www.jusletter-it.eu

Rolf H. Weber

EU-Datenschutz-Grundverordnung: Kernelemente und Ausstrahlungswirkung auf die Schweiz

In June 2015, the EU commission published a trialogue version of the General Data Protection Regulation. As an essential innovation, the stabilisation of the digital single market by a harmonised level of data protection is paramount, alongside the information rights, the right «to be forgotten» and the right to data portability, new regulations regarding the preventive data protection and the transnational data transmission as well as the strengthened provisions regarding surveillance. For the introduced revision of the data protection law in Switzerland, it seems reasonable to learn from the EU data protection legislation. (ah)

Category: Scientific Articles
Region: Switzerland, EU
Field of law: Data Protection

Citation: Rolf H. Weber, EU-Datenschutz-Grundverordnung: Kernelemente und Ausstrahlungswirkung auf die Schweiz, in: Jusletter IT 24 September 2015

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77 EDITIONS WEBLAW

Inhaltsübersicht

1. Einleitung

1.1. Recht und Technologie

[Rz 1] Die rechtliche Rahmenordnung muss grundsätzlich den technologischen und sozialen Gegebenheiten einer Gesellschaft entsprechen; wenn Gesetze so ausgestaltet sind, dass sie an den Bedürfnissen der ihnen Unterworfenen vorbeigehen, ist nicht mit deren Einhaltung zu rechnen, d.h. es entwickelt sich eine Ordnung ausserhalb des gegebenen Regelungsrahmens. Die Problematik der «Anpassung» des Rechts an die «Umweltbedingungen» zeigt sich insbesondere in Bereichen, die einem starken technologischen Wandel unterworfen sind; dazu gehört auch das Datenschutzrecht. Dass der Ruf nach einem verbesserten Schutz persönlicher Daten im Internet immer lauter ertönt, hat nicht zuletzt mit der Tatsache zu tun, dass die Datenschutzgesetze oft noch aus einer «Vor-Internetzeit» stammen und ganz andere Risikoszenarien zu erfassen versuchen. Der Gesetzgeber steht also vor der Frage, ob sich die Grundanliegen des Datenschutzes in der digitalen Welt überhaupt noch verwirklichen lassen bzw. inwiefern neue Schutzkonzepte der Internetwelt gewachsen sein können.[1]

[Rz 2] Beim Datenschutzrecht zeigt sich mit besonderer Deutlichkeit, dass Rechtsregeln kaum die Geschwindigkeit des technologischen Wandels mithalten können; vielmehr offenbart sich exemplarisch das Problem des sog. Regulatory Lag. Seit Jahren ist zudem anerkannt, dass der Datenschutz wesentlich auf technischen Massnahmen aufzubauen ist, weil die Datenschutztechniken – im Gegensatz zum Datenschutzrecht – weltweit wirksam sind und weil Technologien – im Gegensatz zu Regulatoren – schnell lernende Systeme sind.[2] Der technische Datenschutz ist überdies oft auch ef-

[1] Rolf H. Weber/Florent Thouvenin, Einleitung, in: Weber/Thouvenin (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht? Zürich 2012, 1.

[2] So schon Rolf H. Weber, Datenschutzrecht vor neuen Herausforderungen, Zürich 2000, 75.

fizienter als der rechtliche Datenschutz, weil sich bei einer technischen Verhinderung das rechtliche Verbot erübrigt; gegen Verhaltensnormen kann verstossen werden, gegen technische Begrenzungen von Systemen nicht.

1.2. Neuregulierung in der EU

[Rz 3] Angesichts der Tatsache, dass Daten nicht an Landesgrenzen Halt machen (grenzüberschreitender Datenverkehr, auf dem Internet global verfügbare Daten), führen nationale Datenschutzregeln zwingend zu Schutzproblemen; die Umsetzung in den EU-Ländern der Richtlinie 95/46 ist in den EU-Ländern nicht einheitlich erfolgt (z.B. in Grossbritannien durch allgemeine Prinzipien entlang der Richtlinienvorgaben, in Deutschland durch sehr detaillierte Regulierungen). Darüber hinaus sind auch die Melde- bzw. Anzeigepflichten für Datenverarbeitungsvorgänge unterschiedlich ausgestaltet. Nicht zuletzt im Lichte der Schaffung eines digitalen Binnenmarktes erweist sich eine Harmonisierung des Datenschutzrechts der EU-Länder deshalb als sinnvoll.[3] Zudem besteht Handlungsbedarf mit Blick auf die Anpassung an die technischen Entwicklungen der letzten zwanzig Jahre seit Erlass der Richtlinie 95/46 und wird auch eine gewisse Entbürokratisierung angestrebt.

[Rz 4] Die EU-Kommission hat am 25. Januar 2012 (nachdem die Vorversion des Textes schon im Dezember 2011 durch eine Indiskretion bekannt geworden ist) den Entwurf für die Reform des EU-Datenschutzrechts präsentiert.[4] Neben der Datenschutz-Grundverordnung (EU-DSGVO), welche die Richtlinie 95/46 ersetzen soll, steht eine – vorliegend nicht zu vertiefende – Richtlinie für die Zusammenarbeit der europäischen Behörden auf dem Gebiet des Strafrechts[5] zur Diskussion. Weil die EU-Kommission das ordentliche Gesetzgebungsverfahren gemäss Art. 16 Abs. 2 S. 1 AEUV gewählt hat, müssen auch das Europäische Parlament und der Ministerrat zustimmen (Art. 294 AEUV).

[Rz 5] Während Monaten haben im Parlament und im Ministerrat (unter Einwirkung eines nicht unbeachtlichen Lobbying seitens der interessierten Kreise) intensive Beratungen stattgefunden. Anfangs Juni 2015 hat nun die EU-Kommission eine konsolidierte Version der Datenschutz-Grundverordnung veröffentlicht,[6] die als Basis für die abschliessende Bereinigung des Textes dienen soll. Relativ optimistisch wird davon ausgegangen, dass die Beratungen bis Ende 2015 abgeschlossen sein würden; doch selbst wenn sich die Verabschiedung der Verordnung bis ins erste Quartal 2016 verzögern sollte, erscheint es im Lichte der in der Schweiz einsetzenden Revisionsbemühungen sinnvoll, deren Kernelemente und möglichen Auswirkungen genauer zu analysieren.

---

3 In diesem Sinne European Commission, Fact Sheet, Stronger data protection rules for Europe, Luxembourg, 15 June 2015 (MEMO/15/5170).

4 Europäische Kommission, Pressemitteilung, Kommission schlägt umfassende Reform des Datenschutzrechts vor, um Nutzern mehr Kontrolle über ihre Daten zu geben und die Kosten für Unternehmen zu verringern, Brüssel, 25. Januar 2012 (IP/12/46).

5 Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. 2008 L 350 vom 30. Dezember 2008, 60–71.

6 Council of the European Union, Doc 9398/15 of 1 June 2015.

1.3. Unausweichlicher Regulierungsschub?

[Rz 6] Quantitativ betrachtet zeichnet sich die Datenschutz-Grundverordnung zweifellos dadurch aus, dass sie einen erheblichen Regulierungsschub verursacht, weil sie nicht nur sehr umfangreich ist, sondern auch – ungeachtet der direkten Anwendbarkeit als Verordnung – die einzelstaatlichen Datenschutzgesetze nicht vollumfänglich überflüssig macht, sondern nationale Erlaubnisvorbehalte zur Erhöhung des Datenschutzniveaus enthält (Art. 80 ff. EU-DSGVO), insbesondere zur sehr nationalstaatenbezogenen und damit wohl konkretisierend geregelten Arbeitnehmerdatenkontrolle (Art. 82 EU-DSGVO), und zudem durch sektor-spezifische Regulierungen ergänzt werden kann, was schon auf der EU-Ebene durch die sog. E-Privacy-Richtlinie 2002/58[7], die Sonderregeln für Internetsachverhalte vorsieht, der Fall ist.

[Rz 7] Die Änderung der Regelungstechnik (unmittelbar geltende Verordnung statt umzusetzende Richtlinie, welche auf Privatunternehmen und die «normale» öffentliche Verwaltung anwendbar ist) bedeutet somit nicht, dass die Regulierungsdichte abnimmt. Der vorliegende Entwurf der Verordnung enthält auf nicht weniger als 67 Seiten 135 Erwägungsgründe. Der eigentliche Verordnungstext ist in 91 Artikel gegliedert, die 183 Seiten in Anspruch nehmen. Dass die abschliessenden Verhandlungen im Rahmen der Finalisierung des Textes zu wesentlichen Kürzungen führen, ist nicht anzunehmen. Ein Dokument von über 250 Seiten ist indessen in der Praxis nur noch von Experten zu bewältigen.

[Rz 8] Selbst wenn sich nicht übersehen lässt, dass der Datenschutz eine technisch und rechtlich schwierig durchzusetzende Materie darstellt, bleibt doch die Frage offen, ob mittel- und langfristig eine Konzentration der Regulierung auf die wesentlichen Datenschutzprinzipen nicht erfolgsversprechender wäre. Wenn die Datenbearbeiter die Verantwortung für die Einhaltung solcher Datenschutzprinzipien haben, sind sie auch gehalten, diejenigen Vorkehren zu treffen, die im gegebenen Kontext als sachgerecht erscheinen. Wie die technischen Verfahren konkret aussehen, vermag Gegenstand des «Datenschutzwettbewerbs» unter den Datenbearbeitern zu sein, die Einhaltung der Prinzipien ist letztlich ein Qualitätsmerkmal der Erbringung von Güter- und/oder Dienstleistungen. Zur Vermeidung «schwarzer Schafe» bedarf es indessen einer angemessenen Überwachung mit Blick auf die Einhaltung von Datenschutzprinzipien.

[Rz 9] Die detaillierte Regulierungstechnik mag für international tätige Unternehmen erwünscht sein; zudem kann sie innerhalb der EU zu einer stärkeren Harmonisierung führen, ohne dass dieser aber angesichts der Funktionen einzelstaatlicher Aufsichtsbehörden und Gerichte, die oft nach nationalen Überlegungen offene Auslegungsfragen entscheiden, schon eine entsprechende Wirkung gewährleistet. Für die Schweiz spielt dieses Element der Harmonisierung indessen keine Rolle, weil jedenfalls im privaten Bereich der Datenschutz seit Erlass des DSG[8] vor über zwanzig Jahren auf Bundesebene geregelt ist.

---

7 Richtlinie 2002/58/EG des Europäisches Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutz für elektronische Kommunikation), ABl. 2002 L 201 vom 31. Juli 2002, 37-47.

8 Bundesgesetz vom 19. Juni 1992 über den Datenschutz mit seitherigen Anpassungen (SR 235.1).

2. EU-Datenschutz-Grundverordnung im Überblick

[Rz 10] Der nachfolgende Überblick über die Datenschutz-Grundverordnung skizziert vorerst kurz die Hauptstossrichtungen der neuen rechtlichen Rahmenordnung, thematisiert hernach die wesentlichen Neuerungen und geht schliesslich spezifisch auf die besonders umstrittenen Regelungen ein.

2.1. Hauptstossrichtungen

[Rz 11] In den neuesten Verlautbarungen der EU-Kommission steht nicht (mehr) der Schutz des Individuums vor einem Datenmissbrauch im Vordergrund, sondern die Stärkung des digitalen Binnenmarktes durch einen harmonisierten Datenschutz.[9] Materiell ist die Grundsystematik der Datenschutzregulierung beibehalten worden, d.h. es gilt das Verbotsprinzip mit Erlaubnisvorbehalt (Art. 6 EU-DSGVO). Auch die zentralen Schutzvorgaben (Verhältnismässigkeit, Zweckbindung, Richtigkeit der Daten, Verfahrens- und Aufbewahrungssicherheit) haben keine grundlegenden Änderungen erfahren (Art. 5 EU-DSGVO). Die Datenminimierung ist hingegen neu ausdrücklich in Art. 23 EU-DSGVO erwähnt; damit soll diesem Grundsatz ein höheres Gewicht beigemessen werden.

[Rz 12] Als Hauptstossrichtungen der neuen Rechtsgrundlagen lassen sich folgende Zielsetzungen herauskristallisieren:

- Harmonisierung der Rechtsgrundlagen zur Erhöhung der Rechtssicherheit und zur Erleichterung des grenzüberschreitenden Datenverkehrs sowie zur Gleichbehandlung (gleiche Regeln) der (potentiell) Betroffenen (one-stop-shop-Ansatz);
- Erleichterter Zugang zu den eigenen Daten und Recht auf Datenportabilität;
- Recht auf Auskunft mit Bezug auf potentielle Hacker der eigenen (geschützten) Daten;
- Recht auf Vergessenwerden;
- Weitgehende Abschaffung der bisherigen Anzeige- und Meldepflichten;
- Verstärkung des vorbeugenden Datenschutzes durch betriebsinterne Massnahmen;
- Neukonzeption des grenzüberschreitenden Datenverkehrs, insbesondere durch das Accountability-Konzept;
- Realisierung von verbesserten Überwachungs- und Rechtsdurchsetzungsregelungen (inkl. Bussenausfällung).

[Rz 13] Als Grundlage der neuen Datenschutzregulierung ist das Bemühen zu sehen, das Vertrauen der Zivilgesellschaft in die Korrektheit der Datenbearbeitung zu stärken; «Trust» und «Confidence» sind zentrale Elemente einer Werteordnung, die in der heutigen Realität oft fehlen, und müssen gestärkt werden.[10] Zudem sollen die Unternehmen mehr Geschäftsmöglichkeiten durch den Einsatz von datenschutzrechtlich einwandfreien Gütern und Dienstleistungen erhalten.

---

9 Memo/15/5170 (Fn. 3), 1.

10 Vgl. auch Memo/15/5170 (Fn. 3), 3/4.

2.2. Wesentliche Neuerungen

[Rz 14] Ein zentrales Ziel der EU-Datenschutzreform besteht, wie erwähnt, darin, die rechtliche Rahmenordnung zu harmonisieren; dieses Anliegen, das mit Blick auf den digitalen Binnenmarkt als sachgerecht erscheint, ist ein spezifisches Thema eines (regionalen) Staatenbundes, das – mit den entsprechenden Konsequenzen für die nationale Gesetzgebung – vorliegend nicht weiter vertieft zu werden braucht. Abgesehen von diesem Aspekt sind die folgenden wesentlichen Neuerungen der EU-Datenschutzreform diskussionswürdig:

2.2.1. Räumlicher Anwendungsbereich

[Rz 15] Art. 3 EU-DSGVO nimmt eine erhebliche und auch für Schweizer Unternehmen relevante Erweiterung des räumlichen Anwendungsbereichs vor: Der EU-Datenschutzregulierung unterstehen nicht nur in einem EU-Mitgliedschaft domizilierte Unternehmen, sondern auch ausserhalb der EU lokalisierte Unternehmen, sofern diese Unternehmen (auch) Daten über in der EU ansässige Personen entweder beim Angebot von Waren oder Dienstleistungen in der EU verarbeiten, und zwar unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist, oder aber deren Verhalten beobachten, soweit ihr Verhalten in der EU erfolgt.

[Rz 16] Mit Bezug auf die Auslegung des Begriffs des «direkten Angebots» hat eine autonome Auslegung stattzufinden, weil ein Abstellen auf bekannte (z.T. von der Rechtsprechung herausgearbeitete) Kriterien wie etwa die angegebene Währung, die verwendete Sprache oder der Einsatz lokaler Domain-Namen nicht als sachgerecht erscheint.[11] Eine solche autonome Auslegung, deren Konturen sich erst im Laufe der Jahre ergeben dürften, führt jedoch anfänglich zu Rechtsunsicherheiten.

[Rz 17] Der Begriff des «Beobachtens» erlaubt ebenfalls eine extensive Auslegung bei der Beurteilung von werbebezogenen Massnahmen: Die Verwendung von Profilen über Internet-Aktivitäten für Verhaltensanalysen, die zielgerichtete Werbung (behavioral advertising) und eine nach Nutzung differenzierte Ausgestaltung von Internet-Angeboten und Preisen dürften deshalb künftig zur Anwendbarkeit der Verordnung auf ausländischen Unternehmen führen.[12]

[Rz 18] Überdies haben auch nicht in der EU lokalisierte Unternehmen, wenn die vorgenannten Aktivitäten nach EU-Recht zu beurteilen sind, einen Vertreter in der EU zu bestellen (Art. 25 EU-DSGVO), der die Vertretung (nicht zuletzt in der Form der Zustellungsadresse) bei Beschwerden und Aufsichtsmassnahmen übernimmt. Ein Vorbehalt für Unternehmen aus anerkannten Drittländern, wie z.B. der Schweiz, ist abweichend vom Entwurf in der konsolidierten Version der Verordnung nicht mehr enthalten; Schweizer Unternehmen kommen deshalb nicht (mehr) in den Genuss einer privilegierten Behandlung. Hingegen besteht die Pflicht nach Art. 25 EU-DSGVO nicht für Behörden und öffentliche Einrichtungen; zudem ist kein Vertreter zu bestellen, sofern die Verarbeitung gelegentlich erfolgt – unter Berücksichtigung der Umstände, des Umfangs und der Zwecke der Verarbeitung – und diese voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

---

11 Vgl. die Nachweise bei Jürgen Hartung, Neue Regulierungsaspekte in der EU-Datenschutzreform, in: Weber/Thouvenin (Hrsg.), Neuer Regulierungsschub im Datenschutzrecht?, Zürich 2012, 31, 39/40.

12 Hartung (Fn. 11), 40.

2.2.2. Begriff der Personendaten

[Rz 19] Der Begriff der Personendaten ist ein Element des *sachlichen Anwendungsbereichs*. Ähnlich wie bei der räumlichen Umschreibung kommt es nach der neuen Verordnung auch bei der sachlichen Umschreibung zu einer Erweiterung des Anwendungsbereichs: Nach Art. 4 EU-DSGVO liegt namentlich ein Personendatum vor, wenn ein Individuum direkt oder indirekt mittels Zuordnung zu einer Kennnummer, zu Standortdaten oder zu einer Online-Kennung bestimmt werden kann.[13] Aus diesem Grunde dürften alle Informationen, die mit einer solchen technischen Kennung verbunden sind, künftig als personenbezogene Daten gelten.[14] Insbesondere trifft dies auf IP-Adressen zu; diese in der Schweiz zwar seit dem Logistep-Entscheid des Bundesgerichts[15] geklärte, in Deutschland aber weiterhin diskutierte Frage wird also gesetzgeberisch entschieden.

[Rz 20] Der Wortlaut der Umschreibung von Personendaten, der auf die für die Bearbeitung Verantwortlichen oder jede sonstige natürliche oder juristische Person Bezug nimmt, lässt den Schluss zu, dass die Bestimmbarkeit der Person nach einer objektiven Betrachtungsweise zu beurteilen ist. Nicht entscheidend sein dürfte somit die subjektive Beurteilung des die Daten Bearbeitenden sowie die ihm zustehenden Mittel und Möglichkeiten. Die Konsequenzen eines solchen Perspektivenwechsels sind noch kaum absehbar; tendenziell dürften künftig aber mehr Daten als Personendaten zu qualifizieren sein, weil z.B. Internet Service Provider als Dritte objektiv betrachtet oft eine Person zu bestimmen vermögen und weil Cloud Computing Anbieter ebenfalls nicht selten die Möglichkeit haben, personenbezogene Daten wahrzunehmen und/oder zu bearbeiten.[16]

[Rz 21] Gewisse gesetzgeberische Anpassungen erfolgen auch mit Blick auf die Erstellung von Profilen und die Möglichkeit der Pseudonymisierung von Daten. Weil Persönlichkeitsprofile besonders sensitiv sein können, ist die Einhaltung der allgemeinen Datenschutzprinzipien von herausragender Bedeutung; nicht nur sind hohe Datensicherheitsstandards einzuhalten, sondern es muss auch dem Grundsatz der Zweckbindung bei der Verwendung von Daten aus Persönlichkeitsprofilen besondere Beachtung geschenkt werden.[17] Die Pseudonymisierung von Daten erlaubt die «Verwischung» des Personenbezugs. Dass aus diesem Grunde eine Pseudonymisierung oft wünschbar ist, erweist sich als offensichtlich; die vornehmliche Problematik der Pseudonymisierung besteht aber im Risiko der De-Anonymisierung der entsprechenden Daten.[18]

[Rz 22] Anstelle der weitgehend wegfallenden Anzeige- und Meldepflichten sieht die Verordnung neu umfangreiche Anordnungen zu den Pflichten der Datenbearbeiter vor: Im Vordergrund stehen die technischen Anforderungen an den Bearbeitungsprozess («processing») sowie die Dokumentationspflichten.[19] Die detaillierten Vorgaben helfen zumindest den betroffenen Unternehmen, ihre Datenschutzvorkehren in einer Weise auszugestalten, dass die Einhaltung des Regulierungsrahmens

---

13 Vgl. auch schon Art. 29 Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff «personenbezogene Daten» vom 20. Juni 2007.

14 Hartung (Fn. 11), 41.

15 BGE 136 II 508 E. 3.5.

16 Hartung (Fn. 11), 42/43.

17 Gerald Spindler/Fabian Schuster, Recht der elektronischen Medien, 3. Aufl., München 2015, TMG § 15 N 9, 12.

18 Rolf H. Weber/Dominic Oertly, Aushöhlung des Datenschutzes durch De-Anonymisierung bei Big Data Analytics?, in: Jusletter IT 21. Mai 2015, N 9.

19 Zu den Dokumentationspflichten vgl. Art. 28: Aufzeichnungen zu den Kategorien von Tätigkeiten der Verarbeitung personenbezogener Daten.

sich als wahrscheinlich erweist.[20]

[Rz 23] Eine vollständige Neuerung der Datenschutz-Grundverordnung betrifft die Einführung von Regeln zur Verarbeitung personenbezogener Daten über Kinder (Art. 8 EU-DSGVO).[21] Kinder sollen bewusst stärker als Erwachsene geschützt werden, etwa mit dem Erfordernis des Einwilligungsvorbehalts von Eltern (Vormündern), mit der Gestaltung von Informationen in einer kindergerechten Weise sowie mit einem erweiterten Recht auf Vergessenwerden im Hinblick auf im Kindesalter veröffentlichte Daten.

2.2.3. Recht auf Vergessenwerden und Datenportabilität

[Rz 24] Seit gut fünf Jahren hat das schon früher bekannte Recht auf Vergessen eine starke Wiederbelebung in der wissenschaftlichen und in der öffentlichen Diskussion erfahren,[22] insbesondere aber seit dem bekannten Google/Spanien-Fall des Europäischen Gerichtshofes vom Mai 2013, der zumindest im Grundsatz, wenn zwar zum Teil mit unklaren Konturen, ein Recht auf Vergessen anerkannt hat.[23] Ob die Überschrift von Art. 17 EU-DSGVO nach der Verabschiedung tatsächlich den Begriff «Right to be Forgotten» enthält, ist derzeit noch ungewiss, weil weiterhin nur schon die «Titelgebung» umstritten ist. Hingegen dürfte dieses (neue) Grundrecht zumindest in einer gegenüber dem Entwurf abgeschwächten Form überleben. Die Bestimmung ist zwar weiterhin kompliziert formuliert und lässt verschiedene Fragen offen,[24] doch geht es im Kern um den Schutz des Interesses von Individuen, dass lang zurückliegende negative Ereignisse nicht länger öffentlich bleiben sollten. Von besonderer Brisanz in diesem Kontext ist die Abwägung zwischen dem Privatheitsschutz und der Meinungsäusserungsfreiheit.[25]

[Rz 25] Von mindestens so grosser praktischer Bedeutung ist das Recht auf Datenportabilität (Datenmitnahme bzw. Datenübertragung): Gemäss Art. 18 EU-DSGVO in der jetzigen Fassung hat jede Person das Recht, die sie betreffenden personenbezogenen Daten, welche sie einem für die Bearbeitung Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Hinsichtlich des Formats bleibt abzuwarten, in welchen Fällen diese als «gängig» bzw. als «strukturiert» zu qualifizieren ist.[26] Art. 18 des Entwurfs der EU-Kommission vom 25. Januar 2012 schränkte dieses Recht noch auf diejenigen Fälle ein, in denen personenbezogene Daten in einem «strukturierten, gängigen elektronischen Format» bearbeitet werden. Diese Einschränkung hätte in der Praxis wohl dazu geführt, dass dem Einzelnen kein Recht auf Datenmitnahme zustünde;[27] somit ist die Neuformulierung von Art. 18 EU-DSGVO zu begrüssen.

---

20 Im Gegensatz zu dieser (rechtlichen) Feststellung ist jedoch darauf hinzuweisen, dass die technische Umsetzbarkeit insbesondere bei kleineren Unternehmen oftmals eine grosse Herausforderung darstellt.

21 Vgl. dazu auch Hartung (Fn. 11), 48.

22 Rolf H. Weber, The Right to be Forgotten: More than a Pandora's Box?, JIPITEC 2011, 120 ff.

23 EuGH, Urteil vom 13. Mai 2014, Rs. C-131/12, Google Spain und Google.

24 Giovanni Sartor, The right to be forgotten in the Draft Data Protection Regulation, International Data Privacy Law, 2015, Vol. 5(1), 67.

25 Vgl. nun auch Rolf H. Weber, On the Search for an Adequate Scope of the Right to be Forgotten, JIPITEC 2015, 2 ff.

26 Vgl. dazu Stellungnahme 47/2012 des Deutschen Anwaltsvereins vom Mai 2012, 23.

27 Hartung (Fn. 11), 46.

2.2.4. Ausbau der Informationsrechte

[Rz 26] Eine nicht unbeachtliche Problematik der heutigen Rechtslage besteht in der Tatsache, dass wenig Transparenz herrscht, wer welche Daten bearbeitet und weiterleitet. Aus diesem Grunde ist es sachgerecht, das Niveau der Transparenz anzuheben und insbesondere die Informationsrechte der Betroffenen auszubauen (Art. 12–19 und 32 EU-DSGVO).

[Rz 27] In Ergänzung des bestehenden Auskunftsrechts sieht Art. 14 DEU-DSGVO nun eine proaktive Information durch den Datenbearbeiter vor, wenn eine Mitteilung an den Betroffenen als sinnvoll erscheint. Insbesondere besteht eine Informationspflicht, wenn Personendaten von dritter Seite gehackt worden sind. Als Ausfluss des Anliegens «Zugang zu den eigenen Daten» hat der Betroffene überdies ein jederzeitiges Auskunftsrecht, das er durch Anfrage ausüben kann (Art. 15 EU-DSGVO). Neu (und z.T. umstritten) ist auch die Pflicht des Datenbearbeiters, bei Datenschutzverstössen eine Meldung zu erstatten (Art. 32 EU-DSGVO).

[Rz 28] Richtlinien und Policies sollen die Art und Weise der Transparenzschaffung klären und hernach das betroffene Unternehmen auch binden; die Information ist zudem in einer klaren, dem jeweiligen Empfängerhorizont angemessenen Sprache abzugeben (Art. 12 EU-DSGVO). Ebenfalls in Art. 12 EU-DSGVO ist die Möglichkeit der Informationsübermittlung «in elektronischer Form» verankert; diese Regelung wird insbesondere bei den Suchmaschinen und beim Online Behavioral Advertising zur Anwendung kommen, weil das betroffene Individuum erkennen können muss, auf Grund welcher personenbezogenen Daten die konkrete Suchanfrage bzw. die konkrete Werbung angezeigt wird.

2.2.5. Neukonzeption der Einwilligung

[Rz 29] Die Einwilligung des Betroffenen stellt regelmässig einen Rechtfertigungsgrund für Datenbearbeitungen dar. Zwischenzeitlich ist aber erkannt, dass die Einwilligung oft entweder versteckt oder gestützt auf eine wenig klare Darstellung ihrer Konsequenzen gegeben wird.[28] In der Praxis laden Datenbearbeiter die betroffenen Nutzer regelmässig ein, die Einwilligung durch Anklicken von Allgemeinen Geschäftsbedingungen zu erklären; in einzelnen Ländern (z.B. Grossbritannien) ist sogar ein «implied consent» möglich.

[Rz 30] Nach Art. 4 (8) EU-DSGVO muss künftig die Einwilligung eine für den konkreten Fall erfolgende ausdrückliche Willenskundgebung darstellen. Der Wortlaut lässt auch den Schluss zu, dass der EU-Gesetzgeber das System der «Opt-in» Einwilligung verwirklichen will.[29] Demgemäss kann der Datenbearbeiter nur dann von einer Einwilligung ausgehen, wenn tatsächlich die entsprechende Erklärung vorliegt, und angenommen werden darf, dass der Erklärende die Tragweite seiner Einwilligung erkannt hat. Insbesondere mit Blick auf Cookies dürfte gelten, dass die ausdrückliche Einwilligung gestützt auf Pop-up-Felder einzuholen ist.[30]

[Rz 31] Der heutigen Technologie entsprechend wird für die Einwilligung nicht mehr die Schriftform verlangt (Art. 7 EU-DSGVO); gesicherte elektronische Formen einer nachvollziehbaren bzw. protokollierten Einwilligung dürften künftig zum Normalfall werden.

[Rz 32] Der Widerruf der Einwilligung ist jederzeit und voraussetzungslos möglich (Art. 7 (3)

---

28 Rolf H. Weber, Big Data: Sprengkörper des Datenschutzrechts, in: Jusletter IT 11. Dezember 2013, N 25.

29 Vgl. Hartung (Fn. 11), 43 mit Verweisen auf die deutsche Rechtsprechung.

30 Hartung (Fn. 11), 43/44.

EU-DSGVO). Für die Unternehmen ergibt sich damit eine gewisse Unsicherheit, die dazu zwingt, jederzeit Datenlöschungsvorkehren durchführen zu können.[31]

2.2.6. Vorbeugender Datenschutz

[Rz 33] In den letzten Jahren haben Praxis und Lehre verstärkt darauf gedrängt, Massnahmen des vorbeugenden Datenschutzes einzuführen.[32] Das Ziel solcher Massnahmen besteht darin, durch präventive Massnahmen mögliche Verletzungen des Datenschutzrechts zu vermeiden. Die ursprünglichen Stichworte lauten «Privacy by Design» und «Privacy by Default».[33] Solche Vorkehren des Datenschutzes durch Technik sind nun in Art. 23 EU-DSGVO vorgesehen: Die Einhaltung des Datenschutzes ist schon bei der Wahl der Mittel sicherzustellen, d.h. Konzeption und Implementierung des Datenbearbeitungsprozesses haben dem gegebenen Stand der Technik (unter Berücksichtigung des Verhältnismässigkeitsprinzips und des Kostenaufwandes) zu entsprechen (Abs. 1). Weiter unterliegt der Datenbearbeiter der Pflicht, durch vorhandene Voreinstellungen den Umfang der Datenbearbeitung und die Löschungsfristen möglichst datenschutzfreundlich auszugestalten.[34] Im Falle eines Outsourcings hat der Datenbearbeiter die detaillierten Vorgaben von Art. 26 EU-DSGVO zu berücksichtigen. Spezifische Anordnungen zur Datensicherheit regelt überdies Art. 30 EU-DSGVO.[35]

[Rz 34] Weiter kommt der Datenschutz-Folgenabschätzung ein grösseres Gewicht zu. Was gestützt auf eine Empfehlung der EU-Kommission von 2009 im Kontext der RFID-Technik in der Praxis bereits Anwendung gefunden hat, nämlich das Konzept eines «Privacy (Data Protection) Impact Assessment»,[36] wird nun als Mechanismus durch Art. 33 EU-DSGVO gesetzgeberisch eingeführt. Diese Massnahmen sind sachlich nicht umstritten, auch wenn sich nicht übersehen lässt, dass die konkrete Ausgestaltung gewisse Fragen aufzuwerfen vermag. Immerhin liegen zwischenzeitlich schon von Berufsorganisationen ausgearbeitete Handbücher und Richtlinienwerke vor, auf welche sich die betroffenen Datenbearbeiter stützen können.[37]

[Rz 35] Art. 22 EU-DSGVO führt auch den in den letzten Jahren bereits intensiv diskutierten «Accountability»-Grundsatz ein. Nach diesem Prinzip hat ein Unternehmen die interne Organisation in einer Art und Weise zu gestalten, dass die Einhaltung des Datenschutzrechts sichergestellt wird; aus diesem Grunde müssen Richtlinien und Prozesse dokumentiert sein und der Nachweis

---

31 Diesbezüglich ist auf Art. 17 (1) der Verordnung (Recht auf Löschung und auf «Vergessenwerden») zu verweisen, wonach die für die Verarbeitung verantwortliche Person verpflichtet ist, personenbezogene Daten ohne ungebührliche Verzögerung zu löschen.

32 Vgl. den Überblick bei Rolf H. Weber, Privacy management practices in the proposed EU Regulation, IDPL 2014, 290 ff.

33 Vgl. dazu Ann Cavoukian, «Privacy by Design, The 7 Foundational Principles», http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf (alle Internetseiten zuletzt besucht am 18. August 2015).

34 Vgl. auch Hartung (Fn. 11), 49.

35 Im Rahmen der Sicherheit der Verarbeitung hat die verantwortlichtliche Person unter Berücksichtigung der verfügbaren Technologie, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Wahrscheinlichkeit und der Höhe des Risikos für die persönlichen Rechte und Freiheiten geeignete technische und organisatorische Massnahmen zu ergreifen.

36 Dazu Rolf H. Weber, Can Data Protection be Improved through Privacy Impact Assessments?, in: Jusletter IT 12. September 2012.

37 Eingehender dazu Weber (Fn. 32), 293 ff.

der eingeleiteten Massnahmen bedarf der entsprechenden Ausgestaltung.[38] Selbst wenn die Unternehmen zum Teil zusätzliche Bürden und Kosten beklagen, ist der Accountability-Grundsatz nicht auf heftigen Wiederstand gestossen, weil dieses Prinzip den verantwortlichen Stellen auch eine recht grosse Organisationsautonomie und Flexibilität bei der Implementierung der Datenschutz-Compliance überlässt.[39]

2.2.7. Grenzüberschreitender Datenverkehr

[Rz 36] Nach bisherigem Recht in der EU und der Schweiz dürfen Daten grenzüberschreitend transferiert werden, sofern das Empfängerland über dasselbe adäquate Datenschutzniveau wie das Ursprungsland verfügt. Die Feststellung der Adäquanz ist oft aber problematisch, weil es nicht nur um die formelle Gesetzesausgestaltung, sondern auch um die praktische Anwendung und Durchsetzung der Normen geht.[40] Fehlt es am adäquaten Datenschutzniveau, muss der Mangel durch Vereinbarungen, sog. «Safe Harbor Agreements», geheilt werden; die Erfahrungen mit den Vereinigten Staaten haben indessen gezeigt, dass solche Vereinbarungen kaum einen vergleichbaren Datenschutz zu begründen vermögen.[41]

[Rz 37] Art. 41 EU-DSGVO konkretisiert nun die Kriterien für die Angemessenheitsentscheidung der EU-Kommission über das Datenschutzniveau in Drittländern. Diese Kriterien beseitigen gewisse bestehende Rechtsunsicherheiten. Wichtiger ist indessen die Möglichkeit, durch Binding Corporate Rules (BCR) innerhalb von Unternehmensgruppen gesellschafts- oder vertragsrechtlich das angemessene Vertragsniveau sicherzustellen (Art. 43 EU-DSGVO). Solche Binding Corporate Rules sind insbesondere im Bereich des Outsourcing und des Cloud Computing von grosser praktischer Relevanz.[42] Die neue Regelung ist zudem im Einklang mit dem Accountability-Grundsatz, d.h. die hauptsächlichste Verantwortung für die Einhaltung des angemessenen Datenschutzniveaus wird vom Regulator auf das Unternehmen verschoben. Zudem besteht weiterhin die Möglichkeit, durch EU-Vertragsklauseln das Datenschutzniveau des Inlands im Ausland sicherzustellen (Art. 42 EU-DSGVO).

2.2.8. Überwachung und Verantwortlichkeit

[Rz 38] Eine grössere Zahl von Bestimmungen der Verordnung betrifft die Überwachung der Einhaltung der Datenschutzprinzipien sowie die Schaffung von Kohärenz unter den nationalen Datenschutzbehörden. Zwar lässt sich die Frage stellen, ob der Detaillierungsgrad der Regulierungen so hoch sein muss, doch ist nicht zu unterschätzen, dass zumindest ein gewisser Koordinierungsbedarf besteht, der die Einrichtung eines Konsistenzmechanismus rechtfertigt.

[Rz 39] Die «Überwachung» der Datenschutz-Compliance kann vorerst durch betriebsinterne Datenschutzbeauftragte erfolgen; nach der aktuellen Fassung der Verordnung sind diese aber nur dann einzurichten, wenn dies im Unionsrecht oder im nationalen Recht vorgesehen ist (Art. 35 ff.

38 Weber (Fn. 36), N 25 ff.

39 Vgl. auch Hartung (Fn. 11), 51.

40 Vgl. Rolf H. Weber, Transborder data transfers: concepts, regulatory approaches and new legialative initiatives, IDPL 2013, 117 ff.

41 Weber (Fn. 40), 118 f.

42 Weber (Fn. 40), 123, 128.

EU-DSGVO). Je nach Grösse des Unternehmens wird es sich in diesen Fällen um eine Einzelperson oder um ein internes Inspektorat, das von der Geschäftsleitung unabhängig ist, handeln. Der interne Datenschutzbeauftragte hat die Aufgabe, die sachgerechten Massnahmen des erläuterten vorbeugenden Datenschutzes auszuarbeiten und im Unternehmen zu implementieren. In der EU ist Deutschland bislang der einzige Staat, welcher die Einsetzung eines betriebsinternen Datenschutzbeauftragten gesetzlich verankert hat. Die Pläne des EU-Ministerrates, die Überwachung der Datenbearbeitungen in Unternehmen alleine den nationalen Datenschutzbehörden zu überlassen – und nicht zwingend betriebsinterne Datenschutzbeauftragte vorzusehen – stossen aber auf durchaus nachvollziehbare Kritik.[43]

[Rz 40] Im Sinne der Rechtsharmonisierung untersteht ein grenzüberschreitend tätiges Unternehmen nach dem Konzept der Verordnung «nur» noch einer Aufsichtsbehörde (der sog. «Lead Authority»[44]); eingeführt wird dementsprechend das «one-stop-shop»-Modell. Die Aufsichtsbehörden haben aber einheitliche und recht weitgehende Befugnisse (Art. 46–54 EU-DSGVO); zudem ist die Zusammenarbeit unter den nationalen Behörden detailliert geregelt (Art. 54a–72 EU-DSGVO).

[Rz 41] Wesentlich verschärft gegenüber dem heutigen Rechtszustand werden die Verantwortlichkeitsbestimmungen: Datenbearbeiter, die sich nicht an die Vorgaben des anwendbaren Datenschutzrechts halten, haften nicht nur im Falle des Verschuldens, sondern im Sinne einer Gefährdungshaftung für jeglichen Schadenseintritt. Überdies ist die Einführung sehr hoher (am Umsatz des Unternehmens ausgerichteten) administrativer Bussen vorgesehen, die sich in der Vernehmlassung auch als besonders umstritten erwiesen haben. Die Bussenhöhe kann bis zu 2% (gemäss Auffassung des Parlaments sogar 5%) des weltweiten Jahresumsatzes des betroffenen Unternehmens betragen (Art. 79a (3) EU-DSGVO).[45]

2.3. Umstrittene Regelungen und voraussichtliche Implementierung

[Rz 42] Wie bereits erwähnt, sind verschiedene neue Regelungen zumindest im Grundsatz nicht sehr umstritten; einzelne Teile der Verordnung stossen aber auf Widerstand, zum Beispiel:

- Ausdehnung des räumlichen Anwendungsbereichs;
- Erweiterung des sachlichen Anwendungsbereichs durch die extensivere Umschreibung des Begriffs der Personendaten;
- Recht auf Vergessenwerden;
- Überwachung und Verantwortlichkeit, insbesondere Bussen.

[Rz 43] Ungeachtet der Tatsache, dass einzelne Teile der neuen Verordnung umstritten sind, ist aus heutiger Sicht nicht daran zu zweifeln, dass die Verabschiedung des Gesetzestextes in den nächsten Monaten erfolgen wird. Konkretisierende Regelungen sind aber später noch zu erwarten, insbesondere mit Blick auf die Ausgestaltung der notwendigen Kohärenzmechanismen.

[Rz 44] Für die Unternehmen bedeutet dies, dass die Vorbereitung der notwendigen Umsetzungsarbeiten nun an die Hand zu nehmen ist. Die bereits etablierten Massnahmen der Unternehmen,

---

43 Vgl. dazu Berufsverband der Datenschutzbeauftragten Deutschlands, Pressemitteilung, EU-Datenschutzverordnung darf kein Bürokratiemonster werden, Berlin, 23. Juni 2015.

44 Dieses Konzept wird im Finanzmarktbereich schon seit Jahren praktiziert («Lead Regulator/Supervisor»).

45 Vgl. dazu Tim Wybitul, Die EU-Datenschutz-Grundverordnung – hohe Bussgeldrisiken für Unternehmen, in: Compliance Berater, 8/2015, I.

welche aufgrund der nationalen Datenschutzgesetzgebungen zu ergreifen waren, werden in vielen Fällen nicht ausreichen, um die neuen Vorgaben zu erfüllen. Zudem haben die Unternehmen zu beachten, dass die geplante Verordnung nicht in nationales Recht zu übertragen ist; eine entsprechende Übergangsfrist fällt somit weg. Eine zeitige Vorbereitung auf die anstehenden Neuerungen hat zudem den Vorteil, dass ein allenfalls bereits implementiertes Datenschutzmanagement optimiert werden kann.[46]

2.4. Anhang: Revision der Datenschutzkonvention des Europarates

[Rz 45] Der Vollständigkeit halber bleibt noch darauf hinzuweisen, dass die Datenschutzkonvention des Europarates aus dem Jahre 1980, d.h. eine der ältesten grenzüberschreitenden und auch für die Schweiz verbindlichen Vereinbarungen zum Datenschutz, seit längerer Zeit in Revision ist. Der Umfang der Anpassungen ist zwar geringer als in der EU, die Ziele sind zum Teil aber ähnlich formuliert und der informelle Informationsaustausch mit den EU-Organen erscheint als offensichtlich.

[Rz 46] Viele der geplanten Änderungen in der Datenschutzkonvention sind hierzulande insofern nicht weiter von Bedeutung, als die Schweiz in den entsprechenden Bereichen bereits über ein adäquates Datenschutzniveau verfügt. Kurz zusammengefasst strebt der Europarat mit den Revisionsbemühungen namentlich folgende für die Schweiz bedeutsame Neuerungen an:

- *Meldepflichten*: Der vorliegende Entwurf der Datenschutzkonvention des Europarates sieht eine ausdrückliche Meldepflicht bei Datenschutzverstössen vor, sofern eine ernsthafte Gefährdung der Persönlichkeitsrechte der Betroffenen zu befürchten ist (Art. 7 (2) der Konvention). Das schweizerische Datenschutzgesetz kennt bis anhin (noch) keine entsprechende Pflicht.
- *Auskunftsrechte*: Gemäss Art. 8 lit. c der Konvention soll eine leichte Ausweitung der Auskunftsrechte stattfinden. Demzufolge haben die Unternehmen in Zukunft nicht nur Angaben über die Art und den Zweck der Datenbearbeitungen zu machen, sondern auch darüber, welche Resultate aus der Datenbearbeitung resultieren.
- *Aufsichtsbehörden und Sanktionen*: Neben den Gerichten soll es in Zukunft auch den Aufsichtsbehörden (Verwaltung) möglich sein, Sanktionen zu erlassen (Art. 10 der Konvention). Daraus folgt gemäss Art. 12^{bis} des Entwurfs eine Pflicht der Konventionsstaaten, ihre nationalen Datenschutzaufsichtsbehörden mit einer Verfügungskompetenz auszustatten, damit diese künftig rechtlich verbindliche Massnahmen ergreifen können.

[Rz 47] Weitere Änderungen, z.B. im Bereich des Anwendungsbereichs oder bei der Einwilligung, sind mit Blick auf die Schweizer Datenschutzgesetzgebung nicht als wesentliche Reformen einzustufen.

3. Handlungsoptionen für die Schweiz und Ausblick

3.1. Ausgangslage

[Rz 48] Der Bundesrat hat schon vor 4 Jahren anerkannt, dass das auf die Grossrechnertechnologie ausgerichtete Datenschutzgesetz (DSG) von 1992, ungeachtet einer beschränkten Revision im Jah-

46 Oliver Schonschek, EU-Datenschutz-Grundverordnung: Was sich für Unternehmen ändert, http://www.searchsecurity.de/lernprogramm/EU-Datenschutz-Grundverordnung-Was-sich-fuer-Unternehmen-aendert.

re 2007, nach Ablauf von zwei Dezennien einer grundsätzlichen Überarbeitung bedarf. Immerhin ist der Bundesrat (etwas erstaunlich) in seinem Bericht über die Evaluation des DSG zum Schluss gekommen, das DSG habe «insgesamt zweifellos eine gewisse Wirksamkeit erzielt».[47] Als Hauptziele einer die raschen technologischen und gesellschaftlichen Entwicklungen reflektierenden Revision sind im Bericht das frühe «Einsetzen» des Datenschutzes, die verstärkte Sensibilisierung der betroffenen Personen, die Erhöhung der Transparenz sowie die Verbesserung der Datenkontrolle und -herrschaft genannt.[48]

[Rz 49] Am 1. April 2015 hat der Bundesrat beschlossen, das Eidgenössische Justiz- und Polizeidepartement (EJPD) zu beauftragen, bis spätestens Ende August 2016 einen Vorentwurf zur Revision des DSG auszuarbeiten.[49] Neben den laufenden Reformbestrebungen in der EU und im Europarat, die als Referenzpunkte angesprochen sind, sollen insbesondere die Ergebnisse der Arbeitsgruppe, die in einem Bericht an den Bundesrat den Handlungsbedarf aufgezeigt hat[50], Berücksichtigung finden. Das Ergebnis soll den Bundesrat in die Lage versetzen, die modernisierte Europarats-Konvention zum Schutze der Menschen bei der automatischen Verarbeitung personenbezogener Daten (SEV 108) zu ratifizieren.

[Rz 50] In ihrem Bericht schlägt die Arbeitsgruppe vor, verschiedene neue Sorgfaltsvorkehren einzuführen, welche die Datenbearbeiter verpflichten, Massnahmen zu ergreifen, die zur Datenschutz-Compliance beitragen bzw. negative Folgen von Datenschutzverstössen abmildern. Vorgeschlagen wird:[51]

- *Einführung des Grundsatzes der «Privacy by Design» und der «Privacy by Default»:* Bei der Personendatenbearbeitung sind angemessene Schutzmassnahmen vorzukehren, damit die allgemeinen DSG-Grundsätze wie das Verhältnismässigkeits- und das Datenminimierungsprinzip eingehalten werden können (z.B. Beschränkung auf das zwingende Minimum an Daten, die zur Zweckerreichung nötig sind, oder dezentrale Speicherung von beschafften Personendaten). Überdies sollen die Nutzer die Option zwischen mehreren unterschiedlich datenschutzfreundlichen Systemeinstellungen haben.
- *Angemessene Dokumentation der Datenbearbeitungsvorgänge:* Der Grundsatz der Transparenz gebietet es, dass der Datenbearbeiter weiss, wer welche Daten wie bearbeitet und die entsprechenden Vorgänge auch nachweisen kann (z.B. durch eine angemessene Dokumentation).
- *Abschätzung von Datenschutzfolgen:* Die potentiellen Auswirkungen einer Datenbearbeitung auf die betroffenen Personen sind zu analysieren und Risikopositionen zu minimieren (Privacy Impact Assessment).
- *Meldung von Verletzungen:* Datenbearbeiter sollen verpflichtet sein, den EDÖB über Datenschutzverletzungen ohne unangemessene Verzögerung zu informieren; die Einzelheiten einer solchen Meldepflicht hat die Arbeitsgruppe aber nicht konkretisiert.
- *Einsetzung eines Datenschutzverantwortlichen:* Im Kontext der Datenschutz-Compliance und des Privacy Impact Assessment erweist sich die Einsetzung eines Datenschutzverantwortlichen

47 Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, 345.

48 Bericht des Bundesrates (Fn. 47), 350.

49 Medienmitteilung des Bundesrates, Der Datenschutz soll gestärkt werden, vom 1. April 2015.

50 Bericht der Begleitgruppe Revision DSG vom 29. Oktober 2014, Normkonzept zur Revision des Datenschutzgesetzes.

51 Bericht der Begleitgruppe (Fn. 50), 18 ff.

im Unternehmen als sinnvoll; diese Person ist eine Art interner Kontrollstelle, die für die Einführung der notwendigen Massnahmen sowie für deren Einhaltung verantwortlich ist.

[Rz 51] Ein weiterer zentraler Bereich der Verbesserung des Datenschutzes betrifft die Stärkung der Rechte der betroffenen Personen. Als mögliche Neuerungen schlägt die Arbeitsgruppe vor:[52]

- *Recht auf Berichtigung:* Wenn die betroffene Person feststellt, dass gewisse Daten nicht zutreffend sind, muss der Datenbearbeiter verpflichtet sein, auf entsprechendes Gesuch dieser Person hin die falschen Daten zu berichtigen.
- *Automatisierte Einzelentscheidungen:* Im Falle automatisiert generierter Daten soll die betroffene Person rechtzeitig ihre persönliche Stellungnahme zur Richtigkeit der Daten abgeben können (z.B. mit Blick auf Kreditwürdigkeit, Zuverlässigkeit, Verhalten oder spezifische Risiken).
- *Zertifizierungspflicht:* Bereits bisher sieht Art. 11 DSG die Möglichkeit der freiwilligen Datenschutzzertifizierung vor; für risikobehaftete Bereiche lässt sich spezialgesetzlich eine Zertifizierungspflicht einführen.
- *Beweislastverteilung:* Wie in vielen anderen, für die Verbraucher relevanten Rechtsbereichen ist es der betroffenen Person oft nur schwer möglich, den Nachweis einer Rechtsverletzung bzw. eines Schadens zu erbringen. Aus diesem Grunde lässt sich die Frage erwägen, ob eine Beweislastverteilung zu Lasten des Datenbearbeiters zu sachgerechteren Resultaten führt, weil die Beweisstücke dem Datenbearbeiter leichter zugänglich sind.

[Rz 52] Schliesslich regt die Arbeitsgruppe an, die Aufsichtsbehörden, insbesondere den EDÖB, zu stärken; dabei wird an folgende Aufgaben und Kompetenzen gedacht:[53]

- *Vorabklärungen:* Ähnlich der Ausgestaltung im Kartellgesetz (Art. 26 KG) wäre denkbar, dem EDÖB die Möglichkeit einzuräumen, von Amtes wegen oder auf Begehren betroffener Personen bzw. Dritter ein Vorabklärungsverfahren zur einfachen, raschen, informellen und einvernehmlichen Lösung eines datenschutzrechtlichen Problems beizutragen.
- *Beratung Privater:* Über die schon heute in Art. 28 DSG vorgesehene Beratungstätigkeit hinaus wäre es überlegenswert, ein Vorprüfungsverfahren in Betracht zu ziehen, in dessen Rahmen die beabsichtigte Datenbearbeitung dem EDÖB vorgelegt werden könnte; ein ähnliches Verfahren kennt heute bereits das Kartellgesetz.
- *Informationsbeschaffung:* Wiederum ähnlich zur kartellgesetzlichen Regelung könnte die Kompetenz des EDÖB vorgesehen werden, über die Auskunftseinholung und Aktenedition hinaus das Recht auf Zugang zu den Räumlichkeiten und Datenbearbeitern zu erwirken sowie Beschlagnahmungen durchzuführen und Siegel anbringen zu lassen.
- *Verfügungs- und Sanktionskompetenz:* Die obrigkeitliche Durchsetzung von Datenschutzmassnahmen verlangt im Sinne der Effizienzsteigerung auch die Möglichkeit, Sanktionen auszusprechen; bisher ist das Bussenwesen im DSG nur sehr mangelhaft ausgestaltet gewesen.

[Rz 53] Die von der Arbeitsgruppe vorgeschlagenen, vorerwähnten Empfehlungen sind ganz offensichtlich in vielen Punkten den europarechtlichen Änderungen sehr nahe. Aus diesem Grunde dürfte die Datenschutz-Grundverordnung einen nicht zu unterschätzenden Einfluss auf die Anpassung des DSG in der Schweiz haben, weshalb es als angebracht erscheint, Lehren aus der EU-Gesetzgebung zu ziehen.

---

52 Bericht der Begleitgruppe (Fn. 50), 22 ff.

53 Bericht der Begleitgruppe (Fn. 50), 41 ff.

3.2. Lehren aus der EU-Gesetzgebung

[Rz 54] Das schweizerische DSG kennt keine ausdrückliche Bestimmung zum räumlichen Anwendungsbereich. Weil Art. 29 DSG aber als öffentlich-rechtliche Bestimmung zu qualifizieren ist, geht das Bundesgericht vom Territorialitätsprinzip aus.[54] Mit Blick auf die geplante Erweiterung des räumlichen Anwendungsbereichs in der EU-Datenschutz-Grundverordnung – die materiell das Territorialitätsprinzip einzuführen gedenkt – wäre es sinnvoll, eine entsprechende Normierung im Schweizer DSG vorzunehmen. Damit könnte die Rechtssicherheit für die Rechtsanwender, welche oftmals keine Juristen sind, erhöht werden.

[Rz 55] In Anlehnung an die datenschutzrechtlichen Reformvorhaben in der EU wäre es auch beim sachlichen Anwendungsbereich des DSG denkbar, die Definition des Personendatums «digitalbasiert» zu formulieren. Neben einer gesetzlichen Verankerung der Erkenntnis im Logistep-Entscheid[55] liesse sich die direkte oder indirekte Zuordnung zu einer technischen Angabe, wie z.B. der Online-Kennung, als neues Definitionsmerkmal der personenbezogenen Daten verankern. Eine entsprechende Erweiterung führte zu einer anzustrebenden Modernisierung des DSG.

[Rz 56] Das Recht auf Vergessenwerden, welches in der aktuellen Fassung der EU-Datenschutz-Grundverordnung vorgesehen ist, erscheint mit Blick auf die Kompatibilität der Datenschutzniveaus auch für die Schweiz als geeignetes Instrument. Es ist jedoch abzuwarten, wie die diesbezügliche Endfassung der EU aussehen wird; insbesondere gilt dies mit Bezug auf die technische Umsetzbarkeit. Zudem ist die angestrebte Datenportabilität ein zentrales Instrument, um die Individualbetroffenenrechte zu stärken. Im Unterschied zur konsolidierten Version des Entwurfs sollte die Schweiz aber darauf verzichten, die Bereitstellung der Daten nur in einem «gängigen, strukturierten und maschinenlesbaren» Format zu garantieren. Vielmehr ist darauf zu achten, dass der Betroffene die Daten in einer Art und Weise zur Verfügung gestellt bekommt, dass er diese öffnen und in seinem Datenherrschaftsbereich speichern kann.

[Rz 57] Die im Rahmen des Ausbaus der Informationsrechte angestrebte Verstärkung der Transparenz gilt es auch in der Schweiz zu implementieren; dieses Anliegen hat die Arbeitsgruppe bereits aufgenommen.[56] Die Einführung einer Informationspflicht, welche bei einem Hackerangriff von dritter Seite greift, erscheint mit Blick auf die Betroffenenrechte ebenfalls als gelungene Errungenschaft. In diesem Zusammenhang ist auch die in der EU-Datenschutz-Grundverordnung und in der Datenschutzkonvention des Europarates vorgesehene Meldepflicht zu sehen: Damit die Schweiz die neue Konvention ratifizieren kann, ist eine entsprechende Meldepflicht zwingend in der revidierten Fassung des DSG zu verankern.[57]

[Rz 58] Die neu konzipierte Einwilligung hat künftig in Form einer ausdrücklichen Willenskundgebung zu erfolgen.[58] Ob diese Neukonzeption oder gar das Opt-in System auch für die Schweiz den richtigen Weg darstellt, ist hingegen unklar. Aus einer rein rechtlichen Perspektive wäre dieser Richtungswechsel zwar zu befürworten, weil der Erklärende damit die Tragweite seiner Einwilligung verstehen und nachvollziehen kann, doch gilt es zu beachten, dass diese Neukonzeption

54 Vgl. BGE 138 II 346 E. 3.2.

55 Vgl. oben 2.2.b).

56 Bericht der Begleitgruppe (Fn. 50), 18 ff.

57 Bericht der Begleitgruppe (Fn. 50), 20 f.

58 Zur Problematik der Einwilligung im geltenden Recht vgl. Rolf H. Weber, E-Commerce und Recht, 2. Aufl. Zürich 2010, 456 ff.

viele Unternehmen vor nicht zu unterschätzende (technische) Herausforderungen stellen würde: Ist z.B. vorausgesetzt, dass Einwilligungen gestützt auf Pop-up-Felder einzuholen sind, müssen insbesondere kleine Unternehmen eine entsprechende Technik «nachrüsten», was praktisch nicht zu unterschätzen ist und wohl kostspielig sein würde.[59] Es wäre deshalb wünschenswert, wenn die Neukonzeption der Einwilligung im DSG solche technischen Faktoren mitberücksichtigen würde.

[Rz 59] Im Rahmen des vorbeugenden Datenschutzes sind die Konzepte der «Pricacy by Design» und der «Privacy by Default», welche in Form von Art. 23 Eingang in die Datenschutz-Grundverordnung der EU Eingang gefunden haben, ebenso wie auch des «Privacy Impact Assessment», in die Schweizer Gesetzgebung aufzunehmen.[60] Ferner darf im Rahmen des präventiven Datenschutzes die Verwirklichung des Accountability-Grundsatzes nicht fehlen; eine entsprechende Implementierung ist in der EU deshalb nicht auf grosse Gegenwehr gestossen, weil den Unternehmen eine gewisse Autonomie in der Umsetzung belassen werden soll. Diese erfolgsversprechende Vorgehensweise ist deshalb auch in der Schweiz zu verfolgen.

[Rz 60] Die in der aktuellen Fassung der EU-Datenschutz-Grundverordnung vorgesehenen Bestimmungen zum grenzüberschreitenden Datenverkehr sind ebenfalls überzeugend und eignen sich für einen autonomen Nachvollzug. Namentlich scheint in einer Zeit der Globalisierung die Verankerung von Binding Corporate Rules sinnvoll; somit lassen sich insbesondere die Sachverhalte des Cloud Computing und des Outsourcing sachgemäss abdecken. Eine Anpassung der Regelungen betreffend den grenzüberschreitenden Datenverkehr ist deshalb auch in der Schweiz angezeigt.

[Rz 61] Die Themen der Überwachung und Datenverantwortlichkeit stellen einen wesentlichen Bestandteil von modernen Datenschutzgesetzgebungen dar. Dennoch ist die diesbezügliche Regulierungsdichte in der EU etwas gar weitgehend; diesbezüglich hat die Schweiz auf ein «gesundes Mass» an Regulierung zu achten. Materiell abweichend von der aktuellen Fassung der EU-Datenschutz-Grundverordnung ist für Unternehmen mit einer gewissen Grösse[61] ein betriebsinterner Datenschutzbeauftragter vorzusehen. Damit lässt sich gewährleisten, dass eine vom Unternehmen unabhängige Person sich permanent um die datenschutzrechtlichen Abläufe und Vorkehren im Betrieb kümmert, was zu einer Verbesserung der Compliance und einer Entlastung des nationalen Datenschutzbeauftragten führt.

[Rz 62] Eine Stärkung des nationalen EDÖB wäre zwar auch in der Schweiz zu begrüssen, jedoch sind seine Ressourcen limitiert und eine diesbezügliche Aufstockung wäre mit der Gefahr von mehr Bürokratie verbunden.[62] Somit gilt es einen «goldenen Mittelweg» zwischen einer Kompetenzerweiterung des EDÖB und nicht ausufernden Ressourcen zu finden. Darüber hinaus hat der Schweizer Gesetzgeber das Sanktionssystem entsprechend dem Vorbild der EU zu reformieren: Eine Busse von bis zu 5% des weltweiten Jahresumsatzes, wie es das EU-Parlament noch vorsah, scheint jedoch allzu weitgehend, weshalb eine entsprechende Vorgabe für die Schweiz ungeeignet ist. Eine tiefere Spanne erschiene mit Blick auf das Verhältnismässigkeitsprinzip als sachgemäss.

---

59 Vgl. jedoch z.B. https://www.signatu.com/home; dabei handelt es sich um eine Art «Toolbox», welche verschiedene (technische) Funktionen für Unternehmen bereitstellt. Die Implementierung dieser Tools soll dazu beitragen, das geforderte Datenschutzniveau einzuhalten; die Funktionen befinden sich derzeit aber noch im Entwicklungsstadium.

60 Dazu ebenfalls Bericht der Begleitgruppe (Fn. 50), 19 f.

61 Analog zur Fassung der EU-Datenschutz-Grundverordnung vom 25. Januar 2012 sind KMU mit bis zu 250 Mitarbeitenden von dieser Regelung auszunehmen.

62 Zur Gefahr der Bürokratie und für weitere Hinweise vgl. Berufsverband der Datenschutzbeauftragten Deutschlands (Fn. 43).

3.3. Weitere Vorgehensoptionen

[Rz 63] Als weitere, wenn auch radikale Vorgehensoption könnte das DSG der Zukunft auf eine Differenzierung zwischen Personen- und Sachdaten verzichten. Dieses Vorgehen würde jedoch eine wesentliche Abweichung von den bisherigen datenschutzrechtlichen Konzepten bedeuten; angesichts des in zahlreichen Staaten tiefer liegenden Datenschutzniveaus wäre dies fast unmöglich zu verwirklichen.[63] Zudem ist mit Blick auf die geplante Ratifikation der Datenschutzkonvention des Europarates eine Abkehr vom Personendatum als massgebendem Referenzpunkt undenkbar.

[Rz 64] Eine weitere, weit erfolgversprechendere Vorgehensoption könnte die Implementierung neuer Vorschriften sein, welche auf eine Nutzengemeinschaft von wirtschaftlichem Datenerzeuger und Datenherrn hinwirken. Damit ist ein rechtlicher Rahmen angesprochen, welcher die sog. «sharing the wealth strategy» im Auge behält und damit beide Seiten am Nutzen der Daten partizipieren lassen möchte.[64] Ein diesbezüglicher (datenschutzrechtlicher) Regulierungsrahmen setzt aber voraus, dass der Gesetzgeber vorab die Frage klärt, inwiefern Daten als eigentumsähnliche Rechte qualifiziert werden können. Das von Nationalrat *Schwaab* eingereichte Postulat, welches der Bundesrat zur Annahme empfohlen hat, bringt den Stein in dieser Frage möglicherweise ins Rollen.[65]

Prof. Dr. iur. Rolf H. Weber ist Ordinarius für Privat-, Wirtschafts- und Europarecht an der Universität Zürich, Visiting Professor an der Hong Kong University und praktizierender Rechtsanwalt in Zürich.

63 Dazu Weber (Fn. 28), N 22 ff.

64 Ira S. Rubinstein, Big Data: The End of Privacy or a New Beginning?, International Data Privacy Law 2013, Vol. 3, No. 2, 81; Weber (Fn. 28), N 31.

65 Postulat 14.3782 vom 24. September 2014, Richtlinien für den «digitalen» Tod; vgl. dazu Rolf H. Weber, Big Data: Herausforderungen für das Datenschutzrecht, erscheint Ende 2015 in Epiney/Nüesch (Hrsg.), Schweizerischer Datenschutzrechtstag 2015, Schulthess Juristische Medien, Zürich 2015, B. IV. c).