# Durchsetzungsmechanismen im EU-Recht und ihre Implikationen für die Schweiz

*Markus Kern/Astrid Epiney*

**Dieser Beitrag wurde erstmals wie folgt veröffentlicht:**
***Markus Kern/Astrid Epiney*, Durchsetzungsmechanismen im EU-Recht und ihre Implikationen für die Schweiz, in: Astrid Epiney/Daniela Nüesch (Hrsg.), Durchsetzung der Rechte der Betroffenen im Bereich des Datenschutzes / La mise en oeuvre des droits des particuliers dans le domaine de la protection des données, Zürich 2015, 19-54. Es ist möglich, dass die Druckversion – die allein zitierfähig ist – im Verhältnis zu diesem Manuskript geringfügige Modifikationen enthält.**

## Inhaltsübersicht

# A. Einleitung

Datenschutzrecht in der Schweiz ist immer auch vor dem Hintergrund der diesbezüglichen Vorgaben auf EU-Ebene zu sehen. Dies beruht nicht nur darauf, dass es grundsätzlich sinnvoll sein kann, als von EU-Mitgliedstaaten umgebener (kleiner) Staat die Entwicklungen in der EU zumindest zur Kenntnis zu nehmen und die Frage zu stellen, ob und inwieweit (legislative) Angleichungen oder Abweichungen von diesen sinnvoll sind, sondern auch auf dem in diesem Zusammenhang relevanten völkerrechtlichen Rahmen: Denn die Schweiz ist über die sog. Schengen- und Dublinassoziierung[1] auch an datenschutzrechtliche Vorgaben des EU-Rechts gebunden,[2] wobei sie in Anwendung der einschlägigen „Übernahmemechanismen" der genannten Assoziierungsabkommen auch die diesbezüglichen Weiterentwicklungen des Schengen- und Dublin-Besitzstands – wozu auch die datenschutzrechtlichen Regelungen (die im Wesentlichen einerseits in der RL 95/46[3] und im Rah-

---

1 Abkommen vom 26. Oktober 2004 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 (SAA; 0.362.31); Abkommen vom 26. Oktober 2004 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 (DAA; SR 0.142.392.68).

2 Vgl. schon ASTRID EPINEY, Datenschutz und „Bilaterale II", SJZ 2006, 121 ff.; 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, 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, 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.

3 RL 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281, 31. Zu dieser Richtlinie m.w.N. EPINEY/HOFSTÖTTER/MEIER/THEUERKAUF, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen (Fn. 2), 89 ff.

menbeschluss 2008/977[4], andererseits in den spezifischen sektoriellen Rechtsakten[5] zu finden sind) gehören – übernimmt.

Zwar ist hier in Bezug auf die genaue Reichweite dieser Einbindung der Schweiz in den unionsrechtlichen Besitzstand im Bereich des Datenschutzes nach wie vor noch einiges streitig, wobei in erster Linie auf die genaue 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)[6] und die Frage, ob auch die geplante Datenschutzgrundverordnung[7] Teil des Schengen- und Dublinbesitzstands sein soll (was auf EU-Ebene offenbar noch nicht abschliessend geklärt ist), hinzuweisen ist. Nichtsdestotrotz ist es in jedem Fall lohnend, die Entwicklungen in der EU zu verfolgen und danach zu fragen, inwieweit sie Implikationen für das schweizerische Recht entfalteten bzw. hier einen Anpassungsbedarf auslösten. Denn einmal erscheint es nach wie vor plausibel, dass auch die neuen Entwicklungen auf EU-Ebene im allgemeinen Datenschutzrecht für die Schweiz über einen Einbezug in den Schengen-/Dublin-Besitzstand verbindlich werden, und zum anderen ist es auch darüber hinaus sinnvoll, in diesem Bereich die unionsrechtlichen Entwicklungen zumindest zur Kenntnis zu nehmen und in die Betrachtungen einzubeziehen, zumal gewisse Aspekte auch im Rahmen der laufenden Revision der Datenschutzkonvention des Europarates – die nach ihren erklärten Zielsetzungen inhaltlich mit den Entwicklungen auf EU-Ebene abgestimmt werden soll[8] – relevant sein dürften.

Vor diesem Hintergrund geht die Zielsetzung der folgenden Ausführungen dahin, auf der Grundlage der Durchsetzungsmechanismen im Rahmen der RL 95/46 im geltenden Datenschutzrecht in der EU (B.), die Entwicklungstendenzen auf EU-Ebene in diesem Bereich im Gefolge des zu

---

4 Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. 2008 L 350, 60.

5 So etwa in den Eurodac oder das SIS betreffenden Regelungen. Vgl. zu diesen ausführlich EPINEY/HOFSTÖTTER/MEIER/THEUERKAUF, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen (Fn. 2), 143 ff.

6 Vgl. für die zuletzt genannte Ansicht EPINEY, SJZ 2006 (Fn. 2), 122 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, 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, 175 f.

7 Vgl. noch unten C.

8 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.

erwartenden Erlasses der sog. Datenschutzgrundverordnung aufzuzeigen (C.) und nach ihren Implikationen für die Schweiz (D.) zu fragen. Der Beitrag schliesst mit einer kurzen Schlussbemerkung (E.).

# B. Durchsetzungsmechanismen im Unionsrecht *de lege lata*

Die RL 95/46 – auf die sich die folgenden Ausführungen beschränken, so dass es hier nur um die Vorgaben des Unionsrechts an die Datenbearbeitung in den Mitgliedstaaten, unter Aussparung derjenigen auf Unionsebene, geht – kennt verschiedene Kategorien von Verpflichtungen bzw. Vorgaben, die der Durchsetzung bzw. effektiven Verwirklichung der materiellen Vorgaben im Bereich des Datenschutzrechts dienen (sollen). Im Wesentlichen können hier formelle Verarbeitungsvoraussetzungen (I.), Beteiligungsrechte der betroffenen Personen (II.), Regelungen betreffend Rechtsschutz, Haftung und Sanktionen (III.) sowie die Pflicht zur Einrichtung unabhängiger nationaler Kontrollstellen, denen bestimmte Befugnisse zukommen müssen (IV.), unterschieden werden.[9] Im Folgenden sollen diese Vorgaben – unter Berücksichtigung der jüngsten Rechtsprechung des EuGH (sog. Google-Urteil[10]) – skizziert werden, wobei jeweils auch auf mögliche Divergenzen im geltenden schweizerischen Recht (auf Bundesebene) hingewiesen wird.

## I. Formelle Verarbeitungsvoraussetzungen

Für eine rechtmäßige Datenverarbeitung müssen nach Art. 18–21 RL 95/46 neben den materiellen Anforderungen (den datenschutzrechtlichen Grundsätzen) auch formelle Verarbeitungsbedingungen respektiert werden:

– Art. 18 Abs. 1 RL 95/46 sieht eine grundsätzliche Meldepflicht für den für die Verarbeitung Verantwortlichen bei der nationalen Kontrollstelle vor, bevor er eine vollständig oder teilweise automatisierte Verarbeitung oder eine Mehrzahl von Verarbeitungen vornimmt. Die gemeldeten Verarbeitungen werden in ein Register aufgenommen, das von den nationalen

---

[9] Die folgenden Ausführungen stützen sich teilweise auf bereits durchgeführte Untersuchungen, vgl. insbesondere EPINEY/HOFSTÖTTER/MEIER/THEUERKAUF, Schweizerisches Datenschutzrecht vor europa- und völkerrechtlichen Herausforderungen (Fn. 2), 112 ff.; ASTRID EPINEY, Zu den völker- und europarechtlichen Rahmenbedingungen der Revision des Datenschutzgesetzes, Astrid Epiney/Patrick Hobi (Hrsg.), Die Revision des Datenschutzgesetzes / La révision de la Loi fédérale sur la protection des données, 2009, 19 ff. S. im Übrigen ausführlich zum EU-Datenschutzrecht, m.w.N. (auf die daher nachfolgend weitgehend verzichtet wird) ASTRID EPINEY/YVONNE SCHLEISS, in: Eva Maria Belser/Astrid Epiney/Bernhard Waldmann (Hrsg.), Datenschutzrecht. Grundlagen und öffentliches Recht, 2011, § 4.

[10] EuGH, Rs. C-131/12 (Google Spain), Urt. v. 13.5.2014.

Kontrollstellen zu führen ist und das von jedermann eingesehen werden kann (Art. 21 RL 95/46). Die Meldung zum Register der Kontrollstelle hat jedoch nur informatorischen Charakter; sie stellt daher keine Genehmigung für die Datenverarbeitung dar, und aus ihr können damit auch keine Aussagen über die Rechtmässigkeit der Verarbeitung abgeleitet werden. Daher ist die Kontrollstelle auch nicht verpflichtet, alle gemeldeten Verarbeitungen auf ihre Rechtmässigkeit zu prüfen. Art. 19 Abs. 1 RL 95/46 umschreibt die Angaben, die die Meldung enthalten muss. Die Mitgliedstaaten können aber auch Ausnahmen von oder eine Vereinfachung der Meldepflicht vorsehen, insbesondere bei Verarbeitungskategorien, bei denen eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen unwahrscheinlich ist (Art. 8 Abs. 2 RL 95/46).[11] Damit ist der Anwendungsbereich der Meldepflicht letztlich auf die Konstellationen beschränkt, bei denen eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen „wahrscheinlich" ist, womit diese letztlich sehr relativiert wird, insbesondere auch angesichts des Umstands, dass die Beurteilung der „Wahrscheinlichkeit" einer solchen Beeinträchtigung weitgehend im Gestaltungsspielraum der Mitgliedstaaten stehen dürfte.

– Nach Art. 20 RL 95/46 unterliegen Verarbeitungen mit spezifischen Risiken für die Rechte und Freiheiten der Personen einer sog. Vorabkontrolle durch die Kontrollstelle; der Datenschutzbeauftragte kann vorgeschaltet werden. In diesem Fall ist die Zulässigkeit der Datenverarbeitung und damit die Erfüllung der Rechtmässigkeitsanforderungen vor der Durchführung der Verarbeitung zu prüfen; insofern handelt es sich um eine echte Genehmigung der Datenverarbeitung. Allerdings wird den Mitgliedstaaten bei der Umschreibung des materiellen Anwendungsbereichs dieser Bestimmung ein denkbar weiter Gestaltungsspielraum eingeräumt: Sie legen fest, welche Verarbeitungen spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können und damit der Vorabkontrolle zu unterwerfen sind. Die Bestimmung präzisiert also weder die Voraussetzungen, unter denen vom Bestehen solcher Risiken auszugehen ist, noch ist ihr eine Verpflichtung zu entnehmen, in allen Fällen des Bestehens eines solchen Risikos auch tatsächlich eine Vorabkontrolle vorzusehen. Immerhin wird man aus der effektiven Wirksamkeit der Bestimmung ableiten können, dass eine solche Vorabkontrolle zumindest in einigen (wenn auch wenigen) Fällen durchzuführen ist und dass die Mitgliedstaaten tatsächlich das Vorliegen spezifischer Risiken für die Rechte und Freiheiten der Personen evaluieren müssen und auf der Grundlage vertretbarer Kriterien zu entscheiden haben, ob sich eine Vorabkontrolle

[11] Weiter können Register, die ausschliesslich der Information der Öffentlichkeit dienen (Art. 18 Abs. 3 RL 95/46), und bestimmte Verarbeitungen von Organisationen, die keinen Erwerbszweck erfüllen (Art. 18 Abs. 4 i.V.m. Art. 8 Abs. 2 lit. d RL 95/46), von der Meldepflicht ausgenommen werden.

rechtfertigt.[12] Nur auf der Grundlage dieser Auslegung kann die Zielsetzung des Art. 20 RL 95/46, im Falle besonders „risikoreicher" Datenverarbeitungen eine vorgängige Kontrolle sicherzustellen, zumindest annähernd erreicht werden.

Trotz der erwähnten Spielräume, die den Mitgliedstaaten in Bezug auf die Meldepflicht eingeräumt werden, entspricht die in Art. 11a DSG vorgesehene Meldepflicht den Vorgaben der RL 95/46 nicht, unterliegen doch Private nur im Falle der regelmässigen Bearbeitung besonders schützenswerter Personendaten oder von Persönlichkeitsprofilen oder im Falle der regelmässigen Bekanntgabe von Personendaten an Dritte einer Meldepflicht. Diese allgemeine Regelung erfüllt auch nicht die Anforderungen an die nach der RL 95/46 möglichen Ausnahmen.[13]

Soweit die Vorabkontrolle betroffen ist, kennt zumindest das DSG bislang kein solches Instrument.

## II. Beteiligungsrechte

In Bezug auf die Beteiligungsrechte sind in erster Linie folgende Aspekte zu erwähnen:

– Art. 10 RL 95/46 sieht für den Fall, dass die Daten beim Betroffenen selbst erhoben werden, eine umfassende Informationspflicht vor: Der Betroffene hat zumindest einen Anspruch, Informationen über die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmung der Verarbeitung und weitere Informationen, u.a. zu Empfängern oder über das Bestehen von Auskunfts- und Berichtigungsrechten, sofern sie unter Berücksichtigung der spezifischen Verarbeitungsumstände notwendig sind, um eine Verarbeitung nach Treu und Glauben zu gewährleisten, zu erhalten. Diese Information hat vorab und unaufgefordert zu erfolgen. Falls Daten nicht beim Betroffenen erhoben werden oder falls die bei ihm erhobenen Daten nachträglich an Dritte weitergegeben werden, kommt Art. 11 RL 95/46 zum Zuge, der parallele Informationspflichten vorsieht, wobei jedoch nach Art. 11 Abs. 2 RL 95/46 Ausnahmen für die Fälle vorgesehen sind, dass die Information der betreffenden Person unmöglich ist, einen unverhältnismässigen Aufwand erfordert oder eine gesetzliche Grundlage vorhanden ist. Die beiden Informationspflichten unterscheiden sich damit im Wesentlichen in Bezug auf den Mitteilungszeitpunkt.

---

[12] Vgl. in diesem Zusammenhang auch die Rechtsprechung des EuGH zu der strukturell parallel gelagerten Frage der Ausdehnung der Verpflichtung, eine UVP durchzuführen, auf (weitere) besonders umweltgefährdende Projekte: EuGH, Rs. C-301/95 (Kommission/Deutschland), Slg. 1998, Rz. 38 ff.; EuGH, Rs. C-392/96 (Kommission/Irland), Slg. 1999, I-5901, Rz. 64; EuGH, Rs. C-72/95 (Kraaijeveld), Slg. 1996, I-5403, Rz. 50; EuGH Rs. C-474/99 (Kommission/Spanien), Slg. 2002, I-5293, Rz. 30; EuGH, Rs. C-87/02 (Kommission/Italien), Slg. 2004, I-5975, Rz. 38 ff.

[13] Vgl. zu dieser Divergenz auch Botschaft zur Revision des DSG, BBl 2003 2101, 2118.

- Nach Art. 12 lit. a RL 95/46 hat die betroffene Person das Recht, vom Verantwortlichen in angemessenen Abständen, ohne unzumutbare Verzögerung oder übermässige Kosten Auskunft darüber zu erhalten, ob es eine ihn betreffende Datenverarbeitung gibt, welche Zweckbestimmung sie hat, wer der Empfänger der Daten ist, welche Daten Gegenstand der Verarbeitung sind, woher diese kommen und wie die Verarbeitung (im Falle automatischer Entscheidungen) logisch aufgebaut ist. Weiter hat die betroffene Person ein Recht auf Berichtigung, Löschung oder Sperrung von Daten, deren Verarbeitung nicht den Bestimmungen der Richtlinie entspricht (Art. 12 lit. b RL 95/46). Der für die Verarbeitung Verantwortliche muss die Gewähr abgeben, dass jede Berichtigung, Löschung oder Sperrung den Dritten, denen die Daten übermittelt wurden, mitgeteilt wird, wenn dies nicht mit einem unverhältnismäßigen Aufwand verbunden ist (Art. 12 lit. c RL 95/46). In gewissen Konstellationen und unter bestimmten Voraussetzungen können die Rechte des Art. 12 RL 95/46 eingeschränkt werden (Art. 13 Abs. 2 RL 95/46).
- Nach Art. 14 lit. b RL 95/46 ist im Falle der Verwendung von Daten für Zwecke der Direktwerbung die Möglichkeit der Einlegung eines Widerspruchs vorzusehen. Wird Widerspruch eingelegt, kann sich die vom für die Verarbeitung Verantwortlichen vorgenommene Verarbeitung nicht mehr auf diese Daten beziehen, wobei die Rechtswirkung grundsätzlich *ex nunc* eintritt. Ein „abgeschwächtes“ (weil einzelstaatliche Bestimmungen etwas anderes vorsehen können) Widerspruchsrecht gilt auch allgemein, so dass die Betroffenen danach gegen jede sie betreffende Datenbearbeitung aus überwiegenden, schutzwürdigen bzw. sich aus ihrer besonderen Situation ergebenden Gründen Widerspruch einlegen können und sich die Datenbearbeitung im Falle eines berechtigten Widerspruchs nicht mehr auf diese Daten beziehen darf (Art. 14 lit. a) RL 95/46).
- Nach Art. 15 RL 95/46 ist jeder Person das Recht einzuräumen, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschliesslich aufgrund einer automatisierten Datenverarbeitung zum Zwecke der Bewertung einzelner Aspekte dieser Person ergeht. Die Vorschrift beruht auf dem Grundgedanken, dass Entscheidungen, die das Persönlichkeitsrecht einer Person zentral berühren, nicht einem Computerprogramm überlassen werden dürfen, sondern stets personal verantwortet werden müssen. Art. 15 Abs. 2 RL 95/46 sieht eng begrenzte Ausnahmen zu diesem Grundsatz vor.

Das geltende schweizerische Recht dürfte im Verhältnis zu den Vorgaben betreffend die Informationspflicht noch (trotz der Art. 14, 18a DSG) defizitär sein. So dürfte die „Informationspflicht“ in Art. 14 DSG im Verhältnis zu Art. 4 Abs. 4, Art. 10 RL 95/46 (in Bezug auf bei den Betroffenen selbst erhobenen Daten) insofern nicht „weit“ genug gehen, als die Richtlinie eine aktive Information erfordert, so dass es eben gerade nicht ausreicht, dass die Erhebung und Bearbeitung in „irgendeiner Form“ – etwa, weil sie aus den

Umständen ersichtlich ist[14] – erkennbar ist. Art. 14 DSG betrifft nämlich nur besonders schützenswerte Daten oder Persönlichkeitsprofile.
Soweit das Auskunftsrecht betroffen ist, fehlt im schweizerischen Recht – trotz der weitgehend parallelen Ausgestaltung des Art. 8 DSG im Verhältnis zu Art. 12 RL 95/46 – eine ausdrückliche Verpflichtung des Inhabers einer Datensammlung, auch Dritte, denen die Daten übermittelt wurden, über allfällige Berichtigungen, Löschungen oder Sperrungen zu unterrichten (vgl. Art. 12 lit. c RL 95/46).
Das Datenschutzgesetz kennt kein Widerspruchsrecht im Sinn des Art. 14 lit. b RL 95/46.[15] Art. 12 Abs. 2 lit. b DSG sieht zwar vor, dass gegen den ausdrücklichen Willen einer Person keine Daten dieser Person bearbeitet werden dürfen, lässt aber die Bearbeitung im Falle eines „Rechtfertigungsgrundes" gleichwohl zu, so dass auch diese Bestimmung nichts an dem Anpassungsbedarf des DSG in dieser Hinsicht ändern dürfte.
Ebensowenig ist dem geltenden schweizerischen Recht ein grundsätzliches Verbot, ausschliesslich aufgrund einer automatisierten Einzelentscheidung eine beschwerende Verfügung zu erlassen, bekannt.
Diese punktuellen Defizite des schweizerischen Rechts ändern jedoch nichts daran, dass es in weiten und bedeutenden Teilen den Vorgaben der Richtlinie entsprechende Garantien vorsieht.
Die Bedeutung der Rechte der Betroffenen wurde jüngst in der Rs. C-131/12 (sog. Google-Urteil[16]) illustriert: Auf der Grundlage der Bejahung der Eröffnung des Anwendungsbereichs der RL 95/46, da die Tätigkeit einer Suchmaschine als Datenverarbeitung im Sinne der RL 95/46 anzusehen sei und diese auch im Rahmen der Niederlassung von Google in Spanien ausgeübt werde (so dass der räumliche Anwendungsbereich der RL 95/46 betroffen sei) nahm der Gerichtshof in erster Linie zur rechtlichen Tragweite der Art. 12 lit. b und Art. 14 Abs. 1 lit. a RL 95/46 Stellung: 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 bzw. Art. 8 Grundrechtecharta räumen den Betroffenen ein Recht ein, dass bestimmte, sie betreffende Informationen nicht mehr auf der Ergebnisliste angezeigt werden, so dass diese Rechte grundsätzlich sowohl gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers als auch dem Interesse der breiten Öffentlichkeit am Zugang zu solchen Informationen überwiegen, letzteres unter dem Vorbehalt, dass nicht besondere Gründe (z.B. die Rolle der Person im öffentli-

[14] Was im Übrigen regelmässig Unsicherheiten unterworfen sein wird.
[15] Auf diese Divergenz auch hinweisend Botschaft zur Revision des DSG, BBl 2003 2102, 2118.
[16] EuGH, Rs. C-131/12 (Google Spain), Urt. v. 13.5.2014.

chen 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.

Das Urteil überzeugt im Ergebnis und in der Begründung und ist in erster Linie aus dreierlei Gründen bemerkenswert:

- Erstens dürfte ihm der auch in anderen Bereichen relevante Grundsatz zu entnehmen sein, dass der grundrechtliche Anspruch darauf, dass bestimmte personenbezogene Daten nicht mehr (in einer bestimmten Art und Weise) der Öffentlichkeit zugänglich gemacht werden dürfen, schwerer wiegt als ebenfalls implizierte wirtschaftlich Interessen. Die Schwierigkeit in diesem Zusammenhang wird regelmäßig darin liegen festzustellen, ob tatsächlich ein „Löschungsanspruch" besteht, wobei es die Ausführungen des Gerichtshofs nahelegen, dass grundsätzlich bereits aufgrund der Verknüpfungsmöglichkeiten und der damit einhergehenden Eingriffe in die Persönlichkeitsrechte der Betroffenen ein derartiger Löschungsanspruch besteht.
- Zweitens, und damit in engem Zusammenhang stehend, gilt dies auch in reinen Privatrechtsverhältnissen, womit der Gerichtshof im Ergebnis von einer Drittwirkung der genannten Grundrechte ausgeht, wobei diese Drittwirkung jedoch auf der Einräumung der entsprechenden Rechte in der RL 95/46 beruhen dürfte, seien diese doch im Lichte der Grundrechte auszulegen.
- Schliesslich ist die Differenzierung zwischen einer Veröffentlichung von Personendaten auf „irgendeiner" Webseite und ihrer Zugänglichkeit über eine Suchmaschine und die strengeren Anforderungen an letztere angesichts der Rolle von Suchmaschinen für die Auffindbarkeit von Informationen in jeder Beziehung überzeugend und wohl auch auf andere Formen „differenzierter" Information übertragbar.

Da die Schweiz in Bezug auf die in dem Urteil relevanten Rechte der Betroffenen eine parallele Rechtslage kennt (s. insbesondere Art. 12 und 15 DSG), ist davon auszugehen, dass die Erwägungen des Gerichtshofs aus letztlich parallelen Gründen auch für die Rechtslage in der Schweiz relevant sind, so dass Vieles dafür spricht, dass man auf der Grundlage des schweizerischen Rechts zu einem ähnlichen Ergebnis kommen würde bzw. müsste.

## III. Rechtsschutz, Haftung und Sanktionen

Art. 22 RL 95/46 ist eine Rechtsbehelfsgarantie zu entnehmen: Jede Person muss gegen die Verletzung der Rechte, die ihr durch die für die betreffende

Verarbeitung geltenden einzelstaatlichen Rechtsvorschriften garantiert sind, bei Gericht einen Rechtsbehelf einlegen können.
Falls ihr wegen einer rechtswidrigen Verarbeitung ein Schaden entstanden ist, muss sie das Recht haben, von dem für die Verarbeitung Verantwortlichen Schadensersatz zu verlangen (Art. 23 Abs. 1 RL 95/46). Dabei besteht eine Haftung für vermutetes Verschulden, von der sich der Verantwortliche exkulpieren kann, wenn er nachweist, dass der Umstand, durch den der Schaden eingetreten ist, ihm nicht zu Last gelegt werden kann (Art. 23 Abs. 2 RL 95/46).
Die einschlägigen Regelungen im schweizerischen Recht betreffend Rechtsschutz, Haftung und Sanktionen dürften diesen (eher allgemein formulierten) Vorgaben entsprechen.

## IV. Nationale Kontrollstelle

Nach Art. 28 RL 95/46 ist bzw. sind zur Überwachung der Anwendungen der Richtlinie in den Mitgliedstaaten eine oder mehrere „völlig unabhängige“ Kontrollstelle(n) zu schaffen; diese sind für die Kontrolle aller Verarbeitungen zuständig, die auf dem Hoheitsgebiet ihres Mitgliedstaates stattfinden, unabhängig vom einzelstaatlichen Recht, das auf die jeweilige Verarbeitung anzuwenden ist (Art. 28 Abs. 6 RL 95/46/EG). Den Kontrollstellen müssen Untersuchungsbefugnisse, wirksame Einwirkungsbefugnisse sowie Klagerechte oder Anzeigebefugnisse zukommen.[17]
Während davon auszugehen ist, dass der EDÖB die Anforderungen an die Unabhängigkeit erfüllt, sind in Bezug auf die kantonalen Behörden mitunter gewisse Zweifel angebracht, insbesondere soweit die personelle und finanzielle Ausstattung sowie die Budgethoheit betroffen sind.
In Bezug auf die der Kontrollstelle einzuräumenden Befugnisse unterliegt es gewissen Zweifeln, ob die Beschränkung der Befugnisse des EDÖB im Privatrechtsbereich auf die Abklärung und Abgabe von Empfehlungen von „Systemfehlern“ (Art. 29 Abs. 1 lit. a DSG) mit den unionsrechtlichen Vorgaben in Einklang stehen: Art. 28 Abs. 3 RL 95/46 jedenfalls ist keine diesbezügliche Einschränkung zu entnehmen. Sodann stellt sich die Frage, ob die Befugnis zum Erlass von Empfehlungen und die Möglichkeit, diese gerichtlich durchzusetzen, den Anforderungen von Art. 28 Abs. 3 3. Spiegelstrich RL 95/46 im Einklang steht.[18]

[17] Vgl. zu den Anforderungen an die Kontrollstellen im Einzelnen, m.w.N. auf die Rechtsprechung des EuGH, EPINEY/SCHLEISS, in: Belser/Epiney/Waldmann, Datenschutzrecht (Fn. 9), § 4, Rn. 77 ff.
[18] Vgl. hierzu auch unten D.II.1.

# C. Entwicklungsperspektiven: die Datenschutzgrundverordnung

## I. Allgemeines

Mit dem Vertrag von Lissabon hat die Europäische Union eine umfassende Kompetenzgrundlage im Bereich des Datenschutzes erhalten (Art. 16 AEUV) und steht zudem unter der Verpflichtung von Art. 8 EU-Grundrechtecharta, den Schutz personenbezogener Daten sicherzustellen. Diesen kompetenz- und grundrechtlichen Impuls hat die EU-Kommission mit einem Vorschlag für eine sogenannte Datenschutzgrundverordnung (DSGV) aufgenommen. Die Grundverordnung soll die Richtlinie 95/46 als heutiges Kernstück des europäischen Datenschutzrechts ersetzen, dabei das europäische Datenschutzrecht auf eine neue Grundlage stellen und innerhalb der EU eine vollständige Rechtsvereinheitlichung herbeiführen.[19] Bereits vor ihrer Verhandlung im EU-Parlament war die Datenschutzgrundverordnung Gegenstand heftiger Debatten, was sich in der Tatsache wiederspiegelte, dass für die Behandlung im Ausschuss Bürgerliche Freiheiten, Justiz und Inneres des EU-Parlaments 3‘133 Änderungsanträge eingereicht wurden. Am 12. März 2014 hat nun das Plenum des EU-Parlaments die Verordnung in erster Lesung verabschiedet. Nach der Einigung im Rat soll gemäss aktueller Planung ab Sommer 2014 mit den Verhandlungen zwischen Rat, EU-Parlament und EU-Kommission (sogenannter Trilog) begonnen werden. Im Gleichzug hatte die EU-Kommission auch einen Vorschlag für eine Richtlinie zum Schutz der Personendaten bei behördlicher Verwendung in der Strafverfolgung und Strafvollstreckung unterbreitet.[20] Im Gesetzgebungsprozess soll der Richtlinienvorschlag demselben Verfahrensrhythmus folgen wie die Datenschutzgrundverordnung und letztlich den Rahmenbeschluss 2008/977/JI ersetzten. Die folgenden Ausführungen konzentrieren sich nun allerdings auf Neuerungen der Datenschutzgrundverordnung, da sich die mit der Richtlinie angestrebten Anpassungen inhaltlich weitgehend an den entsprechenden Vorschriften der Grundverordnung orientieren bzw. direkt auf diese verweisen.

---

[19] Vorschlag vom 25. Januar 2012 für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012) 11 endgültig; zum Wechsel auf die Erlassform der Verordnung, GERRIT HORNUNG, Eine Datenschutz-Grundverordnung für Europa? ZD 2012, 100.

[20] Vorschlag vom 25. Januar 2012 für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM(2012) 10 endgültig.

## II. Materielle Elemente

Die Datenschutzgrundverordnung soll gemäss Vorschlag der EU-Kommission eine Reihe materieller Neuerungen bringen, die im Folgenden kurz skizziert werden sollen:[21]

- Eine wichtige – und insbesondere seitens der ausländischen Internetkonzerne äusserst umstrittene – Neuerung der Datenschutzgrundverordnung betrifft den *Anwendungsbereich* des Datenschutzrechts der Union. Demnach soll die Verordnung künftig auch auf Datenbearbeiter in Drittstaaten Anwendung finden, sofern diese entweder in der EU ansässigen Personen Waren oder Dienstleistungen anbieten oder deren Verhalten beobachten (Art. 3 Abs. 2 E-DSGV).
- Im Hinblick auf die Rechte der betroffenen Personen sind insbesondere Anpassungen im Bereich der *Einwilligung* vorgesehen. Diese soll inskünftig eine ausdrückliche Willenskundgabe voraussetzen und muss zudem ohne jeden Zwang, für den konkreten Fall sowie in Kenntnis der konkreten Sachlage erfolgen (Art. 4 Ziff. 8 E-DSGV). Die Beweislast liegt neu ausdrücklich beim Datenverarbeiter (Art. 7 Abs. 1 E-DSGV) und der betroffenen Person steht jederzeit die Möglichkeit einer Widerrufung offen (Art. 7 Abs. 3 E-DSGV). Keine ausreichende Grundlage für eine Datenbearbeitung stellen Einwilligungen dar, die in einer Konstellation eines „erheblichen Ungleichgewichts" zwischen Datenbearbeiter und betroffener Person ergehen (Art. 7 Abs. 4 E-DSGV)[22] sowie wenn im Falle eines Kindes unter dreizehn Jahren keine Zustimmung der Eltern oder des Vormundes vorliegt (Art. 8 Abs. 1 E-DSGV).[23]
- Das sogenannte „*Recht auf Vergessenwerden*" beinhaltete gemäss Vorschlag der EU-Kommission einen Anspruch auf Löschung von Daten sowie darauf, dass der für die Verarbeitung Verantwortliche sämtliche vertretbaren Schritte unternimmt, um bei veröffentlichten Daten auch Dritte über die Löschung zu informieren (Art. 17 E-DSGV). Das EU-Parlament hat die Betitelung des entsprechenden Rechts nun auf ein „Recht auf Löschung" reduziert und damit einen „Etikettenschwindel" berichtigt und darüber hinaus die Tragweite des Anspruches, namentlich gegenüber Drittpersonen, teilweise reduziert.
- Im Vorschlag vorgesehen ist auch ein *Recht auf Datenübertragbarkeit* (Art. 18 E-DSGV), welches der betroffenen Person gegenüber dem Bearbeiter von elektronischen Daten den Anspruch einräumt, eine Kopie der

---

[21] Für einen Überblick siehe etwa HORNUNG, ZD 2012 (Fn. 19), 100 ff.; MARKUS KERN, Datenschutzrevision in Europa: Neuer Wein? Neue Schläuche?, digma 2013/01, 34 ff.

[22] Vgl. nun jedoch die Einschränkung gemäss der Version nach der Ersten Lesung des EU-Parlaments, wonach in diesem Fall lediglich eine enge Zweckbindung vorgenommen werden soll, wobei die Gültigkeit der Zustimmung erlischt, wenn der Zweck nicht mehr gegeben ist oder die Datenbearbeitung zur Zweckerfüllung nicht mehr erforderlich ist.

[23] Das EU-Parlament hat in der ersten Lesung eine Beschränkung des Zustimmungserfordernisses auf den Verkauf von Gütern und Dienstleistungen vorgenommen.

verarbeiteten Daten in einem gängigen elektronischen Format zu erhalten. Damit soll einerseits eine Schutzgewährleistung gegenüber betroffenen Personen erreicht werden und andererseits der Wettbewerb zwischen Onlineplattformen (Agenden, sozialen Netzwerken etc.) verstärkt werden, indem den Nutzern der Wechsel zwischen den Anbietern erleichtert wird.

– Sodann soll mit der Verankerung einer Reihe von Datenschutzinstrumenten erreicht werden, dass den Datenschutzinteressen insbesondere in technischen Entwicklungsprozessen eine gewichtigere Rolle zukommt (Vorgaben zum Datenschutz durch Technik – sogenanntes *data protection by design* und *data protection by default* – gemäss Art. 23 E-DSGV; *Zertifizierungsverfahren* sowie Datenschutzsiegel und –zeichen gemäss Art. 39 E-DSGV), dass Risiken frühzeitig erkannt werden, um gegebenenfalls für geeignete Abhilfe zu sorgen (*Datenschutz-Folgeabschätzung* gemäss Art. 33 E-DSGV), sowie dass Datenschutzverletzungen gegenüber Behörden, betroffenen Personen und der Öffentlichkeit (Meldung von Verletzungen sowie Benachrichtigung der betroffenen Person – sogenannte *data breach notification* – gemäss Art. 31 und 32 E-DSGV) kundgetan werden. Diese Schaffung von Transparenz in Bezug auf erfolgte Datenschutzverletzungen kann einerseits dazu dienen, die aktuelle Gefahrenlage darzustellen, dürfte aber andererseits aufgrund der drohenden Prangerwirkung für Datenbearbeiter auch einen Anreiz darstellen, ein hohes Datensicherheitsniveau zu erreichen.

## III. Institutionelle Anpassungen

Neben den genannten Anpassungen in Bezug auf die Rechte der Betroffenen und neue Datenschutzinstrumente besteht die Hauptstossrichtung der Datenschutzgrundverordnung insbesondere in einer Neugestaltung des institutionellen Gefüges in diesem Bereich. Hierbei sind Anpassungen auf Ebene der Datenbearbeiter, der Mitgliedstaaten sowie im Hinblick auf die europäische Behördenlandschaft vorgesehen.

### *1. Datenschutzbeauftragte*

Gewissermassen auf der untersten institutionellen Hierarchiestufe sieht die Grundverordnung die Benennung von *Datenschutzbeauftragten* in Behörden oder öffentlichen Einrichtungen, in Unternehmen mit über 250 Mitarbeitern sowie bei Verarbeitern, die im Bereich der Beobachtung von Personen tätig sind, vor (Art. 35 ff. E-DSGV).[24] Zwar ausserhalb der eigentli-

[24] Gemäss dem aktuellen Stand der Debatten nach der ersten Lesung des EU-Parlaments sollen neben öffentlichen Einrichtungen und Datenbearbeitern, die im Bereich der regelmässigen Beobachtung von Personen tätig sind, auch juristische Personen, die Daten von mehr als 5000 Personen pro Jahr bearbeiten, sowie Verarbeiter von schützenswerten Daten zur Ernennung eines Datenschutzbeauftragten verpflichtet werden; kritisch zum ursprünglichen Vorschlag der EU-Kommission PETER GOLA/SEBASTIAN SCHULZ,

chen Behördenorganisation angesiedelt, aber dennoch als Teil eines weit verstandenen institutionellen Rahmens sollen die Datenschutzbeauftragten für eine dezentrale und einer allfälligen Behördenintervention vorgelagerte Rechtsdurchsetzung sorgen. Dabei kommt ihnen unter anderem die Aufgabe zu, die Verantwortlichen über ihre datenschutzrechtlichen Pflichten zu unterrichten, die Umsetzung der Strategien zum Schutz personenbezogener Daten zu begleiten, die Umsetzung der datenschutzrechtlichen Vorgaben des Unionsrechts, beispielsweise im Rahmen von *privacy by design*, zu überwachen und sicherzustellen, dass die von den Behörden ergriffenen Massnahmen effektiv umgesetzt werden (Art. 37 Abs. 1 E-DSGV).

*2. Nationale Ebene*

Eine wichtige Rolle in der künftigen institutionellen Ordnung wird den *nationalen Datenschutzbehörden* zugedacht:[25] Bereits unter geltendem Recht sieht Art. 28 RL 95/46 die Pflicht der Mitgliedstaaten vor, eine oder mehrere unabhängige öffentliche Stellen einzurichten, die mit Untersuchungs- und Einwirkungsbefugnissen sowie mit einem Klagerecht bzw. einer Anzeigebefugnis zu betrauen sind. In der Grundverordnung werden diese Stellen nunmehr als „Aufsichtsbehörden" bezeichnet, deren grundsätzliche Aufgabe darin bestehen soll, die Anwendung der rechtlichen Vorgaben zu überwachen und die einheitliche Anwendung der Vorschriften in der Union sicherzustellen (Art. 46 Abs. 1 und Art. 52 Abs. 1 Bst. a und c E-DSGV). Die Grundverordnung enthält detaillierte Vorgaben sowohl zur Unabhängigkeit der Behörde als auch ihrer Mitglieder sowie zur gesetzlichen Verankerung der Behörde (Art. 47–49 E-DSGV). In Bezug auf die Durchsetzung des Datenschutzrechts soll den Aufsichtsbehörden neben der generellen Sicherstellung einer einheitlichen Rechtsumsetzung insbesondere die Aufgabe der konkreten Rechtsdurchsetzung im Einzelfall zukommen. Hierfür hätten sie die Kompetenz, aus eigener Initiative oder auf Beschwerde betroffener Personen und Verbände hin Untersuchungen zu konkreten Sachverhalten durchzuführen (Art. 52 Abs. 1 Bst. b und d E-DSGV), dürften dazu Zugriff auf alle erforderlichen personenbezogenen Daten und Informationen nehmen und erhielten Zugang zu den Geschäftsräumlichkeiten der Datenbearbeiter (Art. 53 Abs. 2 E-DSGV). Sodann soll den Aufsichtsbehörden die Kompetenz zukommen, als Resultat dieser Untersuchungen Verarbeiter auf Verstösse gegen die Vorschriften hinzuweisen, zu ermahnen oder zu verwarnen, zur Ausführung der Anträge betroffener Personen anzuhalten sowie die Berichtigung, Löschung oder Vernichtung von Daten anzuordnen oder die Verarbeitung vorübergehend oder endgültig zu untersagen (Art. 53 Abs. 1 E-DSGV).

---

Der Entwurf für eine EU-Datenschutz-Grundverordnung – eine Zwischenbilanz, RDV 2013, 4 f.; SUSANNE DEHMEL/NILS HULLEN, Auf dem Weg zu einem zukunftsfähigen Datenschutz in Europa?, ZD 2013, 152 f.

[25] Vgl. dazu HORNUNG, ZD 2012 (Fn. 19), 101 u. 104.

### *3. Europäische Ebene*

Auch der institutionelle Rahmen auf europäischer Ebene soll mit der Grundverordnung Anpassungen erfahren: Zum einen ist die Schaffung eines *Europäischen Datenschutzausschusses* geplant, der als Nachfolger der bestehenden „Artikel 29-Gruppe" schwergewichtig eine beratende und koordinative Funktion übernehmen und als Plattform für den Austausch von Fachwissen und zur Erstellung gemeinsamer Leitlinien dienen soll (Art. 64 ff. E-DSGV). Der Ausschuss setzt sich aus den Leitern der mitgliedstaatlichen Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten zusammen.

Zum anderen soll der *EU-Kommission* künftig eine zentrale Rolle bei der weiteren Konkretisierung und der Durchsetzung des europäischen Datenschutzrechts zukommen. Gemäss dem Vorschlag der Kommission würde diese unter anderem die Befugnis erhalten, im Rahmen des sogenannten Kohärenzverfahrens, welches die Zusammenarbeit zwischen nationalen Aufsichtsbehörden auf eine neue Grundlage stellen soll, Stellungnahmen zu Massnahmen der nationalen Aufsichtsbehörden abzugeben (Art. 59 E-DSGV), von diesen geplante Massnahmen gegebenenfalls auszusetzen (Art. 60 E-DSGV) und den Entscheidungsgegenstand unter Umständen in letzter Konsequenz an sich zu ziehen und mittels Durchführungsrechtsakt selbst zu entscheiden (Art. 62 Abs. 1 Bst. a E-DSGV).[26] Darüber hinaus erhielte die Kommission äusserst weitreichende Ermächtigungen zum Erlass von delegierten Rechtsakten (Art. 86 E-DSGV), welche weit über die „Ergänzung oder Änderung bestimmter nicht wesentlicher Vorschriften" der Verordnung hinausgehen, wofür das Instrument der delegierten Rechtsakte gemäss Art. 290 AEUV eigentlich gedacht ist. Demzufolge würde die Kommission künftig zum eigentlichen Protagonisten bei der Überwachung, Durchsetzung und legislativen Ergänzung der unionsrechtlichen Datenschutzvorschriften.[27] Durchaus denkbar ist allerdings, dass diese Kompetenzfülle der EU-Kommission im EU-Parlament und insbesondere im Rat kritisch beurteilt und dementsprechend im Verlaufe des Gesetzgebungsprozesses noch reduziert wird.

---

[26] Diesfalls soll das sogenannte Prüfverfahren gemäss Art. 5 Verordnung 182/2011 zur Anwendung gelangen. Danach kann der Durchführungsrechtsakt lediglich unter der Bedingung erlassen werden, dass der beizuziehende Ausschuss, welcher sich aus Vertretern der Mitgliedstaaten zusammensetzt, eine befürwortende Stellungnahme abgibt. Die Beschlussfassung erfolgt dabei nach den Modalitäten und den Stimmengewichtungen im Rat.

[27] Kritisch in dieser Hinsicht etwa auch HORNUNG, ZD 2012 (Fn. 19), 105 f.; NIKO HÄRTING, Starke Behörden, schwaches Recht – der neue EU-Datenschutzentwurf, BB 2012, 460.

*4. Einschätzungen*

Werden diese institutionellen Anpassungen insgesamt in den Blick genommen, so drängen sich in Bezug auf die Rechtsdurchsetzung einige Feststellungen auf:

Zunächst stellt die Pflicht zur Ernennung von Datenschutzbeauftragten einen Mechanismus dar, um bereits frühzeitig für eine Einhaltung der datenschutzrechtlichen Vorgaben zu sorgen. Damit könnte auf der institutionellen Ebene ein Schritt genommen werden, um den datenschutzrechtlichen Interessen bei Bearbeitungsstrukturen und Bearbeitungskontext ein grösseres Gewicht zuzumessen und damit Rechtsverletzungen frühzeitig vorzubeugen oder solche überhaupt zu verhindern.[28] Inwieweit jedoch eine interne und – selbst bei Sicherstellung einer gewissen Unabhängigkeit – letztlich interessensgebundene Instanz ohne Dotierung mit einem eigentlichen Durchsetzungsinstrumentarium diese Funktion tatsächlich erfüllen kann, wird sich allerdings in der (unionsrechtlichen) Praxis erst zeigen müssen.

Die gewichtigste Rolle im zu schaffenden Behördengefüge soll, wie obenstehend dargetan, der EU-Kommission zukommen. Diese würde an die Spitze einer Behördenpyramide gesetzt, erhielte zudem weitgehende Legislativkompetenzen und einen privilegierten Rückgriff auf die nationalen Aufsichtsbehörden, einerseits über das Kohärenzverfahren und andererseits über den Europäischen Datenschutzausschuss. In Anbetracht dieser Fülle an Befugnissen kann mit Fug die Frage aufgeworfen werden, weshalb die für die mitgliedstaatlichen Aufsichtsbehörden geltenden Unabhängigkeitsanforderungen auf Unionsebene nicht ebenfalls zur Anwendung gebracht werden und ob nicht das Subsidiaritätsprinzip eine ausgewogenere Verteilung der Zuständigkeiten zwischen Union und Mitgliedstaaten nahelegen würde.

Über die Funktionen und Kompetenzen der EU-Kommission hinausgehend zeigt sich der generelle Ansatz der Datenschutzgrundverordnung, durch ein starkes, mit weitreichenden Kompetenzen und ausreichenden Mitteln ausgestattetes Behördengeflecht eine effektive Durchsetzung des Datenschutzrechts sicherzustellen.[29] Dies erscheint insofern als begrüssenswert, als die Rechtsdurchsetzung tatsächlich das wohl schwerwiegendste Problem des Datenschutzes darstellt. Gleichzeitig ist jedoch die Gefahr nicht gänzlich von der Hand zu weisen, dass eine übermässig komplex gestaltete und bis in die Details unionsrechtlich geregelte Verfahrens- und Behördenstruktur einen beträchtlichen administrativen Aufwand sowohl für die öffentliche Hand als auch für die beteiligten Datenbearbeiter und die betroffenen Personen nach sich zieht, ohne umgekehrt aufgrund der Schwerfälligkeit der Abstimmungsprozesse Gewähr für eine wirksame und insbesondere zügige Rechtsdurchsetzung zu bieten.

---

[28] Vgl. dazu auch nochmals unten C.III.

[29] Vgl. dazu ebenfalls nochmals C.III.

## IV. Rechtsbehelfe

### *1. Beschwerde bei der mitgliedstaatlichen Aufsichtsbehörde*

Das geltende Unionsrecht verbrieft in Art. 28 Abs. 4 RL 95/46 das Recht, sich zur Geltendmachung der Datenschutzansprüche mit einer Eingabe an die Kontrollstelle zu wenden. Die Grundverordnung sieht nun ein analoges Beschwerderecht vor, wonach jeder Person das Recht auf Beschwerde bei einer mitgliedstaatlichen Aufsichtsbehörde eingeräumt werden soll, um Datenbearbeitungen zu rügen, welche die Vorgaben der Verordnung verletzen (Art. 73 Abs. 1 E-DSGV).[30] Den mit den Beschwerden befassten Aufsichtsbehörden kommt die Pflicht zu, entsprechende Untersuchungen in entsprechendem Umfang vorzunehmen und die betroffenen Personen innert angemessener Frist über den Gang der Beschwerde sowie dessen Ergebnis zu unterrichten (Art. 52 Abs. 1 Bst. b E-DSGV). Die Leistungen der Aufsichtsbehörden und somit auch das eigentliche Beschwerdeverfahren sind für die betroffenen Personen grundsätzlich kostenlos. Eine Ausnahme besteht für offensichtlich missbräuchliche Vorbringen (Art. 52 Abs. 5 und 6 E-DSGV).

Ein eigentlicher Schwerpunkt der geplanten unionsrechtlichen Regeln stellt die Zusammenarbeit zwischen den mitgliedstaatlichen Aufsichtsbehörden sowie zwischen diesen und der EU-Kommission dar. Dazu besteht eine Pflicht zur Leistung von Amtshilfe (Art. 55 E-DSGV), es wird eine rechtliche Grundlage zur Durchführung gemeinsamer Untersuchungs-, Durchsetzungs- und anderweitiger Massnahmen geschaffen (Art. 56 E-DSGV) und schliesslich das Kohärenzverfahren verankert, welches eine inhaltliche Koordination der Verfahren sicherstellen soll und der EU-Kommission Zugriff auf die Verfahren vor den nationalen Aufsichtsbehörden ermöglicht (Art. 57 ff. E-DSGV).

Zur Sanktionierung ihrer Entscheidungen wird der Aufsichtsbehörde die Befugnis zur Verhängung von Geldstrafen eingeräumt, welche gemäss den Vorschriften der Grundverordnung gleichzeitig verhältnismässig und abschreckend zu sein haben. Dabei sieht der Vorschlag eine dreistufige Sanktionsandrohung vor: Bei Fällen ohne eigenwirtschaftliches Interesse oder bei kleinen Unternehmen kann bei einem ersten Verstoss auf eine Sanktion verzichtet und lediglich eine schriftliche Verwarnung vorgenommen werden. Für weitergehende Verstösse sollen je nach Schwere der Rechtsverletzung Geldbussen in unterschiedlicher Höhe (bis zu 1‘000‘000 Euro bzw. bei Unternehmen 2% des weltweiten Jahresumsatzes für die schwerwiegendsten Verletzungen) verhängt werden können. Der Verordnungsvorschlag sieht hierzu jeweils eine Liste von Verstössen pro Sanktionskategorie vor (Art. 79 Abs. 3–6), wobei sich die innere Logik der Kategorisierung

[30] Zusammenfassend zu den Neuerungen der DSGV im Bereich des Rechtsschutzes, HORNUNG, ZD 2012 (Fn. 19), 101 u. 105.

nicht immer unmittelbar erschliesst.[31] Das EU-Parlament hat in der ersten Lesung massgebliche Anpassungen der Bestimmung vorgenommen, wonach auf die Kategorisierung verzichtet und stattdessen eine Reihe von Faktoren verankert werden soll, welche für die Determinierung der Sanktion heranzuziehen wären, namentlich die Natur, Schwere und Dauer des Verstosses, die Höhe des verursachten Schadens, die zur Schadensminderung ergriffenen Massnahmen etc. Gemäss der Parlamentsversion der Vorschrift werden die schriftliche Verwarnung, regelmässige Betriebskontrollen sowie Bussen in der Höhe bis 100 Mio. Euro bzw. 5% des weltweiten Jahresumsatzes als mögliche Sanktionen vorgesehen (Art. 79 Abs. 2a–2c DSGV). Damit wurde im Parlament einerseits eine drastische Erhöhung des maximalen Sanktionsmasses vorgenommen und andererseits eine Entschlackung der Bestimmung, die allerdings unter dem Gesichtspunkt des Bestimmtheitsgebots in dieser offenen Formulierung mit einem derart weitgefassten Strafrahmen als problematisch zu betrachten ist.

Gegen die Entscheidungen von Aufsichtsbehörden steht den betroffenen Personen ein gerichtliches Beschwerderecht zu (Art. 74 Abs. 1 E-DSGV). Ebenso kann Beschwerde erhoben werden, falls eine Aufsichtsbehörde keine Entscheidung zum Schutze der betroffenen Person getroffen oder innert drei Monaten nach Eingang einer Beschwerde nicht über den weiteren Fortgang des Verfahrens informiert hat (Art. 74 Abs. 2 E-DSGV). Für die Behandlung der Beschwerde zuständig sind die Gerichte des Staates, in denen die betroffene mitgliedstaatliche Aufsichtsbehörde ihren Sitz hat (Art. 74 Abs. 3 E-DSGV). Ist die betroffene Person in einem anderen Staat ansässig, so besteht darüber hinaus die Möglichkeit, die Aufsichtsbehörde des Wohnsitzstaates zu ersuchen, in ihrem Namen gerichtlich gegen die zuständige Aufsichtsbehörde vorzugehen (Art. 74 Abs. 4 E-DSGV). Da hierzu jedoch keine Pflicht besteht und die Aufsichtsbehörden eher zögerlich sein dürften, gegen ihre Pendants in anderen Mitgliedstaaten vorzugehen, ist mit einer regen Nutzung dieser Möglichkeit wohl nicht zu rechnen.

### *2. Gerichtlicher Rechtsbehelf gegen für die Verarbeitung Verantwortliche*

Neben dem administrativen Rechtsbehelf schreibt die Grundverordnung den Mitgliedstaaten sodann neu auch ausdrücklich die Einrichtung eines gerichtlichen Beschwerdeweges gegen den Datenbearbeiter vor. Demnach steht natürlichen Personen das Recht zu, wegen Verletzungen der Verordnungsvorschriften bei der Verarbeitung ihrer persönlichen Daten an ein

[31] So ist etwa für die Verletzung der Informationspflicht gemäss Art. 12 Abs. 2 E-DSGV eine Geldbusse bis 250‘000 Euro vorgesehen, während das Unterlassen einer Information nach Art. 11 E-DSGV mit bis zu 500‘000 Euro sanktioniert werden kann, obschon sich diese Fälle inhaltlich jedenfalls teilweise überschneiden dürften. Auffallend ist auch, dass es überwiegend Verletzungen von administrativen Pflichten (Nichtfestlegung von internen Datenschutzstrategien oder einer Datenschutzfolgeabschätzung, Nichternennung eines Datenschutzbeauftragten) sind, die der schwersten Kategorie zugeordnet werden.

Gericht zu gelangen. Dieses Beschwerderecht besteht unabhängig von anderweitigen administrativen Behelfen (Art. 75 Abs. 1 E-DSGV) und kann somit auch parallel zu diesen ausgeübt werden. Zuständig sind wahlweise die Gerichte jenes Mitgliedstaates, in dem die für die Verarbeitung verantwortliche Person eine Niederlassung oder jene, in dem die betroffene Person ihren gewöhnlichen Aufenthalt hat. Eine Ausnahme gilt lediglich für hoheitliches Handeln von Behörden, das im entsprechenden Mitgliedstaat vor Gericht gebracht werden muss (Art. 75 Abs. 2 E-DSGV). Darüber hinaus steht auch jeder mitgliedstaatlichen Aufsichtsbehörde ein gerichtliches Klagerecht zu – mit dem Ziel, die Bestimmungen der Verordnung durchzusetzen (Art. 53 Abs. 3 und 76 Abs. 2 E-DSGV).

Zur Sicherstellung der Koordination der unterschiedlichen Verfahren innerhalb der Union sind zwei Mechanismen vorgesehen: Zum einen kann das Gericht Verfahren, die Gegenstand eines Kohärenzverfahrens sind, aussetzen, um den Ausgang des Kohärenzverfahrens abzuwarten. Ausgenommen sind dringliche Fälle (Art. 75 Abs. 3 E-DSGV). Zum zweiten besteht eine Aussetzungsmöglichkeit, wenn in einem anderen Mitgliedstaat Parallelverfahren laufen, welche dieselbe Massnahme, Entscheidung oder Vorgehensweise zum Gegenstand haben (Art. 76 Abs. 3 E-DSGV).

Ist der betroffenen Person durch rechtswidrige Handlungen ein Schaden entstanden, so kann vor Gericht ein Anspruch auf Schadenersatz geltend gemacht werden. Haftbar ist der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter. Sind mehrere Personen beteiligt, so haften diese gesamtschuldnerisch für den gesamten Schaden. Eine Haftungsbefreiung bedarf des Nachweises, dass dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter die Schadensursache nicht zur Last gelegt werden kann. Inhaltlich betrachtet ist die Haftungsbestimmung recht vage formuliert und lässt – auch in Verbindung mit den materiellen Vorschriften der Verordnung – zahlreiche Belange, wie etwa jene nach der Deckung immaterieller Schäden, offen.[32] Damit kann die Frage aufgeworfen werden, ob die Vorschrift überhaupt eine taugliche Grundlage für entsprechende Haftungsklagen darstellt und wenn ja, inwieweit sie sich als Basis für die Schaffung einer unionsweit einheitlichen Rechtsprechung in diesen Belangen eignet.

Schliesslich werden die Gerichte ermächtigt, wegen Verletzungen der Datenschutzvorschriften Sanktionen zu verhängen (Art. 78 E-DSGV). Diese sind von den Mitgliedstaaten in nationalen Rechtsvorschriften zu verankern, wobei keine Harmonisierung der Sanktionen vorgesehen ist. Der unionsrechtliche Standard gibt lediglich vor, dass die Sanktionen „wirksam, verhältnismässig und abschreckend" sein müssen. Haben nicht in der Union

[32] Mit kritischen Einschätzungen auch das Schrifttum: JOCHEN SCHNEIDER/NIKO HÄRTING, Wird der Datenschutz nur endlich internettauglich?, ZD 2012, 202 f. und DEHMEL/HULLEN, (Fn. 24), 152; skeptisch in Bezug auf die Ausgestaltung als Verschuldenshaftung, ALEXANDER ROSSNAGEL/MAXI NEBEL/PHILIPP RICHTER, Besserer Internetdatenschutz für Europa, ZD 2013, 108.

niedergelassene Datenverarbeiter gemäss Art. 25 E-DSGV einen Vertreter ernannt, so entfalten die Sanktionen gegenüber diesem Wirkung, ansonsten werden Sanktionen und Massnahmen direkt verhängt.

*3. Verbandsbeschwerde*

Eine wesentliche Neuerung der Grundverordnung ist die Schaffung einer Verbandsklage. Mit diesem Instrument stünde Einrichtungen, Organisationen und Verbänden, die sich den Schutz von personenbezogenen Daten „zum Ziel gesetzt haben" (Vorschlag EU-Kommission) bzw. im öffentlichen Interesse tätig sind (Erste Lesung EU-Parlament), das Recht zu, entweder im Namen einer oder mehrerer Personen oder unabhängig von einer konkreten Beschwerde, die Verletzung der datenschutzrechtlichen Vorschriften einer mitgliedsstaatlichen Aufsichtsbehörde vorzulegen (Art. 73 Abs. 2 und 3 E-DSGV). Sodann soll diesen Einrichtungen, Organisationen und Verbänden auch das Recht zukommen, im Namen (und Auftrag) betroffener Personen Entscheidungen einer Aufsichtsbehörde den Gerichten vorzulegen oder gegen einen Datenverarbeiter direkt eine gerichtliche Klage zu erheben (Art. 76 Abs. 1 E-DSGV). Nicht vorgesehen ist hingegen die Ermächtigung, ein gerichtliches Verfahren unabhängig von der Beschwerde einer betroffenen Person anzustreben.

Die Verbandsbeschwerde im Bereich des Datenschutzes ist als interessantes Instrument zu werten. Zum einen kann sie – gerade wenn die Wahrnehmung von Beschwerderechten natürlicher Personen in Frage steht – ein Mittel darstellen, um der typischerweise bestehenden faktischen Ungleichheit zwischen Datenverarbeiter und betroffener Person ein Gegengewicht entgegenzuhalten. Zum anderen kann sie dazu dienen, die für den Einzelnen möglicherweise nicht als „beschwerdewürdig" qualifizierten Datenschutzinteressen zu bündeln und auf dem Beschwerdeweg einzufordern.

## V. Zusammenfassend: zu den Stossrichtungen der Reform

In Bezug auf das Durchsetzungsinstrumentarium des Datenschutzrechts lassen sich bei der Datenschutzgrundverordnung zusammenfassend folgende Leitlinien ausmachen:

- *Mechanismen frühzeitiger Umsetzung*: Der Umstand, dass die Rechtsdurchsetzung im Datenschutzbereich besondere Schwierigkeiten bereitet, und die Erkenntnis, dass die datenschutzrechtlichen Grundsätze im Prozess der Datenbearbeitung möglichst früh Berücksichtigung finden sollten, haben im Grundverordnungsvorschlag mit den vorgesehenen Mechanismen zur frühzeitigen Rechtsdurchsetzung eine Umsetzung erfahren. Durch diese Vorwegnahme der Rechtsdurchsetzung soll Rechtsverletzungen vorgebeugt und damit vermieden werden, dass zu einem späteren Zeitpunkt auf die Mittel formeller Rechtsdurchsetzung

zurückgegriffen werden muss. Die Ernennung unternehmens- und behördeninterner Datenschutzbeauftragter (Art. 35 ff. E-DSGV) auf der institutionellen Ebene, aber auch die Pflicht zur Durchführung von Datenschutz-Folgeabschätzungen (Art. 33 E-DSGV), die Zertifizierungsverfahren (Art. 39 E-DSGV), der Grundsatz des Datenschutzes durch Technik sowie der datenschutzfreundlichen Voreinstellungen (Art. 23 E-DSGV) verfolgen – im Sinne einer antizipierten Rechtsdurchsetzung – den Zweck, dem Datenschutzrecht möglichst frühzeitig Beachtung zu verschaffen.

- *Institutionelle Stärkung*: Die Verbesserung der Umsetzung des Datenschutzrechts und der Einheitlichkeit der Rechtsumsetzung soll über die Verankerung bzw. Stärkung einer Reihe von behördlichen Aufgabenträgern erfolgen, die künftig in den Mitgliedstaaten, in Zusammenarbeit zwischen den Mitgliedstaaten sowie insbesondere in enger Abstimmung mit der EU-Kommission das europäische Datenschutzrecht anwenden und durchsetzen sollen. Zur Sicherstellung dieser Aufgabe sollen die mitgliedstaatlichen Behörden mit einem unabhängigen Status, breitgefassten Aufgaben, weitreichenden Kompetenzen sowie mit ausreichenden finanziellen und personellen Mitteln ausgestattet werden.
- *Kooperationsansatz*: Die Verankerung der Amtshilfe, die Schaffung einer Rechtgrundlage für gemeinsame Massnahmen der Aufsichtsbehörden, die Regelung des Umgangs mit gerichtlichen Parallelverfahren sowie insbesondere die Einrichtung des Kohärenzverfahrens sind Ausdruck des Bestrebens, in der Umsetzung des materiellen Datenschutzrechts eine engere Kooperation zwischen den beteiligten Akteuren zu erreichen. Damit soll ein eigentlicher europäischer Behördenverbund im Datenschutzbereich etabliert werden. Im Zentrum dieses Gefüges findet sich die mit weitreichenden Rechtssetzungs-, Überwachungs- und Vollzugskompetenzen ausgestattete EU-Kommission, welche damit zum eigentlichen Protagonisten des Datenschutzrechts avancieren würde. Demzufolge wohnt dem Kooperationsansatz gleichzeitig eine beträchtliche Zentralisierungstendenz inne.
- *Depersonalisierung der Rechtdurchsetzung:* Bei der Rechtsdurchsetzung würde der Vorschlag für eine Datenschutzgrundverordnung die Möglichkeit einer Entpersonalisierung mit sich bringen, in dem Sinne, dass die Beschwerdeführung künftig auch durch Organisationen, Einrichtungen und Verbände oder gegebenenfalls durch die mitgliedstaatliche Aufsichtsbehörde statt durch die betroffenen Personen selbst erfolgen könnte. Dies mutet insofern etwas paradox an, als doch vorliegend gerade die Durchsetzung von Persönlichkeitsrechten in Frage steht, die in manchen Rechtsordnungen zudem aus dem Konzept der informationellen Selbstbestimmung hergeleitet werden. Vor dem Hintergrund der Schwierigkeiten bei der Durchsetzung dieser Ansprüche

erscheint dieser Ansatz jedoch durchaus zielführend.[33] Zudem wird der Entscheid über eine Vertretung bei der Rechtsdurchsetzung selbstredend der betroffenen Person überlassen.[34]

- *Kollektivierung der Rechtsdurchsetzung:* Mit der Depersonalisierung im Zusammenhang stehend eröffnet die Verbandsbeschwerde die Möglichkeit, einerseits zu einer Bündelung der Beschwerden unterschiedlicher betroffener Personen zu einer Kollektivbeschwerde und andererseits zu einer Geltendmachung öffentlicher Interessen im Bereich des Datenschutzes. Damit wird gewissermassen die Summe der oftmals zwischen zahlreichen betroffenen Personen oder der gesamten Öffentlichkeit fragmentierten Interessen gebildet, welche gegenüber den – finanziellen und zeitlichen – Hürden einer Beschwerdeerhebung eher überwiegt als dies für die Interessen einer Einzelperson der Fall wäre.

# D. Zu den Implikationen für die Schweiz

## I. Zur Übernahmepflicht

Die Relevanz des geltenden und zukünftigen EU-Datenschutzrechts für die Schweiz ist wie oben dargetan[35] eine doppelte: Zum einen besteht auf der Grundlage der sektoriellen Abkommen zwischen der Europäischen Union und der Schweiz teilweise eine Pflicht zur Übernahme bestimmter Vorschriften ins schweizerische Recht, und zum anderen kann das Unionsrecht teilweise als Inspirationsquelle für die Schaffung neuer datenschutzrechtlicher Instrumente und die Weiterentwicklung des Datenschutzrechts in der Schweiz herangezogen werden.

Die Richtlinie 95/46 ist demzufolge für die Schweiz grundsätzlich von Relevanz, unabhängig davon, ob lediglich die Sachbereiche von Schengen und Dublin oder mangels entsprechender Einschränkungen in den Assoziierungsabkommen sämtliche Rechtsbereiche erfasst sind.[36] Der schweizerische Gesetzgeber beschränkte die Umsetzung im Grundsatz auf die Bereiche von

---

[33] Dass die kollektive Geltendmachung von Persönlichkeitsrechten durchaus keinen Widerspruch darstellen muss, zeigt auch Art. 89 ZPO, wonach die (allgemeine) Verbandsklage im schweizerischen Recht gerade auf Persönlichkeitsrechtsverletzungen beschränkt wird.

[34] Dahingehend die im EU-Parlament erfolgte Präzisierung von Art. 76 Abs. 1 E-DSGV, wonach die gerichtliche Klageerhebung durch eine Einrichtung, Organisation oder einen Verband eine Beauftragung durch die betroffene Person voraussetzt.

[35] Vgl. oben A.

[36] Für einen Überblick des Meinungsstandes mit zahlreichen weiteren Nachweisen vgl. EPINEY/SCHLEISS, in: Belser/Epiney/Waldmann, Datenschutzrecht (Fn. 9), § 4, Rn. 279 sowie oben A.

Schengen und Dublin[37] und folgte somit einem restriktiven Ansatz, welcher im Rahmen der Schengen-Evaluation im Resultat für ausreichend befunden wurde.[38] Gleichzeitig vollzog der Gesetzgeber jedoch insgesamt eine gewisse Annäherung des Datenschutzrechts an das Unionsrecht[39] und entschied sich bei der Übernahme des Rahmenbeschlusses 2008/977/JI jedenfalls teilweise für eine über den Schengen-Bereich hinausgehende Umsetzung[40].

Die künftige Datenschutzgrundverordnung sowie insbesondere die Datenschutzrichtlinie im Bereich der Strafverfolgung stellen im Grundsatz eine Weiterentwicklung des Schengen- bzw. Dublin-Besitzstandes dar und dürften als solche, jedenfalls soweit „dublin-" bzw. „schengen-"relevante Daten und Datenbearbeitungsvorgänge betroffen sind, einer Übernahmepflicht unterstehen.[41] Da nun mit der Datenschutzgrundverordnung jedoch das Datenschutzrecht innerhalb der EU einer vollständigen Harmonisierung unterzogen werden soll, stellt sich durchaus die Frage, ob es für die Schweiz nicht angebracht sein könnte, die Vorschriften der Verordnung vollständig ins nationale Recht zu übernehmen, um damit für einen einheitlichen Rechtsstandard zu sorgen. Dafür dürfte insbesondere auch der Umstand sprechen, dass sich der räumliche Anwendungsbereich der geplanten Verordnung neben den in der EU ansässigen Personen auch auf jene Personen erstrecken soll, deren Datenverarbeitung dazu dient, „Personen in der Union Waren oder Dienstleistungen anzubieten" oder das Verhalten von Personen in der Union zu beobachten (Art. 3 Abs. 2 E-DSGV). Somit könnten Datenbearbeitungsvorgänge in der Schweiz künftig durchaus auch dem Unionsrecht unterstehen und müssten bei einer divergierenden Rechtslage den doppelten Schutzstandard erfüllen. Vor diesem Hintergrund ist davon auszugehen, dass sich die Relevanz des Datenschutzrechts der EU für die Schweiz in Zukunft eher noch verstärken wird.

---

37 BBl 2004 5965, 6175.

38 Vgl. dazu den Beschluss des Rates vom 27. November 2008 über die vollständige Anwendung der Bestimmungen des Schengen-Besitzstandes in der Schweizerischen Eidgenossenschaft, insb. Erwägung 4.

39 Vgl. Botschaft zur Änderung des DSG und zum Bundesbeschluss betreffend den Beitritt der Schweiz zum Zusatzprotokoll vom 8. November 2001 zum Übereinkommen zum Schutz der Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung (BBl 2003 2102, 2110) sowie die entsprechenden Ausführungen in der Botschaft zur Genehmigung der Bilateralen II (BBl 2004 5965, 6175).

40 Anwendung der geschaffenen Regeln auf sämtliche Datenbearbeitungen durch Bundesorgane statt bloss auf die Bekanntgabe von Daten im Rahmen der Zusammenarbeit von Schengen: BBl 2009 6749, 6769 f.

41 Vgl. Erwägung 137 E-DSGV sowie Erwägung 78 Vorschlag für eine Datenschutzrichtlinie im Bereich Strafverfolgung.

## II. Zu möglichen Übernahmeinhalten

Ausgehend von diesen Feststellungen zur jedenfalls teilweise bestehenden Übernahmepflicht der unionsrechtlichen Vorschriften im Datenschutzbereich soll im Folgenden kurz auf bestehende und insbesondere sich abzeichnende künftige Divergenzen zwischen schweizerischem Recht und Unionsrecht im Hinblick auf die Durchsetzungsmechanismen des Datenschutzrechts eingegangen werden.

### *1. Aus dem geltenden Unionsrecht*

In Bezug auf das geltende Unionsrecht – also insbesondere die Richtlinie 95/46 sowie den Rahmenbeschlusses 2008/977/JI – war der Abgleich mit dem schweizerischen Datenschutzrecht schon vermehrt Gegenstand von Untersuchungen in Wissenschaft und Praxis.[42] Dabei bestehen im materiellen Recht weiterhin gewisse Unterschiede, etwa bei der genauen Definition des datenschutzrechtlichen Anwendungsbereiches (Art. 3 RL 95/46), dem grundsätzlichen Verbot der Bearbeitung gewisser sensibler Personendaten (Art. 8 Abs. 1 RL 95/46), den Anforderungen an die Einwilligung (Art. 7 Bst. a RL 95/46), dem Verbot automatisierter Entscheidungen (Art. 15 RL 95/46) oder dem Widerspruchsrecht zur Verwendung von Daten zum Zwecke der Direktwerbung (Art. 14 Bst. b RL 95/46).[43]

Was die *gerichtlichen Durchsetzungsmechanismen* anbelangt, sieht das schweizerische Recht mit dem Verweis von Art. 15 DSG auf Art. 28, 28a und 28l ZGB Klagerechte vor,[44] um drohende Verletzungen zu verbieten, bestehende Verletzungen zu beseitigen, die Verletzung festzustellen,[45] die Mitteilung und Veröffentlichung einer Berichtigung oder eines Urteils an Dritte zu erlangen,[46] einen Bestreitungsvermerk durchzusetzen,[47] ein Gegendarstellungsrecht zu erhalten[48] oder vorsorgliche Massnahmen zu erwirken.[49]

---

[42] Mit weiteren Hinweisen, vgl. EPINEY, Zu den völker- und europarechtlichen Rahmenbedingungen der Revision des Datenschutzgesetzes (Fn. 9), 5 ff.; vgl. seitens der EU bereits die Entscheidung der Kommission vom 26. Juli 2000 gemäss der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz, ABl. 2000 L 215 sowie der Beschluss des Rates vom 27. November 2008 über die vollständige Anwendung der Bestimmungen des Schengen-Besitzstandes in der Schweizerischen Eidgenossenschaft sowie seitens der Schweiz, BBl 2009 6749, 7665 ff. und bezüglich des Übernahmebedarfs aufgrund des Rahmenbeschlusses 2008/977/JI, BBl 2003 2101, 2117 f.

[43] Siehe dazu BBl 2003 2101, 2117 f. sowie EPINEY, Zu den völker- und europarechtlichen Rahmenbedingungen der Revision des Datenschutzgesetzes (Fn. 9), 5 ff.

[44] Eingehend hierzu etwa DAVID ROSENTHAL, in: Handkommentar DSG, Art. 15 N 14 ff.; CORRADO RAMPINI, Basel Kommentar DSG, 2. Aufl., Art. 15 N 7 ff.

[45] Art. 15 DSG i.V.m. Art. 28a ZGB.

[46] Art. 15 Abs. 3 DSG.

[47] Art. 15 Abs. 2 DSG.

[48] Art. 15 DSG i.V.m. Art. 28l ZGB.

[49] Art. 15 DSG i.V.m. Art. 28 ZGB und Art. 261 ff. ZPO.

Zulässig sind sodann Klagen auf Schadenersatz und Genugtuung sowie auf Gewinnherausgabe.[50] Schliesslich wird die Verletzung der Auskunfts-, Informations- und Mitteilungspflicht durch private Personen sowie die Verletzung der beruflichen Schweigepflicht unter Strafe gestellt (Art. 34 f. DSG). Mit diesen Klagemöglichkeiten dürfte den Anforderungen von Art. 20 (Rechtsbehelfe) und Art. 24 (Sanktionen) Rahmenbeschluss 2008/977/JI sowie von Art. 22 (Rechtsbehelfe), Art. 23 (Haftung) und Art. 24 (Sanktionen) von Richtlinie 95/46 jedenfalls im Grundsatz Genüge getan sein.

An *aussergerichtlichen Mechanismen* sieht das schweizerische Recht die Möglichkeit vor, den EDÖB mittels Mitteilung dazu anzuhalten, einen Sachverhalt in Bezug auf die Datenbearbeitung durch die Bundesorgane (Art. 27 Abs. 2 DSG) bzw. durch Privatpersonen (Art. 29 Abs. 1 DSG) abzuklären. Letzteres steht unter der Voraussetzung, dass die Methoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (Systemfehler), die Registrierung von Datensammlungen in Frage steht oder eine Informationspflicht besteht. Dazu verfügt der EDÖB über recht weitreichende Untersuchungsbefugnisse (Art. 27 Abs. 3 sowie Art. 29 Abs. 2 DSG) und kann gestützt auf die erfolgten Abklärungen Empfehlungen an das zuständige Bundesorgan oder den privaten Datenbearbeiter richten (Art. 27 Abs. 4 und Art. 29 Abs. 3 DSG). Werden Empfehlungen an Bundesorgane nicht befolgt oder abgelehnt, so steht dem EDÖB die Kompetenz zu, die Angelegenheit dem Departement oder der Bundeskanzlei zum Entscheid vorzulegen. Dieser Entscheid kann von betroffenen Personen und nun auch vom EDÖB bei der Beschwerdebehörde und anschliessend beim Bundesverwaltungsgericht angefochten werden (27 Abs. 6 i.V.m. Art. 33 DSG).[51] Wird eine Empfehlung im Privatrechtsbereich nicht befolgt oder abgelehnt, so steht dem EDÖB die Kompetenz zu, die Angelegenheit dem Bundesverwaltungsgericht zu unterbreiten (Art. 29 Abs. 4 i.V.m. Art. 33 DSG). Den privaten Adressaten steht die Möglichkeit offen, die Empfehlung mittels verwaltungsrechtlicher Klage gemäss Art. 35 Bst. b VGG dem Bundesverwaltungsgericht vorzulegen.[52] Kontrastiert man nun die Ausgestaltung der Durchsetzungsmechanismen in der Schweiz mit den Anforderungen des Unionsrechts, so erscheint die Vereinbarkeit der beiden Ordnungen jedenfalls weitgehend gegeben. So dürfte etwa die weit formulierte Kompetenz des Datenschutzbeauftragten zur Empfehlung, das Bearbeiten von Daten „zu ändern oder zu unterlassen“ (Art. 27 Abs. 4 bzw. Art. 29 Abs. 3 DSG), die in der Datenschutzrichtlinie ausführlicher aufgeführten Kompetenzen (Art. 28 Abs. 3 2. Spiegelstrich RL 95/46; Art. 25 Abs. 2 Bst. b Rahmenbeschluss

---

[50] Art. 15 Abs. 1 i.V.m. Art. 28a Abs. 3 ZGB sowie Art. 41 ff. OR (Schadenersatz), Art. 49 OR (Genugtuung) und Art. 423 OR (Gewinnherausgabe).

[51] Die Beschwerdemöglichkeit des EDÖB war eingeführt worden, um das schweizerische Recht mit den entsprechenden Vorgaben des Zusatzprotokolls zum STE 108 (Art. 1 Ziff. 2 Bst. a; SR 0.235.11) bzw. den Vorschriften im Unionsrecht (Art. 28 Abs. 3 3. Spiegelstrich RL 95/46) in Übereinstimmung zu bringen: BBl 2003 2101, 2115.

[52] DAVID ROSENTHAL, in: Handkommentar DSG, Art. 29 N 42.

2008/977/JI) jedenfalls in ihrer inhaltlichen Breite mit umfassen und somit dem geltenden unionsrechtlichen Standard entsprechen. Selbiges gilt nun, wie erwähnt, auch für die Kompetenz der Behörde, Verstösse gegen die datenschutzrechtlichen Vorschriften den Gerichten zu unterbreiten (Art. 28 Abs. 3 4. Spiegelstrich RL 95/46 sowie Art. 25 Abs. 2 Bst. c Rahmenbeschluss 2008/977/JI). Nicht dem Standard des Unionsrechts entsprechen dürfte hingegen die Verengung der Zuständigkeit des EDÖB im Privatrechtsbereich auf Systemfehler (Art. 29 Abs. 1 Bst. a DSG). Vielmehr ergäbe sich aus dem Unionsrecht das Recht der betroffenen Personen, mit jeglichen Verstössen gegen datenschutzrechtliche Vorschriften an die Kontrollstelle zu gelangen (Art. 28 Abs. 4 RL 95/46; Art. 25 Abs. 3 Rahmenbeschluss 2008/977/JI). Dabei kommt der Behörde jeweils ausdrücklich die Pflicht zu, die betroffene Person darüber zu informieren, wie mit der Eingabe verfahren wird. Zudem ist zu bezweifeln, ob die Kompetenz des EDÖB, Empfehlungen an die Adresse von Bundesorganen oder privaten Datenbearbeitern abzugeben, den Anforderungen des Unionsrechts entspricht. Empfehlungen gemäss Art. 27 Abs. 4 bzw. Art. 29 Abs. 3 DSG sind nicht rechtsverbindlich und können demzufolge nicht mit Verwaltungszwang durchgesetzt werden.[53] Auch die Möglichkeit, des EDÖB, die Angelegenheit bei Nichtbefolgung oder Ablehnung in behördlichen Belangen dem Departement oder der Bundeskanzlei zum Entscheid vorzulegen und gegen diesen Entscheid gegebenenfalls bei den Bundesbehörden Beschwerde zu führen (Art. 27 Abs. 5 und 6 i.V.m. Art. 33 DSG) bzw. im Privatrechtsbereich dem Bundesverwaltungsgericht zum Entscheid vorzulegen (Art. 29 Abs. 4 DSG i.V.m. Art. 33 DSG), vermag nichts an der Tatsache zu ändern, dass die Empfehlungen des EDÖB als solche nicht rechtsverbindlich ausgestaltet sind. Dies dürfte mit dem geltenden europäischen Standards kaum in Einklang stehen, ist die Kontrollstelle doch mit der Befugnis auszustatten, „die Sperrung, Löschung oder Vernichtung von Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung *anzuordnen*".[54] Vorausgesetzt wird somit die Befugnis für rechtsverbindliche Entscheidungen. Demzufolge würden sich in dieser Hinsicht für eine vollständige Übernahme des geltenden Unionsrechts im schweizerischen Recht Anpassungen aufdrängen.

### *2. Aus dem künftigen Unionsrecht*

#### *a) Allgemeines*

Mit dem Erlass der Datenschutzgrundverordnung und der Datenschutzrichtlinie im Bereich Strafverfolgung würde sich die Frage nach dem Anpassungsbedarf im schweizerischen Recht stellen. Im Folgenden soll nun das künftige Unionsdatenschutzrecht auf der Grundlage der Vorschläge der EU-

[53] BBl 1998 II 413, 480; VPB 69.106, E. 4.2; YVONNE JÖHRI, in: Handkommentar DSG, Art. 27 N 13 f.; DAVID ROSENTHAL, in: Handkommentar DSG, Art. 29 N 26; PHILIPPE MEIER, Protection des données, 2011, 617.

[54] Art. 28 Abs. 3 3. Spiegelstrich RL 95/46, Hervorhebung hinzugefügt.

Kommission dem schweizerischen Recht im Hinblick auf die Durchsetzungsmechanismen gegenübergestellt werden. Dabei kann lediglich ein ungefährer und punktueller Abgleich vorgenommen werden, insbesondere auch vor dem Hintergrund, dass sich die unionsrechtlichen Erlasse im laufenden Gesetzgebungsprozess befinden und ihre letztliche Ausgestaltung somit noch nicht endgültig absehbar ist.

*b) Beschwerdebehelfe*

Nachdem das schweizerische Recht für betroffene Personen sowohl gerichtliche als auch administrative Behelfe zur Durchsetzung des Datenschutzrechts kennt und dem EDÖB nunmehr auch die Möglichkeit einräumt, mögliche Verstösse vor die Gerichte zu bringen, erscheint der diesbezügliche Anpassungsbedarf im Hinblick auf das künftige Unionsrecht eher begrenzt. Zu erwähnen ist immerhin die noch eingehender zu besprechende Verbandsbeschwerde sowie die schon in Bezug auf das bestehende Recht festgestellte Divergenz aufgrund der Beschränkung der Zuständigkeit des EDÖB (Art. 29 Abs. 1 Bst. a DSG). Diese Kompetenzverengung hat, wie bereits angesprochen, zur Konsequenz, dass die Aufsichtsbehörde sich nicht um sämtliche Verstösse zu kümmern hat, womit der administrative Rechtsschutz diesbezüglich hinter den Vorgaben des geltenden und künftigen Unionsrechts zurückbleibt. Darüber hinaus zu klären wäre eine Reihe von Einzelfragen in der Übernahme, wie etwa jene nach der Möglichkeit von Organisationen, Einrichtungen und Verbänden im Namen einer oder mehrerer Personen bei der nationalen Aufsichtsbehörde Beschwerde einzureichen (Art. 73 Abs. 2 E-DSGV),[55] die Kompetenz der nationalen Aufsichtsbehörden, im Namen einer in ihrem Staat ansässigen Person gegen die zuständige Aufsichtsbehörde in einem anderen Staat Klage zu erheben (Art. 74 Abs. 4 E-DSGV) oder die Möglichkeit, Gerichtsverfahren im Falle von Parallelverfahren in anderen Staaten auszusetzten (Art. 76 Abs. 3 E-DSGV). Die Umsetzung dieser Mechanismen hängt vom anzustrebenden Integrationsgrad in die europäische Datenschutzordnung ab.[56] Bereits in Übereinstimmung mit dem Unionsrecht (Art. 75 Abs. 2 E-DSGV) ist hingegen die Regelung des Gerichtsstandes gemäss Art. 20 Bst. d ZPO, wonach bei Klagen und Begehren im Datenschutzbereich wahlweise das Gericht am Wohnsitz oder am Sitz einer der beiden Parteien zuständig ist.

---

[55] Hierbei ist die Postulationsfähigkeit angesprochen, wobei gemäss Art. 68 ZPO bereits unter geltendem Recht die Möglichkeit bestehen dürfte, einen Vertreter mit der Prozessvertretung zu betrauen. Im Hinblick auf eine Übernahme zu überlegen wäre erstens, ob diese Möglichkeit auch in den datenschutzrechtlichen Grundlagen noch ausdrücklich erwähnt werden sollte und zweitens, ob die Liste der zur berufsmässigen Vertretung befugten Personen und Einrichtungen (Art. 68 Abs. 2 ZPO) zur Klarstellung zu ergänzen wäre.

[56] Vgl. dazu unten D.II.2d).

*c) Kompetenzen der Aufsichtsbehörde*

Würde das neue europäische Datenschutzrecht gemäss dem Vorschlag der EU-Kommission ins schweizerische Recht übernommen, so ergäbe sich im Hinblick auf die Kompetenzen der Aufsichtsbehörden in verschiedener Hinsicht Anpassungsbedarf: Zunächst ist die Beschränkung der Rechtsdurchsetzung des EDÖB auf den Erlass von *Empfehlungen* wie bereits angesprochen, mit dem Standard des heutigen Unionsrechts kaum zu vereinbaren. Mit der Stossrichtung des künftigen Rechts, die darin besteht, die Aufsichtsbehörden in Anlehnung an die Befugnisse der Wettbewerbsbehörden mit umfassenden Zwangsbefugnissen auszustatten,[57] wäre diese Ausgestaltung der aufsichtsrechtlichen Kompetenzen sodann klarerweise unvereinbar. Selbiges gilt für die Ermächtigung der Aufsichtsbehörden, *Zugang zu den Geschäftsräumen* einschliesslich der Datenverarbeitungsanlagen und -geräte zu erlangen (Art. 53 Abs. 2 Bst. b E-DSGV), die heute dem EDÖB nicht zusteht.[58] Schliesslich sollen den Aufsichtsbehörden gemäss der Richtlinie weitgehende *Sanktionskompetenzen* zuerkannt werden (Art. 53 Abs. 4 i.V.m. Art. 79 Abs. 4–6 E-DSGV), wogegen dem EDÖB unter geltendem schweizerischem Recht keine Kompetenz zukommt, gegenüber den Datenverarbeitern überhaupt rechtsverbindliche Entscheidungen zu fällen. Die gesetzlich vorgesehenen Strafbestimmungen (Art. 34 und 35 DSG) sind von den Strafbehörden durchzusetzen.[59] Demzufolge würde eine Übernahme dieser unionsrechtlichen Vorschriften ins nationale Recht die Verankerung einer detaillierten gesetzlichen Sanktionsgrundlage einschliesslich einer dem Bestimmtheitsgebot genügenden Tatbestandsregelung bedingen.

*d) Zusammenarbeit der Aufsichtsbehörden*

Weniger einfach zu bewerkstelligen wäre hingegen die Einbindung der schweizerischen Aufsichtsbehörde in das zu schaffende kooperative Behördengefüge auf Unionsebene. Entscheidend für das zu wählende Einbindungsmodell dürfte dabei der angestrebte Grad der Integration der Schweiz in die europäische Datenschutzordnung sein:

(1) Für eine vollumfängliche Anbindung an das europäische Recht mit umfassendem Einbezug in die behördlichen Strukturen wäre ohnehin ein sektorielles Abkommen zwischen der Schweiz und der EU von Nöten, in dessen Rahmen auch die Frage der behördlichen Einbindung und die Kooperationsmechanismen zu regeln wären.

(2) Wird hingegen eine Anlehnung an das materielle Recht ohne vollständige Einbindung in den unionsrechtlichen Rahmen angestrebt, so erschiene – die Zustimmung beider Vertragsparteien wiederum vorausgesetzt

---

[57] Vgl. dazu insbesondere Art. 53 Abs. 4 i.V.m. Art. 79 Abs. 4 bis 6 E-DSGV.

[58] Art. 29 Abs. 2 DSG; vgl. hingegen Art. 42 Abs. 2 KG: BBl 1995 I 468, 615 f. sowie BBl 2002 2022, 2044.

[59] Vgl. zum Ganzen FRANZ RIKLIN, Basler Kommentar DSG, Vor 7. Abschnitt, N 1 ff., mit dem Hinweis auf die empirische Bedeutungslosigkeit der Bestimmungen.

– eine institutionelle Zusammenarbeit gestützt auf ein Kooperationsabkommen denkbar. Dabei kann der Bereich des Wettbewerbsrechts und die Kooperation der Wettbewerbsbehörden als Beispiel dienen, wo gegenwärtig mit dem Abkommen zwischen der Schweiz und der EU über die Zusammenarbeit bei der Anwendung ihrer Wettbewerbsrechte ein ähnliches Kooperationsmodell verwirklicht wird.[60]

(3) Als Minimalvariante wäre schliesslich eine unilaterale Ausrichtung des schweizerischen Rechts auf die europäischen Vorgaben ohne institutionelle Verknüpfung denkbar. Dabei stellt sich die Frage, inwieweit in dieser Konstellation selbst bei weitgehender oder vollständiger Übernahme des materiellen Rechts überhaupt eine Erfüllung der europäischen Datenschutzstandards gegeben wäre, stellen doch die geplanten Kooperationsmechanismen in der Rechtsdurchsetzung ein gewichtiges Element der Garantien des Unionsrechts dar.

Selbst in einer solchen Minimalvariante wäre die Verankerung nationaler Regelungen in Bezug auf die Amtshilfe (Art. 55 E-DSGV) und die Durchführung gemeinsamer Massnahmen der Aufsichtsbehörden (Art. 56 E-DSGV) wünschenswert. Würde ein Zusammenarbeitsabkommen angestrebt, könnte die entsprechende Anbindung darüber hinaus verpflichtend ausgestaltet werden. Jedenfalls erforderlich dürfte ein solches völkerrechtliches Abkommen für die Einbindung der Schweiz in die Behördenkooperation im Rahmen des geplanten Kohärenzverfahrens (Art. 57 ff. E-DSGV), im Hinblick auf die Mitwirkung der Schweiz am Europäischen Datenschutzausschuss (Art. 64 ff. E-DSGV) sowie zur Umsetzung der Aussetzung von Gerichtsverfahren bei laufenden Parallelverfahren (Art. 76 Abs. 3 E-DSGV) sein. Dabei ist zu erwarten, dass die Einräumung von formellen Mitwirkungsrechten im Europäischen Datenschutzausschuss wohl eine vollständige Übernahme des Datenschutz-*acquis* der Union sowie den Einbezug in das geplante Kohärenzverfahren voraussetzen würde. Die Integration in das Kohärenzverfahren bedeutet aber gleichzeitig in einem gewissen Masse eine Unterstellung der Aufsichtsbehörde unter die EU-Kommission und würde folglich eine Einbusse nationaler Kompetenzen nach sich ziehen. Beim Entscheid über eine entsprechende behördliche Anbindung müssten diese Kompetenzverluste gegen die Vorteile einer effizienteren Rechtsdurchsetzung im Rahmen der Kooperationsmechanismen abgewogen werden.

---

[60] Abkommen vom 17. Mai 2013 zwischen der Schweizerischen Eidgenossenschaft und der Europäischen Union über die Zusammenarbeit bei der Anwendung ihres Wettbewerbsrechts: BBl 2013 3985 sowie die entsprechende Botschaft: BBl 2013 3959. Das EU-Parlament hat dem Abkommen an der Sitzung vom 5. Februar 2014 zugestimmt (P7_TA-PROV(2014)0078). Mit Bundesbeschluss vom 20. Juni 2014 wurde dem Bundesrat unter Vorbehalt eines Referendums die Ermächtigung zur Ratifikation des Abkommens erteilt: BBl 2014 5205.

*e) Verbandsklage*

Das Unionsrecht soll künftig sowohl vor den Aufsichtsbehörden als auch vor den Gerichten das Instrument der Verbandsbeschwerde vorsehen (Art. 73 Abs. 2 und 3 sowie Art. 76 Abs. 1 E-DSGV). Dagegen kennt das schweizerische Datenschutzrecht zum heutigen Zeitpunkt kein spezifisches Verbandsbeschwerderecht.[61] Möglich ist hingegen eine Klage gemäss Art. 89 ZPO, wonach Vereinen oder anderen Organisationen von gesamtschweizerischer oder regionaler Bedeutung ein Klagerecht zukommt, um Verletzungen der Persönlichkeitsrechte von Personengruppen geltend zu machen, sofern sie gemäss ihren Statuten zur Wahrung der Interessen dieser Gruppen befugt sind.[62] Einklagbare Ansprüche sind dabei das Verbot drohender Verletzung, die Beseitigung bestehender Verletzung oder die Feststellung der Widerrechtlichkeit einer Verletzung der Persönlichkeit. Nicht möglich ist hingegen die Einforderung von Schadenersatz, Genugtuung oder Gewinnherausgabe, welche somit grundsätzlich der individuellen Rechtsdurchsetzung überlassen bleibt.[63] Möglich ist zudem eine Abtretung der entsprechenden Forderungen an einen Verband, welcher diese sammeln und mittels objektiver Klagenhäufung (Art. 90 ZPO) geltend machen könnte. Dieses Vorgehen hat allerdings in der Praxis kaum Bedeutung erlangt.[64] Somit dürfte die geltende Rechtlage in der Schweiz hinter den sich abzeichnenden Anforderungen des Unionsrechts zurückbleiben, und entsprechend wären bei der Übernahme entsprechende Rechtsänderungen vorzunehmen. Dies könnte – für den Datenschutzbereich oder darüber hinausgehend – der Anlass sein, die vom Bundesrat im Bereich des kollektiven Rechtsschutzes festgestellten Rechtsschutzlücken zu schliessen.[65] Denkbar ist insbesondere die Schaffung eines datenschutzspezifischen Verbandsklagerechts oder aber die Ausweitung des funktionalen Anwendungsbereichs des allgemeinen Verbandsklagerechts nach Art. 89 ZPO auf die Geltendmachung reparatorischer Ansprüche[66].

---

61 Die Verankerung eines solchen Verbandsklagerechts war bei der Einführung des Datenschutzgesetzes in der Bundesversammlung zwar diskutiert, aber letztlich verworfen worden: AmtlBull StR 1990, 145 ff.; AmtlBull NR 1991, 966 ff.

62 Diese Rechte wurden ursprünglich im Rahmen bundesgerichtlicher Rechtsprechung konstituiert: BGE 125 III 82, E. 1; BGE 121 III 168, E. 4b; BGE 114 II 345, E. 3b.

63 Botschaft zur Schweizerischen Zivilprozessordnung, BBl 2006 7221, 7289; in diesem Sinne auch bereits die frühere bundesgerichtliche Rechtsprechung: BGE 125 III 82, E. 1.

64 Vgl. hierzu auch Bundesrat, Bericht vom 3. Juli 2013 zum kollektiven Rechtsschutz in der Schweiz, 26.

65 Bundesrat, Bericht vom 3. Juli 2013 zum kollektiven Rechtsschutz in der Schweiz, insb. 55 ff.

66 Bundesrat, Bericht vom 3. Juli 2013 zum kollektiven Rechtsschutz in der Schweiz, insb. 56.

# E. Schluss

Ausgehend vom vorausgehenden Abgleich zwischen der geltenden sowie der sich für die Zukunft abzeichnenden Rechtslage in der EU und jener in der Schweiz lassen sich somit im Hinblick auf die Durchsetzungsmechanismen im Datenschutzrecht eine Reihe von Divergenzen feststellen. Stellt man nun die Frage nach der Sinnhaftigkeit einer Übernahme der europäischen Mechanismen und Verfahren ins schweizerische Recht, so drängt sich zunächst die Feststellung auf, dass die heutige Rechtslage in diesem Bereich in der Schweiz kaum als befriedigend bezeichnet werden kann. Faktoren wie der hohe Aufwand zur Erhebung von Beschwerden für den Einzelnen, die faktischen Unterschiede zwischen betroffenen Personen und Datenbearbeitern, das beträchtliche Prozessrisiko und die Beschränkung der Mittel und Kompetenzen des EDÖB führen dazu, dass das Datenschutzrecht in der Schweiz an Durchsetzungsmängeln krankt. Die sich in Erarbeitung befindenden Durchsetzungsinstrumente auf Unionsebene stellen nun eine mögliche Antwort auf diese Mängel dar, deren Tauglichkeit jedenfalls nicht von vornherein verneint werden kann. Vielmehr erscheinen gerade die weitergehenden Kompetenzen der Aufsichtsbehörden, das Prinzip der Sanktionsmöglichkeit, die Vertretung bei der Prozessführung sowie die Verankerung kollektiver Rechtsschutzinstrumente als grundsätzlich durchaus zielführende Instrumente eines verbesserten Rechtsschutzes. Ob diesen Mechanismen Erfolg beschieden sein wird, dürfte einerseits von ihrer konkreten Umsetzung und Handhabung in der Praxis abhängen, andererseits aber auch von „kulturellen“ Parametern, wie der Schaffung und dem Aktivitätsgrad von Verbänden und Organisationen im Bereich des Datenschutzes, dem Engagement der Aufsichtsbehörden, dem generellen Bewusstsein für die Belange des Datenschutzes in Gesellschaft und Politik sowie insbesondere, und damit zusammenhängend, der Bereitschaft der Betroffenen, ihren Persönlichkeitsrechte vor den Aufsichtsbehörden und Gerichten auch tatsächlich zum Durchbruch zu verhelfen.