterweise fehlt in dieser 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. Dies und der Umstand, dass sich im Rahmen von „Schengen“ und „Dublin“ zahlreiche datenschutzrechtliche Fragen stellen, sprechen – im Gegensatz zur Ansicht des Unionsgesetzgebers – dafür, 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 gegen die Datenschutzgrundverordnung (Art. 263 AEUV) wäre hier zwar grundsätzlich denkbar gewesen; die Klagfrist ist aber abgelaufen. 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 – mit Ausnahme der Bereiche, in denen die RL 2016/680 anwendbar ist – die RL 95/46 massgeblich sein wird, während in den EU-Mitgliedstaaten die Datenschutzgrundverordnung gilt, ein Ergebnis, das in einem gewissen Spannungsverhältnis zur Zielsetzung der Schengen- und Dublinasoziiierung, 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 vier 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 muss das Datenschutzrecht von Bund und Kantonen zur Erlangung eines sog. «Angemessenheitsbeschlusses» gemäss Art. 45 DSGVO mit der DSGVO wirkungsgleich sein, womit zwar keine wortgetreue Übernahme

¹⁹ RL 2016/680 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, ABl. 2016 L 119, 89. Diese wurde inzwischen auch in der Schweiz umgesetzt. Vgl. hierzu *Beat Rudin*, Datenschutzreform in der Schweiz, digma 2018, 194 ff.

der Bestimmungen der Verordnung notwendig ist, aber doch ein im Endergebnis gleichwertiges Schutzniveau; eine Vorgabe, die insbesondere im Rahmen der Revision des Datenschutzgesetzes zu beachten ist.²⁰

- Drittens sind in der Schweiz tätige Unternehmen und teilweise auch Behörden aufgrund des weiten Anwendungsbereichs der Datenschutzgrundverordnung insofern betroffen, als sie sich bei Vorliegen der noch zu erörternden Voraussetzungen²¹ 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, da gewisse Aspekte auch im Rahmen der Revision der Datenschutzkonvention des Europarates – die nach ihren erklärten Zielsetzungen inhaltlich mit den Entwicklungen auf EU-Ebene abgestimmt werden sollte²² – 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. Diesfalls wären im Ergebnis auch die Datenschutzgrundverordnung (bzw. Teile derselben) sowie die zu ihr ergehende Rechtsprechung für die Anwendung resp. Umsetzung der revidierten Datenschutzkonvention des Europarates in der Schweiz relevant,²³ 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).²⁴

Nur am Rande sei zudem in diesem Zusammenhang darauf hingewiesen, dass auch die erörterte Rechtsprechung des EuGH zu Art. 7, 8 GRCh durchaus auf dieser Grundlage für die Schweiz relevant sein kann: Es ist nämlich davon auszugehen, dass diese Rechtsprechung auch im Rahmen der Auslegung des Art. 8 EMRK von Bedeutung ist. Denn Art. 7 GRCh knüpft an Art. 8 EMRK

²⁰ Vgl. hierzu, m.w.N., *Nula Frei*, Die Datenschutz-Grundverordnung und die Schweiz, in: Astrid Epiney/Déborah Sangsue (Hrsg.), *Datenschutz und Gesundheitsrecht*, 2019, 79 ff. (83).

²¹ S.u. D.III.1.

²² 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.; *Jean-Philippe Walter*, La révision de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) et les répercussions pour la Suisse, in: Astrid Epiney/Daniela Nüesch (Hrsg.), *Die Revision des Datenschutzes in Europa und die Schweiz*, Zürich 2016, 77 ff.

²³ S. hierzu *Nula Frei*, Die Datenschutz-Grundverordnung und die Schweiz (Fn. 20), 84.

²⁴ 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.).

an, und gemäss Art. 52 Abs. 3 GRCh haben die Rechte der Charta, die den durch die EMRK garantierten Rechten entsprechen, die gleiche Bedeutung und Tragweite, wie ihnen im Rahmen der EMRK zukommt, wobei ein weitergehender Schutz ausdrücklich vorbehalten wird.

D. Zur Datenschutzgrundverordnung

Die Datenschutzgrundverordnung (DGVO bzw. VO 2016/679) wurde nach einem ausgesprochen langen und insbesondere komplexen Gesetzgebungsverfahren erlassen, innerhalb desselben diverse Stellungnahmen, Entwürfe und Vorschläge eingebracht wurden, wodurch einerseits die Komplexität der Thematik, andererseits die durchaus auseinandergehenden (politischen und rechtlichen) Einschätzungen illustriert werden.²⁵ Die Bedeutung der VO 2016/679 erschliesst sich – ausgehend von einem kurzen Hinweis auf die Rechtsgrundlage (I.) – durch die Wahl des Instruments der Verordnung (II.), bevor auf die wesentlichen Inhalte hingewiesen werden soll (III.).

Deutlich wird damit auch, dass im Folgenden keine Vollständigkeit angestrebt wird, sprengte dies doch angesichts der insgesamt 99 Artikel der Verordnung mit rund 90 Seiten im Amtsblatt (die RL 95/46 umfasst im Amtsblatt 20 Seiten) den Rahmen des vorliegenden Beitrags. So erfolgt eine Beschränkung auf einige, nach Ansicht der Autorinnen 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.

I. Zur Rechtsgrundlage

Die Datenschutzgrundverordnung wurde auf Art. 16 Abs. 2 AEUV gestützt.²⁶ Diese Bestimmung sieht den Erlass von 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 gemäss dem ordentlichen Gesetzgebungsverfahren vor. Die Datenverarbeitung durch die Mitgliedstaaten darf nur insoweit erfasst werden, als sie die Ausübung von Tätigkeiten betrifft, die in den Anwendungsbereich des Unionsrechts fallen. Bemerkenswert ist, dass in dieser Bestimmung die Datenverarbeitung durch Private nicht erwähnt wird.

Auf den ersten Blick erscheint der Anwendungsbereich dieser Rechtsgrundlage somit durchaus beschränkt. Im Ergebnis dürfen datenschutzrechtliche Fragen aber auch für die Mitgliedstaaten umfassend geregelt werden: Denn der freie Datenverkehr darf – auch soweit die Mitgliedstaaten betroffen sind, wobei darüber hinaus hierdurch auch durch Private erfolgende Datenverarbeitungen erfasst sind – umfas-

²⁵ Vgl. zur Entstehungsgeschichte, auf die vorliegend nicht weiter eingegangen wird, 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.

²⁶ Allgemein zum primärrechtlichen Rahmen *Stephan Pötters*, Primärrechtliche Vorgaben für eine Reform des Datenschutzrechts, RDV 2015, 10 ff.

send geregelt werden. Da aber der freie Datenverkehr bzw. die grenzüberschreitende Datenübermittlung in engem Zusammenhang 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 einhergehen könnten. 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.²⁷

Illustriert wurde der Zusammenhang des freien Datenverkehrs mit dem Datenschutzniveau in den Mitgliedstaaten – wenn auch in Bezug auf das Verhältnis zu den Vereinigten Staaten – durch das bereits erwähnte Urteil des Gerichtshofs in Bezug auf die sog. *Safe Harbor*-Regelung:²⁸ 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.²⁹

Deutlich wird damit der Zusammenhang zwischen einem angemessenen Datenschutzniveau in einem Staat und der Zulässigkeit einer grenzüberschreitenden Datenübermittlung bzw. dem freien

²⁷ I.Erg. ebenso *Thorsten Kingreen*, in: Christian Calliess/Matthias Ruffert (Hrsg.), EUV/AEUV, Kommentar, 5. Aufl., München 2016, 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.

²⁸ 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.

²⁹ Vgl. im Einzelnen zu diesem Urteil *Epiney/Kern*, in: Revision des Datenschutzes (Fn. 4), 39 (42 f.); s. auch schon oben B.

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 nicht zulässig ist.³⁰ 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 Verwaltung³¹ oder die Verarbeitung öffentlicher Daten durch öffentliche Stellen für die Anwendung aufenthaltsrechtlicher Vorschriften und statistische Zwecke.³²

II. Zum Instrument der Verordnung

Der Unionsgesetzgeber griff bei der Revision der datenschutzrechtlichen Vorgaben nicht mehr auf das Instrument der Richtlinie, sondern auf dasjenige der Verordnung zurück. 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 oder eine solche zumindest sachdienlich sein kann. Denn Verordnungen können Vorgaben sehr unterschiedlicher Art enthalten, so – neben direkt anwendbaren Bestimmungen – auch solche, die es den Mitgliedstaaten aufgeben bzw. erlauben, bestimmte Massnahmen zu ergreifen.³³ Ein Beispiel in der Datenschutzgrundverordnung ist die in Art. 51 ff. DSGVO enthaltene Verpflichtung der Mitgliedstaaten, eine oder mehrere unabhängige nationale Aufsichtsbehörden vorzusehen, denen bestimmte Befugnisse zukommen müssen.

³⁰ EuGH, verb. Rs. C-468/10, C-469/10 (ASNEF), ECLI:EU:C:2011:777, Rn. 30; aus der Literatur, m.w.N., Pötters, RDV 2015 (Fn. 26), 10 (11 f.).

³¹ EuGH, verb. Rs. C-465/00, C-138/01, C-139/01 (Österreichischer Rundfunk), ECLI:EU:C:2003:294.

³² EuGH, Rs. C-542/06 (Huber), ECLI:EU:C:2008:724.

³³ Zur Zulässigkeit solcher Bestimmungen auch in Verordnungen z.B. EuGH, Rs. C-403/98 (Azienda Agricola Monte Arcosu), ECLI:EU:C:2001:6, Rn. 26; zur Zulässigkeit bzw. Notwendigkeit mitgliedstaatlicher Durchführungsmassnahmen z.B. EuGH, Rs. C-541/16 (Kommission/Dänemark), ECLI:EU:C:2018:251.

Der Hintergrund für die Wahl der Verordnung als Instrument (an Stelle der Richtlinie) ist nach den Erwägungsgründen der Verordnung³⁴ in erster Linie darin zu sehen, dass mit der Verordnung eine weitergehende Harmonisierung erreicht werden kann, da die notwendigerweise mit der mitgliedstaatlichen Umsetzung 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 Bereichen ausgesprochen weite (Umsetzungs-) Spielräume einräumt (insbesondere durch die teilweise sehr offenen Formulierungen sowie die in gewissen Bereichen weitgehenden Ausnahme- bzw. Abweichungsmöglichkeiten),³⁵ eine ungleich grössere Rolle spielen.

In diesem Sinn dürfte denn auch in Bezug auf die mit der VO 2016/679 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. Nicht zu verkennen ist freilich, dass auch die VO 2016/679 insofern im Ergebnis eine weniger weitgehende Harmonisierung mit sich bringt als dies auf den ersten Blick den Anschein erwecken mag, als sie zahlreiche sog. Öffnungsklauseln kennt, die es den Mitgliedstaaten erlauben, in bestimmten Bereichen bzw. in Bezug auf gewisse Fragen die Vorgaben der Verordnung zu konkretisieren, zu spezifizieren, zu ergänzen oder / und zu verschärfen.³⁶ Insofern lohnt sich dann jeweils immer doch ein Blick auf die nationale Durchführungsgesetzgebung. Nur am Rande sei dabei bemerkt, dass sich damit im Datenschutzrecht die Frage, ob und inwieweit die Mitgliedstaaten Verordnungsbestimmungen im nationalen Recht aufnehmen dürfen, mit besonderer Relevanz stellt. Denn der in den 70er Jahren formulierte Grundsatz des «Verbots» der Wiederholung von Verordnungsbestimmungen im nationalen Recht³⁷ kann in dieser Form an sich nicht (mehr) angewandt werden, können solche Wiederholungen doch mitunter notwendig sein, damit die nationalen Durchführungsbestimmungen verständlich sind.

In Bezug auf die Reichweite der Harmonisierungswirkung der VO 2016/679 ergibt sich schon aus ihrer Zielsetzung, (auch) den freien Datenverkehr sicherzustellen, dass die Vorgaben der Verordnung grundsätzlich abschliessend zu verstehen sind, so dass die Mitgliedstaaten auch keine strengeren Schutzmassnahmen ergreifen dürfen. Allerdings enthalten verschiedene Bestimmungen der Verordnung – wie soeben erwähnt – die Harmonisierungswirkung der Richtlinie relativierende „Erlaubnisvorbehalte“, wonach es den Mitgliedstaaten offen steht, in der betreffen-

³⁴ S. insbesondere Erw. 9 f. DGVO.

³⁵ 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.

³⁶ Vgl. hierzu *Friederike Detmering/Andreas Splittgerber*, DSGVO und nationale Umsetzungsgesetze, digma 2018, 172 ff., die insgesamt rund 70 Öffnungsklauseln zählen.

³⁷ S. insbesondere EuGH, Rs. 34/73 (Variola), ECLI:EU:C:1973:101.

den Frage und im vorgesehenen Ausmass ggf. auch ein erhöhtes Schutzniveau anzulegen bzw. dieses zu spezifizieren. Beispielhaft erwähnt seien das Einwilligungsalter bei Kindern, Datenschutz im Zusammenhang mit Arbeitsverhältnissen oder gewisse Aspekte der Meldepflicht bei Datenschutzverletzungen sowie zusätzliche Sanktionen.

Die Relevanz bzw. die Bedeutung des abschliessenden Charakters der Verordnung – welcher bereits für die RL 95/46 galt – kann durch die Rs. C-582/14³⁸ illustriert werden. Der Gerichtshof hielt hier zunächst fest, dass auch eine dynamische IP-Adresse ein personenbezogenes Datum darstelle, dies soweit der Nutzer anhand von Zusatzinformationen bestimmbar sei und diese Informationen aus tatsächlicher und rechtlicher Sicht zugänglich seien. Art. 7 RL 95/46 sehe eine erschöpfende und abschliessende Liste derjenigen Fälle vor, in denen eine Verarbeitung personenbezogener Daten als rechtmässig anzusehen sei, so dass die Mitgliedstaaten weder neue bzw. weitere Zulässigkeitsgründe einführen dürften noch zusätzliche Bedingungen stellen dürften, welche die Tragweite einer der in dieser Bestimmung enthaltenen Grundsätze modifizieren würde.³⁹ Daher sei es nicht mit der RL 95/46 vereinbar, wenn ein Anbieter von Online-Mediendiensten ohne Einwilligung des Nutzers dessen personenbezogene Daten nur verarbeiten dürfe, um die Inanspruchnahme der Dienstleistungen zu ermöglichen und die Abrechnung sicherzustellen (mit der Folge, dass z.B. eine Verarbeitung zur Gewährleistung der generellen Funktionsfähigkeit eines Online-Mediendienstes nicht zulässig wäre), stehe Art. 7 lit. f RL 95/46 doch einer mitgliedstaatlichen Regelung entgegen, die kategorisch und ganz allgemein die Verarbeitung bestimmter personenbezogener Daten ausschliesse, ohne eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu ermöglichen, so dass ein Mitgliedstaat das Ergebnis der Abwägung dieser Rechte und Interessen nicht abschliessend vorschreiben dürfe, ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfalle.

Im Verhältnis zum nationalen Recht kommt der VO 2016/679 aufgrund der allgemeinen Prinzipien des Verhältnisses von Unionsrecht und nationalem Recht Vorrang vor mitgliedstaatlichem Recht zu, so dass das nationale Recht soweit wie möglich unionsrechtskonform auszulegen ist; ist eine solche unionsrechtskonforme Auslegung nicht möglich, sind die nationalen Vorschriften nicht anzuwenden.⁴⁰

III. Aufbau und wesentliche Neuerungen

Die Datenschutzgrundverordnung knüpft in verschiedener Hinsicht – insbesondere soweit die Ziele und Grundsätze betroffen sind – an die RL 95/46 an und nimmt deren Vorgaben auf, wenn auch gelegentlich mit Präzisierungen.⁴¹ Gleichzeitig bringt sie einige, durchaus bedeutende und ins Gewicht fallende Neuerungen mit sich, auf die nachfolgend der Akzent gelegt werden wird. Bemerkenswert ist, dass auch die neue Verordnung auf dem Konzept der „Technikneutralität“ beruht, so dass keine spezifisch technischen Fragen für bestimmte Datenverarbeitungen, die

³⁸ EuGH, Rs. C-582/14 (Breyer), ECLI:EU:C:2016:779.

³⁹ S. insoweit auch schon EuGH, verb. Rs. C-468/10, C-469/10 (ASNEF), ECLI:EU:C:2011:777

⁴⁰ Zu diesen allgemeinen Grundsätzen aus der jüngeren Rechtsprechung z.B. EuGH, verb. Rs. C-569/16, C-570/16 (Bauer), ECLI:EU:C:2018:871; EuGH, Rs. C-684/16 (Shimizu), ECLI:EU:C:2018:874; EuGH, Rs. C-619/16 (Kreuziger), ECLI:EU:C:2018:872.

⁴¹ S. insoweit auch Erw. 9 VO 2016/679.

auf gewisse Techniken zurückgreifen, sondern allgemein geltende datenschutzrechtliche Anforderungen formuliert werden, wenn auch einigen Vorgaben gerade im Internetzeitalter besondere Bedeutung zukommt.⁴²

Im Einzelnen erschliessen sich die wesentlich Neuerungen der Datenschutzgrundverordnung durch folgende Aspekte: Anwendungsbereich (1.), Rechte der 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 in verschiedener Hinsicht im Verhältnis zu den Vorgaben der RL 95/46 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 Durchführungsrechtsakte (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 trat, jedoch erst zwei Jahre danach tatsächlich Geltung erlangte (Art. 99 DSGVO).

⁴² Hierzu etwa *Gernot Sydow/Markus Kring*, Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug. Konkurrierende Leitbilder für den europäischen Rechtsrahmen, ZD 2014, 271 ff.

Die Begriffsdefinitionen der RL 95/46 waren gelegentlich Gegenstand von Urteilen des EuGH, die auch im Rahmen der Datenschutzgrundverordnung weiter von Bedeutung sind. Hingewiesen sei auf zwei Urteile des Gerichtshofs:

- In der Rs. C-210/16⁴³ fasste der Gerichtshof den Begriff des für eine Datenverarbeitung Verantwortlichen unter Hinweis auf das Ziel der Richtlinie, durch dessen weite Definition einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten, eher weit und subsumierte darunter nicht nur das Unternehmen, welches ein soziales Netzwerk betreibt (wie Facebook), sondern auch den Betreiber einer Fanpage. Denn der Betreiber einer auf Facebook unterhaltenen Fanpage erlaube es Facebook durch die Einrichtung einer solchen Seite, auf den Computer oder jedes andere Gerät, der Person, die seine Fanpage besucht hat, Cookies zu platzieren, unabhängig davon ob diese Person über ein Facebook-Konto verfügt; mit Hilfe von durch Facebook zur Verfügung gestellten Filtern könne der Betreiber auch die Kriterien festlegen, nach denen Statistiken erstellt werden sollen, und sogar die Personenkategorien bezeichnen, deren personenbezogene Daten von Facebook ausgewertet werden. Damit trage der Betreiber zur Verarbeitung der personenbezogenen Daten der Besucher seiner Seite bei und sei somit auch als Verantwortlicher für die Datenverarbeitung im Sinne der RL 95/46 anzusehen. Die hieraus folgende gemeinsame Verantwortlichkeit führe im Übrigen nicht zwangsläufig zu einer gleichwertigen Verantwortlichkeit der verschiedenen Akteure für die Verarbeitung, sondern der Grad der Verantwortlichkeit eines jeden von ihnen sei unter Berücksichtigung aller Umstände des Einzelfalls zu beurteilen. Weiter legte der Gerichtshof die Befugnisse der Kontrollstellen gegenüber einem ausserhalb der Union angesiedelten Unternehmen, welches in mehreren Mitgliedstaaten Niederlassungen betreibt (wie Facebook), extensiv aus: Die Kontrollstellen seien jedenfalls dann zuständig, wenn eine in «ihrem» Staat angesiedelte Niederlassung allein für den Verkauf von Werbeflächen und sonstige Marketingtätigkeiten in diesem Staat zuständig ist. Denn in einer solchen Konstellation erfolge die Verarbeitung der personenbezogenen Daten «im Rahmen der Tätigkeit der Niederlassung» (wie von Art. 4 RL 95/46 vorausgesetzt), woran auch der Umstand, dass die ausschliessliche Verantwortung für die Verarbeitung personenbezogener Daten für das gesamte Unionsgebiet einer in einem anderen Mitgliedstaat gelegenen Niederlassung obliegt, nichts ändert. In einem solchen Fall sei dann auch das nationale Datenschutzrecht anwendbar und folgerichtig dürften die Kontrollstellen ihre Einwirkungsbefugnisse gegenüber einer in «ihrem» Staat ansässigen Stelle auch dann ausüben, wenn es um Verstösse gegen datenschutzrechtliche Vorgaben durch Dritte geht, der seinen Sitz in einem anderen Mitgliedstaat hat, und dies, ohne zuvor die Kontrollstelle dieses anderen Mitgliedstaates um ein Eingreifen zu ersuchen, wobei der Gerichtshof insbesondere auf die Unabhängigkeit der Kontrollstellen hinweist. Das Urteil impliziert – wie nunmehr Art. 26 DSGVO auch ausdrücklich festhält – die Möglichkeit einer «gemeinsamen Verantwortlichkeit». Diese erscheint bei Fanseiten auf Facebook in der Tat überzeugend, wobei wohl schon das Vorliegen einer der drei vom Gerichtshof angeführten Gründe (Möglichkeit der Sammlung von Cookies durch Facebook, Bestimmung der Datenauswertung von Facebook durch die Festlegung von Kriterien und die Möglichkeit, von Facebook Statistiken zu verlangen) für die Bejahung der Verantwortlichkeit ausreichend wäre. Unklar bleibt jedoch nach dem Urteil, welche Pflichten genau für jeden der gemeinsam Verantwortlichen sich aus dieser Verantwortlichkeit ergeben, denn der Gerichtshof geht ausdrücklich nicht von einer in jedem Fall gleichwertigen Verantwortlichkeit der verschiedenen Akteure aus. Jedenfalls dürfte aber eine umfassende Informationspflicht aller Beteiligten anzunehmen sein. Die Zuständigkeit der (vorliegend deutschen) Datenschutzbehörde würde unter Art. 58 DSGVO nunmehr wohl anders beurteilt, ist doch gemäss dieser Bestimmung und dem Konzept des «one stop shop» diejenige Datenschutzbehörde federführend, in der sich die Hauptniederlassung befindet. Der Gefahr widersprüchlicher Entscheidungen verschiedener nationaler Kontrollbehörden durch die extensive Auslegung der alleinigen Befugnisse der jeweiligen nationalen Behörde kann zumindest weitgehend durch

⁴³ EuGH, Rs. C-210/16 (Wirtschaftsakademie), ECLI:EU:C:2018:388.

das nunmehr in Art. 60 ff. DSGVO vorgesehene Kooperationssystem begegnet werden. Bemerkenswert ist jedenfalls, dass es auch unter dem Regime der DSGVO durchaus relevant bleiben wird, welches nationale Recht anwendbar ist, da die Verordnung den Mitgliedstaaten zahlreiche Durchführungsspielräume eröffnet.

- In der Rs. C-25/17⁴⁴ hatte sich der EuGH mit Grundfragen der Datenverarbeitung einer Religionsgemeinschaft, hier der Zeugen Jehovas, zu befassen und hielt dreierlei fest: Erstens falle die Verarbeitung von Personendaten, die im Rahmen der Verkündigungstätigkeit von «Tür zu Tür» durch Mitglieder der Religionsgemeinschaft erhoben werden, in den Anwendungsbereich der RL 95/46, da die Ausnahmen des Art. 3 Abs. 2 RL 95/46 (welche eng auszulegen seien) nicht zum Zuge kämen. Es gehe hier um die religiöse Betätigung von Privaten, so dass keine spezifische Tätigkeit staatlicher Stellen vorliege, womit Art. 3 Abs. 2 erster Spiegelstrich RL 95/46 nicht einschlägig sei. Die Ausnahme der Verarbeitung von Daten ausschliesslich für die Ausübung persönlicher und familiärer Tätigkeiten sei ebenfalls nicht einschlägig, da die in Frage stehende Datenverarbeitung wesensgemäss den Zweck habe, den Glauben der Gemeinschaft unter Personen zu verbreiten, die gerade nicht zum Haushalt der verkündigenden Mitglieder gehören, so dass sie auf einen Bericht ausserhalb der Privatsphäre dieser Personen gerichtet sei. Weiter werde zumindest ein Teil der Daten an die Gemeinden der Gemeinschaft weitergegeben, so dass sie einem potentiell unbegrenzten Personenkreis zugänglich gemacht würden. An der somit gegebenen Anwendbarkeit der RL 95/46 ändere auch der Umstand, dass die Verkündigungstätigkeit als solche von der Religionsfreiheit (Art. 10 I GRCh) geschützt ist, nichts. Dem ist in jeder Beziehung zuzustimmen, denn die Religionsfreiheit befreit nicht «automatisch» von der Verpflichtung zur Beachtung von allgemein geltenden Rechtspflichten. Art. 91 DSGVO sieht im Übrigen (inzwischen) eine gewisse Privilegierung von Kirchen und religiösen Gemeinschaften (unter bestimmten Voraussetzungen) vor, woraus sich im Umkehrschluss die Eröffnung des Anwendungsbereichs der Verordnung für deren Datenverarbeitung ergibt. Zweitens liege eine «Datei» im Sinn des Art. 2 lit. c RL 95/46 (wobei die nunmehr massgebliche Definition in Art. 4 Nr. 6 DSGVO im Wesentlichen inhaltsgleich ist) auch dann vor, wenn die Daten strukturiert sind, so dass sie «leicht wiederauffindbar» sind; die Erstellung spezifischer Kartotheken oder Verzeichnisse oder anderer der Recherche dienender Ordnungssysteme sei nicht notwendig. Damit reicht eine minimale Strukturierung (z.B. nach Alphabet oder Wohnort) der Personendaten aus, so dass kaum eine manuelle Datenverarbeitung denkbar ist, die hier nicht erfasst ist, zumal das entscheidende Kriterium offenbar die leichte Auffindbarkeit ist. Diese sehr weite Auslegung des Anwendungsbereichs der Richtlinie (die auch im Rahmen der DSGVO zum Zuge kommt) ist vor dem Hintergrund des effektiven Schutzes der Grundrechte auf Privatheit und Datenschutz (Art. 7, 8 GRCh) zu sehen.

Und drittens seien als Verantwortliche für die Datenverarbeitung nicht nur die Verkündigungstätigkeit von Tür zu Tür durchführenden Mitglieder der Religionsgemeinschaft, sondern auch die Gemeinschaft selbst anzusehen, sofern sie diese Tätigkeit und die damit verbundene Datenverarbeitung organisiert und koordiniert und die Datenverarbeitung somit in ihrem Interesse erfolgt, ohne dass es erforderlich wäre, dass sie selbst Zugriff auf die Daten hat oder ihren Mitgliedern schriftliche Anweisungen oder Anleitungen zu den Verarbeitungen gegeben hat. Dieser Ansatz impliziert, dass bereits eine (mehr oder weniger direkte) Einflussnahme auf die Datenverarbeitung dazu führt, dass eine Verantwortlichkeit im Sinne der RL 95/46 anzunehmen ist. Letztlich ist also wohl ausschlaggebend, dass eine Stelle die Datenverarbeitung in einer Weise beeinflussen kann, dass das Risiko der Beeinträchtigung der Persönlichkeitsrechte erhöht wird; ein Ansatz, der auch in der Rs. C-210/16 zugrunde gelegt wurde.

⁴⁴ EuGH, Rs. C-25/17 (Zeugen Jehovas), ECLI:EU:C:2018:551.

1. Anwendungsbereich

Während der persönliche Anwendungsbereich – insbesondere in Bezug auf die Betroffenen – keine wirklichen Modifikationen erfährt und auch in Bezug auf den sachlichen Anwendungsbereich an die bisherigen Regelungen angeknüpft wird,⁴⁵ wird der räumliche Anwendungsbereich im Verhältnis zur bisherigen Regelung beträchtlich ausgedehnt. Im Einzelnen unterscheidet der hier einschlägige Art. 3 DSGVO zwischen drei Konstellationen:

- Nach Art. 3 Abs. 1 DSGVO findet die Verordnung auf die Verarbeitung personenbezogener Daten Anwendung, soweit diese „im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt“,⁴⁶ 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,⁴⁷ so dass es wohl nicht auf den juristischen „Hauptsitz“ ankommt, wie sich im Gegenschluss aus der Begriffsdefinition der „Hauptniederlassung“ in Art. 4 Nr. 16 DSGVO ergibt, geht diese Definition doch davon aus, dass es neben der Hauptniederlassung auch sonstige Niederlassungen geben muss. Andererseits muss die Verarbeitung aber im Rahmen der Tätigkeit dieser Niederlassung erfolgen, wobei es ausreichend ist, dass die Verarbeitung im Zusammenhang mit einer effektiven und tatsächlichen Tätigkeit der Niederlassung steht, wobei die Tätigkeit der Niederlassung nur geringfügig sein kann und auch der Zusammenhang zwischen der Verarbeitung und der Tätigkeit eher lose ausfallen kann.

Die eher geringen Anforderungen in diesem Kontext 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)⁴⁸ 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

⁴⁵ So findet die Verordnung auf die Verarbeitung personenbezogener Daten Anwendung, wobei diese nach der Begriffsdefinition in Art. 4 Nr. 1 DSGVO nur auf natürliche Personen bezogen 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. 4), Rn. 19 ff., womit jedoch keine wirklichen Modifikationen im Vergleich zur geltenden Rechtslage einhergehen.

⁴⁶ Vgl. die Definitionen der Begriffe „Verantwortlicher“ und „Auftragsverarbeiter“ in Art. 4 Nr. 7, 8 DSGVO.

⁴⁷ 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.

⁴⁸ EuGH, Rs. C-131/12 (Google Spain und Google Inc.), ECLI:EU:C:2014:317.

Tätigkeiten der Niederlassung von Google in Spanien ausgeübt, so dass der räumliche Anwendungsbereich der RL 95/46 betroffen sei. Denn die Niederlassung in dem betreffenden Mitgliedstaat sei für die Förderung des Verkaufs der angebotenen Werbeflächen der Suchmaschine zuständig, 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 – 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)⁴⁹ 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 95/46⁵⁰ (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, dies 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 Zielsetzungen 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. Hinzuweisen ist aber auch darauf, dass auf der Grundlage des Urteils davon auszugehen ist, dass zahlreiche Unternehmen neben dem Datenschutzrecht ihres Gesellschaftssitzes auch diejenigen einer Vielzahl weiterer Mitgliedstaaten zu beachten haben, in denen sie Niederlassungen im Sinne des Urteils betreiben. Dies hat sich zwar mit dem Inkrafttreten der Datenschutzgrundverordnung etwas abgemildert, da diese unmittelbar anwendbares Recht schafft; die zahlreichen Öffnungsklauseln machen eine Berücksichtigung der nationalen Datenschutzgesetzgebung dennoch weiterhin notwendig. Die Grundsätze des Gerichtshofs

⁴⁹ EuGH, Rs. C-230/14 (Weltimmo/Nemzeti), ECLI:EU:C:2015:639.

⁵⁰ 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.

bleiben jedenfalls in Bezug auf ausserhalb der Union ansässige Unternehmen weiterhin relevant.

- Die eigentliche Neuerung der Datenschutzgrundverordnung findet sich in Art. 3 Abs. 2 DSGVO:⁵¹ 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 Datenverarbeiters oder des Auftragsverarbeiters in der Union ist in dieser Konstellation nicht notwendig.⁵² 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 Verarbeitungsvorgänge mit sich, die vollumfänglich ausserhalb des Hoheitsgebiets der Union bzw. ihrer Mitgliedstaaten stattfinden, 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.⁵³ 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 der Datenschutzgrundverordnung – 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 DSGVO nicht immer einfach sein wird und sich hier durchaus Abgrenzungsfragen stellen werden.

So fragt es sich, unter welchen Voraussetzungen davon ausgegangen werden kann, dass Waren oder Dienstleistungen in der Union angeboten werden im

⁵¹ Hierzu spezifisch (neben den einschlägigen Kommentaren, s. Fn. 1) *Philip Uecker*, Extraterritorialer Anwendungsbereich der DS-GVO. Erläuterungen zu den neuen Regelungen und Ausblick auf internationale Entwicklungen, ZD 2019, 67 ff.

⁵² Teilweise wird hier auch vom „Marktortprinzip“ gesprochen, vgl. *Benedikt Buchner*, Grundsätze und Rechtmässigkeit der Datenverarbeitung unter der DS-GVO, DuD 2016, 156.

⁵³ 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 Arnould*, Völkerrecht, 2. Aufl., 2014, Rn. 342 ff.

Sinne von Art. 3 Abs. 2 lit. a) DSGVO: 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.⁵⁴ Fordern wird man daher objektiv erkennbare und zielgerichtete Aktivitäten in diesem Sinn, etwa durch die Verwendung der entsprechenden Sprache oder von Werbung auf dem Gebiet der Union,⁵⁵ ohne dass es jedoch auf eine eigentliche „subjektive“ Absicht ankäme.⁵⁶ Entscheidend wird hier eine Gesamtwürdigung der Umstände des Einzelfalls sein, womit aber auch gewisse Unklarheiten einhergehen können (so z.B. in Bezug auf die Frage, ob auch die Kundenpflege aus dem EU-Ausland erfasst ist, was wohl zu bejahen ist⁵⁷). Ebenso dürfte die Frage, ob eine Beobachtung betroffener Personen im Hoheitsgebiet der Union i.S.v. Art. 3 Abs. 2 lit. b) DSGVO vorliegt, anhand aller Umstände des Einzelfalls zu beurteilen sein, wobei hier in aller Regel jedoch eine subjektive Absicht vorliegen muss, 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 hier 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.⁵⁸

- Zweitens wird die Rechtsdurchsetzung häufig problematisch sein, erlaubt es das Völkerrecht doch grundsätzlich nicht, entsprechende Massnahmen im Hoheitsgebiet anderer Staaten zu ergreifen, so dass die mitgliedstaatlichen Datenschutzbehörden hier auf Massnahmen im eigenen Hoheitsgebiet beschränkt sind, die jedoch in aller Regel wenig effektiv sein werden, fehlt es doch an einer Niederlassung; zudem können Durchsetzungsmassnahmen, wie etwa Sanktionen, jedenfalls nach vorherrschender Ansicht, nicht stellvertretend an den gemäss Art. 27 DSGVO zu ernennenden Vertreter in der Union adressiert werden.⁵⁹ Soweit öffentliche Stellen betroffen sind, kommen die

⁵⁴ S. insoweit auch EuGH, verb. Rs. C-585/08, C-144/09 (Pammer), ECLI:EU:C:2010:740, Rn. 75.

⁵⁵ S. zu einzelnen, hier relevanten Elementen *Passadelis/Roth*, Jusletter v. 4.4.2016 (Fn. 21), Rn. 14.

⁵⁶ S. insoweit auch Erw. 23 DSGVO, wobei hier teilweise etwas missverständlich formuliert wird, so wenn auf ein „offensichtliches Beabsichtigen“ Bezug genommen wird.

⁵⁷ Hierzu, allerdings a.A., *David Rosenthal/David Vasella*, Erste Erfahrungen mit der DSGVO, *digma* 2018, 166 (169 f.).

⁵⁸ 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.

⁵⁹ S. hierzu, m.w.N., *Jürgen Hartung*, in: Kühling/Benedikt Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG Kommentar, 2. Aufl., München 2018, Art. 27 DSGVO, Rn. 20 ff.; *Nikolaus Bertermann*, in: Eugen Ehmann/Martin Selmayr (Hrsg.), DS-GVO Kommentar, 2. Aufl., München 2018, Art. 27 DSGVO, Rn. 14.

völkerrechtlichen Immunitätsregeln zur Anwendung, die einer eigentlichen Rechtsdurchsetzung in aller Regel entgegenstehen werden.

- Schliesslich findet die Verordnung auch Anwendung – und 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 DSGVO 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.⁶⁰ 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 Verkehr personenbezogener Daten, so dass grundsätzlich einmal jede Datenverarbeitung (potentiell) betroffen ist.

Ebenso wie Art. 3 Abs. 2 RL 95/46 findet die Datenschutzgrundverordnung nach Art. 2 Abs. 2 lit. c) VO 2016/679 (u.a.) keine Anwendung auf Datenverarbeitungen, die von einer natürlichen Person zur Ausübung ausschliesslich persönlicher oder familiärer Tätigkeiten vorgenommen wird. Die Reichweite dieses Ausnahmetatbestands ist sehr beschränkt, wie die Rechtsprechung des EuGH verdeutlicht: In der Rs. C-212/13⁶¹ stand die Reichweite dieses Ausnahmetatbestands in Frage, dies im Zusammenhang mit dem Betrieb einer Überwachungskamera, die auch den öffentlichen Raum vor dem durch die Kamera „bewachten“ Haus abdeckte. Nach der wenig überraschenden Feststellung, dass das von einer Kamera aufgezeichnete Bild einer Person als ein personenbezogenes Datum im Sinne der Richtlinie anzusehen sei, schloss der Gerichtshof auf die Nichteinschlägigkeit der Ausnahmebestimmung des Art. 3 Abs. 2 RL 95/46: Denn diese sei schon deshalb eng auszulegen, weil die RL 95/46 letztlich auf die effektive Verwirklichung der in Art. 7, Art. 8 GRC garantierten Rechte abziele, ganz abgesehen davon, dass auch der Wortlaut des Art. 3 Abs. 2 RL 95/46, der von Datenverarbeitungen, die „ausschliesslich“ im Rahmen persönlicher oder familiärer Tätigkeiten vorgenommen werden, spreche, in diese Richtung gehe. Auf dieser Grundlage müsse die Datenverarbeitung ausschliesslich die persönliche oder familiäre Sphäre betreffen, was bei einer Videoüberwachung, die auch öffentlichen Raum umfasst, eben gerade nicht gegeben sei.

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.

⁶⁰ S. schon EuGH, Rs. C-101/01 (Lindqvist), ECLI:EU:2003:596; s. sodann EuGH, Rs. C-524/06 (Huber), ECLI:EU:C:2008:724; EuGH, verb. Rs. C-465/00, C-138/01, C-139/01 (Österreichischer Rundfunk), ECLI:EU:C:2003:294. Hierzu auch bereits oben B.I.

⁶¹ EuGH, Rs. C-212/13 (Rynes), ECLI:EU:C:2014:2428.

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 Vorgaben zur Einwilligung finden sich systematisch in Kapitel II der Verordnung, welches die Grundsätze der Datenverarbeitung enthält. Diese Grundsätze (Art. 5 ff. DSGVO) werden – mit einigen stilistischen, inhaltlich aber nicht ins Gewicht fallenden Anpassungen – weitgehend in Anlehnung an die RL 95/46 formuliert. Mitunter werden einige neue (aber nicht durchgehend überzeugende) Begriffe eingeführt.

So nimmt z.B. Art. 5 Abs. 1 lit. c) DSGVO 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 DSGVO hinzuweisen, der im Kontext der Rechtmässigkeit der Datenverarbeitung spezifische Vorgaben für Art. 6 Abs. 2 lit. c) (Erfüllung einer rechtlichen Verpflichtung) und e) (Wahrnehmung einer Aufgabe im öffentlichen Interesse) DSGVO 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 DSGVO 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 eine recht weitgehende Relativierung des Zweckbindungsgrundsatzes implizieren dürfte.⁶²

Gewisse Modifikationen sind jedoch in Bezug auf die an die Einwilligung in eine Datenbearbeitung zu stellenden Anforderungen zu verzeichnen, wobei die Einwilligung eine der zentralen Rechtfertigungsgründe für eine Datenbearbeitung bleibt,⁶³ dies trotz der damit verbundenen Problematik, die dazu führt, dass es sich hier oft um eine Fiktion handelt.⁶⁴

- Zunächst wird die Begriffsdefinition in Art. 4 Nr. 11 DSGVO 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. Somit erfordert eine rechtsgültige Einwilligung die vier Elemente Freiwilligkeit, Bestimmtheit,

⁶² Zum Problemkreis etwa *Maximilian von Grafenstein*, Das Zweckbindungsprinzip zwischen Innovationsoffenheit und Rechtssicherheit, DuD 2015, 789 ff.

⁶³ Zu den Anforderungen an die Einwilligung neben den einschlägigen Kommentaren (Fn. 1) *Marie-Theres Tinnefeld/Isabell Conrad*, Die selbstbestimmte Einwilligung im europäischen Recht. Voraussetzungen und Probleme, ZD 2018, 391 ff.; *Stefan Ernst*, Die Einwilligung nach der Datenschutzgrundverordnung. Anmerkungen zur Definition nach Art. 4 Nr. 11 D-GVO, ZD 2017, 110 ff.

⁶⁴ 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.; *Winfried Veil*, Die Datenschutz-Grundverordnung: des Kaisers neue Kleider, NVwZ 2018, 686 (688).

Informiertheit und Unmissverständlichkeit. 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.⁶⁵ Der Wortlaut des Art. 4 Nr. 11 DSGVO („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.⁶⁶ Für diesen Ansatz kann auch der Zusammenhang mit der ebenfalls in Art. 4 Nr. 11 DSGVO 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 DSGVO trägt der für die Verarbeitung Verantwortliche die Beweislast für das Vorliegen einer Einwilligung.
- Art. 7 Abs. 2 DSGVO 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. Dabei besteht ein enger Zusammenhang zu den Informations- und Transparenzpflichten nach Art. 12, 13 und 14 DSGVO; eine Verletzung dieser Pflichten – an die entsprechend dem risikobasierten Ansatz der Verordnung umso höhere Anforderungen bezüglich Klarheit und Verständlichkeit gesetzt werden, je höher die mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten der betroffenen Personen sind – wird in der Regel auch zur Unwirksamkeit einer gestützt darauf erteilten Einwilligung führen.
- Die betroffene Person kann ihre Einwilligung jederzeit widerrufen, Art. 7 Abs. 3 DSGVO, wobei der Widerruf so einfach wie die Einwilligung selbst sein muss.
- Sodann ist nach Art. 7 Abs. 4 DSGVO 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, wobei im Sinne einer widerlegbaren Vermutung bei einer Koppelung zunächst vom Fehlen einer Einwilligung ausgegangen werden dürfte, sofern nicht im Einzelfall Umstände vorliegen, die für eine Freiwilligkeit sprechen.⁶⁷
- Art. 8 DSGVO enthält spezifische Anforderungen an die Einwilligung von Kindern; namentlich sind Einwilligungen von Kindern unter 16 Jahren in

⁶⁵ So offenbar *Weber*, Jusletter IT v. 24.9.2015 (Fn. 4), Rn. 30, dies allerdings auf der Grundlage des leicht anders formulierten Entwurfs der Verordnung.

⁶⁶ In diese Richtung auch die Schlussanträge des Generalanwalts in der Rs. C-673/17 (*Planet49*) vom 21.3.2019, Rn. 89, der die Ansicht vertritt, dass bereits vorangekreuzte Kästchen (opt-out) mit der Voraussetzung der Eindeutigkeit der Einwilligung nicht vereinbar sind.

⁶⁷ S. hierzu *Dirk Heckmann/Anne Paschke*, in: Eugen Ehmann/Martin Selmayr (Hrsg.), *DS-GVO Kommentar*, 2. Aufl., München 2018, Art. 7 DSGVO, Rn. 98.

Dienste der Informationsgesellschaft nur durch ihre Erziehungsberechtigten möglich, wobei die Mitgliedstaaten dieses Alter auf 13 herabsetzen können.⁶⁸

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 dem „traditionellen“ Ansatz bei der Einwilligung insofern, als diese nach wie vor einen allgemeinen Rechtfertigungsgrund darstellt, dessen Anwendungsbereich nicht wirklich eingeschränkt wird, so dass die mit der Einwilligung teilweise verbundenen Fiktionen, die Problematik der Freiwilligkeit und der hinreichenden Informiertheit nicht wirklich adressiert werden.⁶⁹ Ob Art. 7 Abs. 4 DSGVO daran etwas ändern wird – schliesslich geht es dort hauptsächlich um eine Berücksichtigungspflicht – bleibt abzuwarten. Verzichtet wurde insbesondere darauf, die Einwilligung als Rechtfertigungsgrund in gewissen Fallgestaltungen – z.B. bei einem erheblichen „Machtgefälle“ zwischen Datenverarbeiter und Betroffenen – auszuschliessen. Hinzuweisen ist allerdings darauf, dass es Art. 88 DSGVO 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.⁷⁰

b) Informations- und Transparenzpflichten

Die Informations- und Transparenzpflichten werden in der Datenschutzgrundverordnung wesentlich ausgebaut, was angesichts der hier häufig herrschenden Intransparenz sehr zu begrüssen ist: So werden die zu übermittelnden Informationen in Art. 13 Abs. 1, 2, 14 Abs. 1, 2 DSGVO in sehr detaillierter Weise umschrieben, wobei – insofern wie bereits in Art. 10, 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, 14 Abs. 4 DSGVO), eine Bestimmung, welche die Relativierung des Zweckbindungsgrundsatzes⁷¹ bestätigt.

Hingewiesen sei in diesem Zusammenhang auf die Rs. C-201/14,⁷² in der es um die Übermittlung von Angaben über die Einkünfte von Selbständigen durch die Steuerverwaltung an die Nationale Kasse der Krankenversicherungen ging, mit der Folge, dass von den Selbständigen rückständige Krankenversicherungsbeiträge eingefordert wurden. Der Gerichtshof erachtete diese Datenübermittlung als nicht mit der RL 95/46 in Einklang stehend: Denn die Verpflichtung, Daten nach Treu und Glauben zu verarbeiten, impliziere eine Pflicht der Verwaltungsbehörde, die Betroffenen

⁶⁸ 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.

⁶⁹ Gerade im Internet und im Zusammenhang mit Big Data stellt sich zudem die Frage, ob eine hinreichende Information erfolgt bzw. möglich ist.

⁷⁰ Hierzu, wenn auch nicht ganz klar, *Tim Wybitul/Stephan Pötters*, Der neue Datenschutz am Arbeitsplatz, RDV 2016, 10 (13).

⁷¹ Dazu oben D.III.2.a).

⁷² EuGH, Rs. C-201/14 (Bara u.a.), ECLI:EU:C:2015:638.

davon zu unterrichten, dass die personenbezogenen Daten an eine andere Verwaltungsbehörde weitergeleitet werden, um von dieser in ihrer Eigenschaft als deren Empfänger verarbeitet zu werden; eine solche Unterrichtung habe im Ausgangsfall offenbar nicht stattgefunden. Zudem seien die sich aus Art. 11 RL 95/46 ergebenden Informationspflichten nicht eingehalten worden. Art. 13 RL 95/46 (der gewisse Ausnahmen von den Verpflichtungen der Richtlinie vorsieht) könne schon deshalb nicht zum Zuge kommen, weil die betreffende Übermittlung nicht durch Rechtsvorschriften vorgesehen war. Nicht ganz klar wird aus dem Urteil, ob bereits allein die Verletzung der Informationspflicht aus Art. 10, Art. 11 RL 95/46/EG quasi „automatisch“ einen Verstoss gegen Treu und Glauben und damit die Rechtswidrigkeit der Verarbeitung nach sich zieht. Da eine Information dann nicht zu erfolgen hat, wenn eine Verarbeitung gesetzlich vorgesehen ist und geeignete Garantien bestehen, spricht Vieles für die Bejahung dieser Frage.

c) Ansprüche der Betroffenen

Die Datenschutzgrundverordnung verankert (insbesondere) zwei neue Rechte der betroffenen Personen:

- Art. 17 DSGVO 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, falls die Rechtmässigkeit der Datenverarbeitung nicht mehr gegeben ist, wobei die entsprechenden Konstellationen in Art. 17 Abs. 1 DSGVO im Einzelnen aufgeführt werden. Art. 17 Abs. 3 DSGVO enthält einige Ausnahmetatbestände (u.a. die Erforderlichkeit der entsprechenden Daten im Hinblick auf das Recht auf freie Meinungsäusserung und Information), wobei 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 Vergessen“ zu erwähnen).⁷³

Erinnert sei hier an das Urteil in der Rs. C-131/12,⁷⁴ in dem der Gerichtshof u.a.⁷⁵ zur rechtlichen Tragweite der Art. 12 lit. b, 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, 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

⁷³ Zur Problematik eines „Rechts auf Vergessen“ instruktiv auch *Gabriele Buchholtz*, Das „Recht auf Vergessen“ im Internet. Vorschläge für ein neues Schutzkonzept, ZD 2015, 570 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.

⁷⁴ EuGH, Rs. C-131/12 (Google Spain und Google Inc.), ECLI:EU:C:2014:317.

⁷⁵ Zu den Aussagen des Gerichtshofs zum Anwendungsbereich der RL 95/46 bereits oben B.III.1.

sowohl gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers als auch dem Interesse der breiten Öffentlichkeit am Zugang zu solchen Informationen überwogen, 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.

Bemerkenswert ist immerhin Art. 17 Abs. 2, der eine Pflicht des Verantwortlichen vorsieht, sofern er die personenbezogenen Daten öffentlich gemacht hat, allfällige weitere Verantwortliche, die diese Daten verarbeiten, über das Löschungsbegehren zu informieren, dies jedenfalls unter Berücksichtigung der verfügbaren Technologie und der Implementierungskosten. Hervorzuheben ist somit, dass Art. 17 DSGVO im Vergleich zur RL 95/46 eine wesentlich detailliertere Regelung enthält. Wenig glücklich erscheint jedoch der Begriff des „Rechts auf Vergessenwerden“, da er insinuiert, 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 noch offenbar 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.

- Ein wahres Novum findet sich in Art. 20 DSGVO, wonach die betroffene Person das Recht hat, 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, dies soweit die Verarbeitung auf bestimmten Rechtfertigungsgründen (insbesondere einer Einwilligung oder einem Vertrag) beruht und die Verarbeitung mittels automatisierter Verfahren erfolgt.⁷⁶ Dieses neue Recht, das auch eine wettbewerbsrechtliche Komponente hat, 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 ändern.

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 folgende Aspekte: *Privacy by design* und *Privacy by default* (a),⁷⁷ Aufzeichnungs-

⁷⁶ Zu diesem Recht, neben den einschlägigen Kommentaren (Fn. 1), *Kirsten Benedikt*, Datenportabilität – das neue Recht des Betroffenen, RDV 2017, 189 ff.

⁷⁷ Hierzu, neben den einschlägigen Kommentaren (Fn. 1), *Felix Bieker/Marit Hansen*, Datenschutz „by Design“ und „by Default“ nach der neuen europäischen Datenschutz-Grundverordnung, RDV 2017, 165 ff.

pflichten (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.⁷⁸

Eigene Regeln werden auch im Hinblick auf die Förderung von Verhaltensregeln und die Zertifizierung formuliert (Art. 40-43 DSGVO), wobei es hier jedoch im Wesentlichen um Förderpflichten unterschiedlicher Reichweite geht.⁷⁹

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, 24 VO 2016/679), was häufig mit dem Begriff der *Accountability* umschrieben wird.

a) *Privacy by design und Privacy by default*

Art. 25 DSGVO 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 (so etwa im Bereich der Datenminimierung oder der Datensicherheit) 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.⁸⁰ 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 DSGVO immer schon dann zum Tragen kommt, wenn aufgrund der Umstände des Einzelfalls damit gerechnet werden muss, dass

⁷⁸ Vgl. zu diesen Regelungen Passadelis/Roth, Jusletter v. 4.4.2016 (Fn. 21), Rn. 46 ff.; Thomas Petri, Auftragsdatenverarbeitung – heute und morgen. Reformüberlegungen zur Neuordnung des Europäischen Datenschutzrechts, ZD 2015, 305 ff. Zur Anwendbarkeit der Datenschutzgrundverordnung bei grenzüberschreitender Auftragsverarbeitung siehe Nula Frei, Die Datenschutz-Grundverordnung und die Schweiz (Fn. 20), 88 ff.

⁷⁹ Spezifisch zur Zertifizierung Sebastian Kraska, Datenschutz-Zertifizierung in der EU-Datenschutzgrundverordnung, ZD 2016, 153 f.

⁸⁰ Passadelis/Roth, Jusletter v. 4.4.2016 (Fn. 21), Rn. 45.

personenbezogene Daten verarbeitet werden bzw. der Verarbeiter dies nicht ausschliesst.

- 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 DSGVO verpflichtet die für eine Verarbeitung Verantwortlichen (bzw. seine Vertreter), ein Verzeichnis aller in ihrer Zuständigkeit liegenden Verarbeitungstätigkeiten zu führen und präzisiert 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 DSGVO formuliert diverse Vorgaben in Bezug auf die Sicherheit personenbezogener Daten, wobei gewisse, zumindest in allgemeiner Form umschriebene Massnahmen in jedem Fall vorgeschrieben werden (Art. 32 Abs. 1 DSGVO), während ansonsten in Bezug auf das anzulegende Schutzniveau auf Verhältnismässigkeitsgesichtspunkte verwiesen wird (Art. 32 Abs. 2 DSGVO).

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

- Nach Art. 33 DSGVO 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 DSGVO), wobei Art. 33 Abs. 3 DSGVO 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 besteht 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 offenbar 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 DSGVO ergänzt die erwähnte Meldepflicht durch eine Pflicht zur Benachrichtigung der betroffenen Person, 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 DSGVO noch ein Entfallen der Benachrichtigungspflicht in gewissen Konstellationen vor, wobei insbesondere Art. 34 Abs. 3 lit. a) DSGVO Fragen aufwirft, lässt diese Bestimmung die Benachrichtigungspflicht doch bereits dann entfallen, wenn der Verantwortliche geeignete Sicherheitsvorkehrungen getroffen hat, was aber nichts daran ändert, 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 DSGVO 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 DSGVO 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 DSGVO 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 DSGVO). Das Konsultationsverfahren ist in Art. 36 DSGVO im Einzelnen geregelt und kann in Empfehlungen der Aufsichtsbehörde münden, die zudem ihre Befugnisse nach Art. 58 DSGVO ausüben kann.

e) Datenschutzbeauftragter

Gemäss Art. 37 DSGVO sind gewisse Datenverarbeiter verpflichtet, einen Datenschutzbeauftragten zu benennen (wobei Konzerne oder Behörden auch gemeinsame Beauftragte vorsehen dürften). 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 Datenschutzbeauftragten 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 DSGVO).

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.⁸¹

Insbesondere werden die Untersuchungs- und Abhilfebefugnisse (letztere umfassen etwa das Recht, Geschäftsräume zu betreten, Verantwortlichen Anweisungen zu erteilen, aber auch das Recht, eine Verarbeitung zu verbieten) detailliert aufgeführt, präzisiert und im Ergebnis beträchtlich ausgeweitet (Art. 58 DSGVO). Weiter werden die Sanktionsbefugnisse ebenfalls detailliert ausgeführt, vereinheitlicht und erheblich ausgebaut; sie umfassen insbesondere die Befugnis zur Verhängung von (hohen) Geldbussen (Art. 83 DSGVO).⁸²

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, 79 DSGVO), 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 DSGVO). Weiter werden die Vorgaben betreffend die Haftung und das Recht auf Schadensersatz präzisiert, und

⁸¹ Zu den Sanktionen (neben den einschlägigen Kommentaren, vgl. Fn. 1) *Mario Martini/David Wagner/Michael Wenzel*, Das neue Sanktionsregime der DSGVO – ein scharfes Schwert ohne legislativen Feinschliff, *VerwArch* 2018, 296 ff.

⁸² 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.

es wird – im Falle eines Verstosses gegen die Verordnung – eine Gefährdungshaftung vorgesehen (Art. 82 DSGVO).⁸³

Schliesslich ist in diesem Zusammenhang auf Kap. VII („Zusammenarbeit und Kohärenz“) hinzuweisen, in dem die Zusammenarbeit zwischen den nationalen 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. DSGVO).⁸⁴ Die Verordnung stellt zudem einen Zuständigkeitsbestimmungsmechanismus bei mehreren betroffenen Aufsichtsbehörden auf (Art. 56), dessen Anwendung beträchtlich von der Auslegung des Begriffs «Hauptniederlassung» (Art. 4 Nr. 16) abhängen dürfte. Ferner wird neu der „Europäische Datenschutzausschuss“ geschaffen (Art. 68 DSGVO), der die sog. „Gruppe 29“ ersetzt. Der Ausschuss – zusammengesetzt aus den Leitern der Aufsichtsbehörden der Mitgliedstaaten und dem Europäischen Datenschutzbeauftragten – ist eine Einrichtung mit eigener Rechtspersönlichkeit. Ihm kommen zahlreiche, in Art. 70 DSGVO detailliert aufgeführte⁸⁵ Befugnisse zu, unter Einschluss der Überwachung und Sicherstellung der ordnungsgemässen Anwendung der Verordnung sowie der Erarbeitung von Leitlinien und Empfehlungen.

E. Schluss

Die technologische Entwicklung der letzten Jahrzehnte und damit aufgetretene Themen wie *big data*, das *internet of things*, soziale Netzwerke oder mobile Internetapplikationen 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. Die Datenschutzgrundverordnung mit ihren teilweise innovativen Ansätzen (Datenportabilität, *privacy by design*, *privacy by default*, Datenschutzfolgeabschätzung etc.) lässt sich als wichtigen Schritt in diese Richtung qualifizieren, wenn auch zu konzedieren ist, dass diese Instrumente auch nach einem Jahr Anwendung der Verordnung vielfach erst im Grundsatz angelegt sind und auf ihre Ausformung im Einzelnen und insbesondere stimmige Umsetzung noch warten.

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

⁸³ 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.

⁸⁴ 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.

⁸⁵ So umfasst die diesbezügliche Aufzählung in Art. 70 Abs. 1 DSGVO die Buchstaben a)-y).

Datenschutzraum gegenüber Drittstaaten aufzutreten. Dieser erweiterte Anwendungsbereich, zusammen mit den durchaus strengen Vorgaben an die Anerkennung eines angemessenen Datenschutzniveaus bei Drittstaaten, hat darüber hinaus das Potential, eine Annäherung des Datenschutzrechts zahlreicher anderer Staaten an dasjenige der EU zu bewirken und damit auch auf globaler Ebene mit Standards für die – gewiss notwendige – Vereinheitlichung voranzugehen.

Auch wenn die Datenschutzgrundverordnung mit dem Anspruch einer Harmonisierung des Datenschutzes angetreten ist, so ist die notwendige Beseitigung der rechtlichen Fragmentierung des Datenschutzes auf Unionsebene allerdings nur teilweise gelungen: 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 geglückt, den datenschutzrechtlichen Flickenteppich in Europa massgeblich zu vereinfachen. Auch die zahlreichen Öffnungsklauseln innerhalb der Datenschutzgrundverordnung führen dazu, dass nach wie vor mitgliedstaatliche Unterschiede bestehen.

Ob die wohl wichtigste Zielsetzung der Reform, nämlich die Überwindung der nach wie vor bestehenden Kluft zwischen datenschutzrechtlichen Aspirationen und der Lebensrealität im öffentlichen wie im privaten Bereich, erreicht werden kann, wird eine der zentralen Fragen und grössten Herausforderungen bleiben. Ein angepasster und stimmiger rechtlicher Rahmen stellt hierfür nämlich 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. Die Verordnung bietet hierzu hilfreiche Ansatzpunkte, etwa durch die Ermöglichung eines «Verbandsbeschwerderechts» auf nationaler Ebene, womit Datenschutzorganisationen im Namen von Betroffenen bei den Aufsichtsbehörden eine Beschwerde einzulegen.

Für die Schweiz sind die Implikationen der Datenschutzgrundverordnung im Ergebnis durchaus bedeutend und führen zur Notwendigkeit, das neue Recht sowohl im Rahmen der Revision des Datenschutzgesetzes wie auch in der Rechtsanwendung zu beachten. In diesem Bereich ist aber vieles noch ungeklärt, und gerade die Frage, welche Implikationen der ausgeweitete territoriale Anwendungsbereich auf Wirtschaftsteilnehmer und öffentliche Stellen in der Schweiz hat, sowohl in Bezug auf die daraus entstehenden Pflichten der Verantwortlichen wie auch die Durchsetzung allfälliger Anweisungen oder Sanktionen mitgliedstaatlicher Aufsichtsbehörden und der dabei dem EDÖB allenfalls zukommenden Rolle, ist derzeit hauptsächlich durch Rechtsunsicherheit geprägt und wird letztlich von der sich erst allmählich entwickelnden Rechtsprechung in der Union abhängen.