■ Alternativen zum Privacy Shield bieten derzeit insbesondere Standarddatenschutzklauseln gem. Art. 46 Abs. 2 lit. c, d DS-GVO, verbindliche interne Datenschutzvorschriften gem. Art. 47 Abs. 1 DS-GVO[76] und – in deutlich geringerem Maße – die übrigen in Art. 46 ff. DS-GVO vorgesehenen Möglichkeiten. Zu beachten ist jedoch, dass auch diese Alternativen nicht darüber hinweghelfen, dass US-Nachrichtendienste (wie im Grunde auch weniger prominente Nachrichtendienste in anderen Ländern) weitreichende Überwachungsbefugnisse genießen. Die gegenüber dem Privacy Shield bestehenden Bedenken gelten daher jedenfalls teilweise auch für die in Art. 44 ff. DS-GVO vorgesehenen Alternativen,[77] wie auch das anhängige Vorabentscheidungsverfahren (Schrems gegen Facebook) betreffend den Datenexport in die USA auf Basis von Standarddatenschutzklauseln zeigt.[78]

Der Privacy Shield bildet damit – so oder in leicht abgewandelter Form – den kleinsten gemeinsamen Nenner angemessenen Datenschutzes.

Dipl.-Jur. Maximilian Mense
ist Head of Business Development bei der LAWLIFT GmbH in Berlin.

Der Autor dankt Dr. Barbara Sandfuchs, Lehrbeauftragte an der Universität Leipzig, für die wertvollen Anregungen im Vorfeld der Veröffentlichung.

76 *Geppert*, ZD 2018, 62; *Schmitz/von Dall'Armi*, ZD 2016, 217; *Karg*, VuR 2016, 457, 461.
77 *Hladjk* (o. Fußn. 42), Art. 46 Rdnr. 17; *Pauly* (o. Fußn. 7), Art. 45 Rdnr 25; *Geppert*, ZD 2018, 62, 65; *Wybitul/Ströbel/Ruess*, ZD 2017, 503, 505.
78 Rs. C-311/18 – Data Protection Commissioner/Facebook Ireland Limited, Maximilian Schrems.

LUKAS BÜHLMANN / HATUN METIN

Totalrevision des Schweizer Datenschutzgesetzes vor dem Hintergrund der DS-GVO

Reichweite der europarechtlichen Vorgaben in der Schweiz

Grenzüberschreitender Datenverkehr
Räumlicher Geltungsbereich
Erlaubnistatbestände
Data Breach
Sanktionen

■ Die Schweiz hat guten Grund, den datenschutzrechtlichen Entwicklungen in der EU Rechnung zu tragen. Die Annäherung an die europäische Datenschutzgesetzgebung ist sowohl völkerrechtlich als auch auf Grund der engen wirtschaftlichen Verknüpfung mit der EU und ihren Mitgliedstaaten geboten. Obschon die laufende Revision des Schweizer Datenschutzrechts diese Annäherung zum zentralen Anliegen hat, werden datenbearbeitende Unternehmen dies- und jenseits der Grenze sich auf unterschiedliche Vorgaben einstellen müssen. Dies stellt insbesondere für Schweizer KMU eine große Herausforderung dar, wenn sie ihre Geschäftstätigkeit auch auf Kunden in der EU ausrichten.

■ Switzerland has good reason to accommodate the data protection law developments in the EU. The approximation to the European data protection laws is both required from an international law aspect, as well as due to the close economic ties with the EU and its Member States. Even though the ongoing revision of the Swiss data protection law's main concern is the approximation, the data processing companies on both sides of the border will have to come to terms with varying requirements. In particular, this will be a big challenge for Swiss SME if they want to also provide business services to EU customers.

Lesedauer: 29 Minuten

I. Einführung

1. Hintergründe und Ziele der Totalrevision

Das aktuelle Schweizer Datenschutzgesetz (DSG)[1] geht zurück auf den 19.6.1992.[2] Um das DSG den technologischen Entwicklungen und den aktuellen Erwartungen an den Schutz personenbezogener Daten anzupassen, hat der *Schweizer Bundesrat* (als Exekutive) entschieden, das DSG einer Totalrevision zu unterziehen. Der Entwurf zur Totalrevision wurde dem Parlament im September 2017 unterbreitet (Entwurf zum DSG – E-DSG).[3]

Im schweizerischen Gesetzgebungsverfahren wird ein neuer Gesetzesentwurf von einer sog. Botschaft begleitet, in welcher der Gesetzgeber den neuen Entwurf begründet, soweit nötig die einzelnen Bestimmungen kommentiert und Angaben u.a. zu den maßgeblichen Rechtsgrundlagen und den Auswirkungen macht.[4] Gemäß Botschaft werden mit dem Entwurf zum neuen Datenschutzgesetz verschiedene Ziele verfolgt, wobei vor allem die Modernisierung des Gesetzes, die Stärkung der Rechte der Betroffenen und Behörden sowie die Förderung der Eigenverantwortung der Verantwortlichen im Vordergrund stehen.[5] Gleichzeitig soll die Totalrevision den Entwicklungen in der EU Rechnung tragen, die sich einerseits aus der Revision des Datenschutzübereinkommens SEV 108 des *Europarats* (Europarats-Konvention)[6] sowie andererseits aus der neuen EU-Richtlinie (EU) 2016/680 über den Datenschutz im Bereich der Strafverfolgung (Schengen-RL)[7] sowie der VO (EU) 2016/679 (DS-GVO)[8]

1 Bundesgesetz über den Datenschutz (DSG) v. 19.6.1992, SR. 235.
2 Das Eidgenössische Justiz- und Polizeidepartement hat das DSG 2011 einer Evaluation unterzogen, vgl. Evaluation des Bundesgesetzes über den Datenschutz – Schlussbericht v. 10.3.2011, *Büro Vatter AG* und *Institut für Europarecht*.
3 Medienmitteilung des *Bundesrats* v. 15.9.2017.
4 Art. 141 Bundesgesetz über die Bundesversammlung (Parlamentsgesetz – schweizParlG) v. 13.12.2002, SR 171.10; der Gesetzesentwurf ist jeweils das Resultat eines Vernehmlassungsverfahrens, das seinerseits auf der Basis eines sog. Vorentwurfs durchgeführt wird, Art. 112 Abs. 2 schweizParlG.
5 Botschaft zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz v. 15.9.2018, BBl 2017, S. 6941 ff., 6970.
6 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten v. 28.1.1981, revidierte Fassung v. Juni 2018, abrufbar (in Englisch) unter: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1.
7 RL (EU) 2016/680 über den Datenschutz im Bereich der Strafverfolgung v. 27.4.2016; sie ersetzt den Rahmenbeschluss 2008/977/JI des Rats v. 27.11.2008 über den Schutz personenbezogener Daten, die i.R.d. polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.
8 VO (EU) 2016/679 v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG.

ergeben und für die Datenbearbeitungen in der Schweiz von großer Relevanz sind.

2. Bedeutung der EU-Datenschutzentwicklungen für die Schweiz

Als Nicht-EU-Mitgliedstaat ist die DS-GVO in der Schweiz nicht direkt anwendbar, dies trotz Maßgeblichkeit für viele Schweizer Unternehmen auf Grund der in Art. 3 DS-GVO vorgesehenen extraterritorialen Anwendbarkeit der DS-GVO (zur extraterritorialen Wirkung der DS-GVO s. unter I.3.).[9] Sie ist deshalb bei der Revision ihres eigenen Datenschutzrechts mit Ausnahme ihrer völkerrechtlichen Verpflichtungen frei. Völkerrechtlich ist die Schweiz einerseits verpflichtet, Teile der DS-GVO direkt umzusetzen, um weiterhin am Schengen-Raum teilnehmen zu können, andererseits ist die Schweiz als Mitglied des *Europarats* verpflichtet, die Europarats-Konvention ins Schweizer Recht umzusetzen sowie – auf Grund des Schengen-Assoziierungsabkommens – die Schengen-RL im Bereich der Strafverfolgung zu übernehmen.[10] Selbstverständlich ist aber die Annäherung an den europäischen Standard grundsätzlich von zentraler Bedeutung, dies schon auf Grund der engen wirtschaftlichen Verknüpfung mit der EU und ihren Mitgliedstaaten.

Die Übernahme der Schengen-RL sowie die Ratifizierung der revidierten Europarats-Konvention sind i.Ü. entscheidend, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt. Aus Sicht der EU hängt der freie Datenverkehr zwischen einem Drittstaat und einem EU-Mitgliedstaat bekanntlich davon ab, ob der Drittstaat über ein angemessenes Schutzniveau verfügt (Art. 45 DS-GVO).[11] Zuletzt hatte die *EU-Kommission* basierend auf der RL 95/46/EG (DS-RL), d.h. nach alter Rechtslage, am 26.7.2000 das angemessene Datenschutzniveau der Schweiz bestätigt.[12]

3. Extraterritoriale Wirkung der DS-GVO und des Schweizer Datenschutzrechts

Die DS-GVO definiert in Art. 3 den räumlichen Geltungsbereich sehr weit. Bekanntlich sollen die neuen Vorschriften auch Anwendung finden auf Datenbearbeitungen, die zwar außerhalb der EU-Mitgliedstaaten erfolgen, sich jedoch auf betroffene Personen in der EU auswirken. Entsprechend verankert Art. 3 Abs. 2 DS-GVO u.a. das Marktortprinzip. Kennzeichnend für das Marktortprinzip ist, dass danach das Recht desjenigen Orts anwendbar ist, an dem aktiv in das Marktgeschehen eingegriffen und auf die Marktgegenseite eingewirkt wird.[13] Eine Bearbeitung von Personendaten durch ein schweizerisches Unternehmen untersteht nach diesem Prinzip somit bereits der DS-GVO, wenn es Waren oder Dienstleistungen Unionspersonen anbietet.[14] Die DS-GVO beansprucht folglich Geltung, die weit über das Hoheitsgebiet der EU reicht.

Anders als die DS-GVO äußert sich weder das aktuelle DSG noch der E-DSG ausdrücklich zum räumlichen Geltungsbereich.[15] In der Schweizer Lehre und Rechtsprechung ist aber anerkannt,[16] dass für privatrechtliche Bestimmungen des Datenschutzrechts grundsätzlich das Auswirkungsprinzip gilt. Damit findet das Schweizer Datenschutzrecht auch auf internationale Sachverhalte Anwendung, die sich nicht in der Schweiz (sondern z.B. in Deutschland) abspielen, aber Auswirkungen in der Schweiz entfalten.[17] Für öffentlich-rechtliche Bestimmungen des Datenschutzrechts gilt hingegen das Territorialitätsprinzip[18], sie kommen deshalb in der Regel nur bei Datenbearbeitungen in der Schweiz zur Anwendung.[19]

Auf Grund der extraterritorialen Wirkung beider Gesetze ist folglich eine weitgehende Harmonisierung sowohl aus Sicht der Schweiz als auch der EU zu begrüßen.

4. Stand der Revision des Schweizer Datenschutzrechts

Um die angestrebten Ziele rasch erreichen zu können, hat der *Bundesrat* beschlossen, die Revision des Schweizer Datenschutzrechts zu staffeln. In einer ersten Etappe wurden vorab die Anforderungen der Schengen-RL im Bereich der Strafverfolgung beraten.[20] Diese sind nun umgesetzt und gelten seit dem 1.3.2019 in der Schweiz.[21] Während die Ratifikation der Europarats-Konvention beim *Bundesrat* anhängig ist, wird die Totalrevision des DSG derzeit (noch immer) im *Schweizer Parlament* beraten. Letztere wird voraussichtlich bis Ende 2020 abgeschlossen sein.[22]

II. Vergleich ausgewählter Regelungen

Die nachfolgenden Ausführungen konzentrieren sich auf ausgewählte Aspekte der laufenden Revision des Schweizer Datenschutzrechts, die im Vergleich (und teilweise in Abweichung) zur DS-GVO besonders bemerkenswert erscheinen. In der Schweiz werden diese vor dem Hintergrund der angestrebten Kompatibilität kontrovers diskutiert.[23]

1. Grundkonzeption von E-DSG und DS-GVO

In der EU gilt das sog. Verbotsprinzip mit Erlaubnisvorbehalt. Nach diesem Prinzip ist jede Bearbeitung personenbezogener Daten grundsätzlich verboten und nur bei Vorliegen eines der in Art. 6 DS-GVO genannten Erlaubnistatbestände zulässig.[24] In der Schweiz gilt hingegen (weiterhin) der Ansatz, wonach Personendaten grundsätzlich bearbeitet werden dürfen, es sei denn, die Bearbeitung führt zu einer widerrechtlichen Persön-

---

9 Viele Schweizer Datenverantwortliche unterstehen auf Grund von Art. 3 DS-GVO dem EU-Datenschutzrecht, vgl. z.B. *Bühlmann/Metin*, Datenschutz im E-Commerce, Jusletter v. 15.10.2018, Rdnr. 14; *Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)*, Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf die Schweiz, Juli 2018, S. 2; *Sievers/Vasella*, TREX 2018, 330 ff.

10 Botschaft (o. Fußn. 5), S. 6943 und 6969; ausf. zu den Anpassungen ans EU-Recht, *Rudin*, digma 2018, 194 ff.

11 Abgesehen vom Erfordernis eines angemessenen Datenschutzniveaus des Empfängerlands gelten die allgemeinen Anforderungen an eine Datenbearbeitung selbstverständlich auch beim Datenverkehr, d.h. insb. das Vorliegen entsprechender Rechtsgrundlagen, Art. 6 DS-GVO.

12 Entscheidung der *Kommission* v. 26.7.2000 gemäß der RL 85/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzes personenbezogener Daten in der Schweiz, ABl. L 215 v. 25.8.2000, S. 1.

13 *Klar*, in: Kühling/Buchner, DS-GVO/BDSG, Komm., 2. Aufl. 2018, Art. 3 Rdnr. 9.

14 Ein Angebot i.S.v. Art. 3 DS-GVO muss offensichtlich beabsichtigt sein, vgl. Erwägungsgrund 23 DS-GVO; vgl. zur Feststellung einer aktiven Ausrichtung die i.R.d. verbraucherrechtlichen Rechtsprechung entwickelten Kriterien, z.B. Urteile des *EuGH* MMR 2011, 132 sowie C-297/14.

15 Vgl. zum aktuellen DSG statt vieler *Belser/Epiney/Waldmann*, Datenschutzrecht, Grundlagen und öffentliches Recht, 2011, § 7 Rdnr. 59; zum E-DSG, vgl. Botschaft (o. Fußn. 5), S. 7017.

16 Der *Bundesrat* hat folglich auch für den E-DSG darauf verzichtet, den räumlichen Anwendungsbereich zu regeln. Bereits nach geltendem Recht kann das Schweizer DSG auch auf internationale Sachverhalte zur Anwendung gelangen,

17 Vgl. zum Ganzen Botschaft (o. Fußn. 5), S. 7017; *Belser/Epiney/Waldmann* (o. Fußn. 15), § 7 Rdnr. 59-60; *Bühlmann/Reinle*, digma 2017, 8 ff.,10.

18 Privatrechtliche Bestimmungen sind z.B. die Datenbearbeitungsgrundsätze, öffentlich-rechtliche Bestimmungen sind hingegen die Informationspflicht an den *EDÖB*, die Pflicht zur Anmeldung einer Datensammlung nach geltendem DSG, vgl. *Bühlmann/Reinle* (o. Fußn. 17), S. 9 m.w.Nw.

19 Vgl. BGE 138 II 346, E. 3; ferner *Bühlmann/Schüepp*, in: Passadelis/Rosenthal/Thür, Datenschutzrecht, 2015, § 19 Rdnr. 19.102 if.

20 Diese wurde prioritär behandelt, weil die zweijährige Umsetzungsfrist der Schengen-RL im Bereich der Strafverfolgung anfangs August 2018 abgelaufen ist, vgl. *Rudin* (o. Fußn. 10), S. 194.

21 Medienmitteilung des *Bundesrats* v. 30.1.2019.

22 Übergangsfristen und -bestimmungen von zwei Jahren sind vorgesehen, vgl. Art. 67-67 E-DSG.

23 Vgl. z.B. ausf. *Rosenthal*, Der Entwurf für ein neues Datenschutzgesetz, Jusletter v. 27.11.2017; *Husi-Stämpfli*, digma 2017, 55 ff.; *Vasella*, digma 2017, 44 ff.; *Epiney/Kern*, Die Revision des Datenschutzes in Europa und die Schweiz, 2016, S. 72 ff.

24 Die in Art. 6 DS-GVO abschließend genannten Erlaubnistatbestände sind: Vertrag, gesetzliche Erlaubnis, überwiegendes berechtigtes Interesse, vgl. statt vieler: *Schulz*, in: Gola, DS-GVO, 2. Aufl. 2018, Art. 6 Rdnr. 9.

lichkeitsverletzung (Art. 12 Abs. 1 DSG, Art. 26 Abs. 1 E-DSG). Eine Persönlichkeitsverletzung liegt vor, wenn das Recht auf informationelle Selbstbestimmung verletzt wird, d.h. das Recht der betroffenen Person, grundsätzlich selbst bestimmen zu können, ob und zu welchen Zwecken Daten über sie bearbeitet werden dürfen.[25] Eine Datenbearbeitung, die gegen datenschutzrechtliche Vorschriften verstößt, führt immer zu einer Persönlichkeitsverletzung der betroffenen Person (Art. 12 Abs. 2 lit. a DSG, Art. 26 Abs. 2 lit. a E-DSG). In einem nächsten Schritt ist sodann jeweils zu prüfen, ob die Persönlichkeitsverletzung auch widerrechtlich ist. Dies ist der Fall, wenn für sie kein Rechtfertigungsgrund vorliegt (vgl. Art. 13 DSG, Art. 27 E-DSG).[26] In der Schweiz gilt demnach das sog. Erlaubnisprinzip mit Verbotsvorbehalt. Obschon der Schweizer Ansatz auf den ersten Blick liberaler erscheint, führt die unterschiedliche Konzeption materiellrechtlich zu keinen nennenswerten Unterschieden.

Soweit als Erlaubnistatbestand (EU) bzw. Rechtfertigungsgrund (Schweiz) vorgebracht wird, es liege eine gesetzliche Grundlage für die Datenbearbeitung vor (Art. 6 Abs. 1 lit. c DS-GVO, Art. 13 Abs. 1 DSG, Art. 27 Abs. 1 E-DSG), muss sowohl in der EU als auch der Schweiz bedacht werden, dass ausländische Gesetzesbestimmungen nicht direkt eine gesetzliche Grundlage bilden können.[27] Ausländisches Recht dürfte indes beim Erlaubnistatbestand bzw. Rechtfertigungsgrund des (berechtigten) überwiegenden Interesse von Relevanz sein (Art. 7 Abs. 1 lit. f DS-GVO, Art. 27 Abs. 1 und 2 E-DSG), insbesondere wenn es sich um zwingendes ausländisches Recht handelt.

Soweit als Erlaubnistatbestand bzw. Rechtfertigungsgrund vorgebracht wird, es liege eine Einwilligung der betroffenen Person in die Datenbearbeitung vor (Art. 6 Abs. 1 lit. a DS-GVO, Art. 13 Abs. 1 DSG, Art. 27 Abs. 1 E-DSG), muss diese sowohl in der EU als auch der Schweiz eindeutig und freiwillig erfolgen (Art. 7 DS-GVO, Art. 5 Abs. 5 DSG, Art. 6 Abs. 5 E-DSG). Die Voraussetzung der Eindeutigkeit wurde im E-DSG zwar neu aufgenommen, die Einwilligung kann in der Schweiz – anders als in der EU – aber weiterhin auch stillschweigend abgegeben werden.[28] Dies bedeutet, dass eine eindeutige Einwilligung weiterhin durch eine Willensäußerung durch konkludentes Verhalten gegeben werden kann, ein bloßes Schweigen oder Untätigkeit können allerdings nie als gültige Einwilligung gesehen werden.

2. Rechte und Pflichten nach E-DSG und DS-GVO

Obschon diverse Rechte und Pflichte der betroffenen Personen und der Datenverarbeiter im E-DSG gestärkt und präzisiert sowie teilweise an die europäischen Regelungen angenähert wurden, bestehen nach wie vor Unterschiede. Auf einige der wesentlichen soll nachfolgend eingegangen werden.

a) Datenschutz-Folgenabschätzung

Datenschutz-Folgenabschätzungen (DSFA) oder sog. Privacy Impact Assessments (PIA) sind an sich nichts Neues im Schweizer Datenschutzrecht.[29] Neu ist hingegen die gesetzlich definierte Pflicht, eine solche durchzuführen und die formellen Vorgaben an diese Durchführung. Die Pflicht zur Durchführung einer DSFA wird sowohl in der EU als auch der Schweiz durch den sog. risikobasierten Ansatz bestimmt und soll bestehen, wenn die fragliche Datenbearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann (Art. 20 Abs. 1 E-DSG, Art. 35 Abs. 1 DS-GVO).[30] Obschon die jeweiligen gesetzlichen Grundlagen versuchen, den Begriff des hohen Risikos zu konkretisieren, wird in der datenschutzrechtlichen Lehre kritisiert, dass weder der Begriff des hohen Risikos noch die Vorgehensweise bei der Risikobewertung genügend präzisiert seien.[31] Anders als der Entwurf des revidierten Schweizer DSG statuiert die DS-GVO in Art. 35 Abs. 4 die Pflicht der Aufsichtsbehörden, eine Liste mit denjenigen Verarbeitungsvorgängen zu erstellen, die in jedem Fall der Durchführung einer DSFA bedürfen. Die Listen sollen das Kriterium des „hohen Risikos" konkretisieren.[32] Da der *Europäische Datenschutzausschuss (EDSA)* bisher noch keine einheitliche Liste mit Kriterien verabschiedet hat,[33] müssen die EU-Mitgliedstaaten derzeit bekanntlich (noch) ihre eigenen „Muss-Listen" erstellen. Es ist davon auszugehen, dass diese Listen auch bei der Beurteilung des Erfordernisses zur Durchführung einer DSFA nach Art. 20 Abs. 1 E-DSG eine sinnvolle Auslegungshilfe werden darstellen können.

In einer DSFA ist insbesondere darzulegen, mit welchen Risiken die entsprechende Datenverarbeitung verbunden ist und mit welchen Maßnahmen diese Risiken adressiert werden sollen (Art. 20 Abs. 3 E-DSG, Art. 35 Abs. 7 DS-GVO). Ergibt die DSFA, dass die geplante Bearbeitung ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen zur Folge hätte, so muss der Verantwortliche vorgängig die Stellungnahme der Aufsichtsbehörde einholen (sog. Konsultationspflicht, Art. 21 Abs. 1 E-DSG, Art. 36 Abs. 1 i.V.m. Abs. 3 DS-GVO). An dieser Stelle sei indes auf eine Abweichung im E-DSG hingewiesen, wonach von der Konsultation in der Schweiz abgesehen werden kann, wenn der private Verantwortliche einen sog. Datenschutzberater[34] unternehmensintern im Einsatz hat und diesen vorgängig konsultiert hat (Art. 21. Abs. 4 E-DSG).

---

25 Das Recht auf informationelle Selbstbestimmung fließt aus dem Grundrecht auf Schutz der Privatsphäre, vgl. Art. 13 Bundesverfassung der Schweizerischen Eidgenossenschaft (BV) v. 18.4.1999; teilweise wird auch von „informationeller Integrität" gesprochen, vgl. *Wermelinger*, in: Baeriswyl/Pärli, Datenschutzgesetz, Stämpflis Handkomm., 1. Aufl. 2015, Art. 12 Rdnr. 2 m.w.Nw.; vgl. sodann statt vieler BGE 140 I 2, E. 9.1

26 Vgl. zum Ganzen BGE 138 II 346, E. 7.1 f.; ferner *Bühlmann/Schüepp*, PinG 2014, 49.

27 So können z.B. kantonale Meldepflichten im Tourismus keine gesetzliche Grundlage i.S.v. Art. 6 Abs. 1 lit. c DS-GVO bilden, sofern die DS-GVO auf die entsprechenden Datenbearbeitungen schweizerischer Tourismusbetriebe auf Grund von Art. 3 DS-GVO Anwendung findet; für die EU vgl. *Schulz* (o. Fußn. 24), Art. 6 Rdnr. 42; für die Schweiz (noch unter dem DSG, aber auch unter dem E-DSG relevant) vgl. *Wermelinger* (o. Fußn. 25), Art. 13 Rdnr. 16.

28 Botschaft (o. Fußn. 5), S. 7028; in der EU stellt ein bereits angekreuztes Kästchen oder das Stillschweigen bzw. die Untätigkeit der betroffenen Person grds. keine Einwilligung dar, vgl. Erwägungsgrund 32 DS-GVO.

29 Bundesorgane sind bereits heute dazu verpflichtet, vgl. Art. 7 DSG i.V.m. Art. 20 Abs. 2 Verordnung zum Bundesgesetz über den Datenschutz (VDSG) v. 14.6.1994, SR 235.11; *Rosenthal* (o. Fußn. 23), Rdnr. 48; die Pflicht für private Datenverantwortliche zur Durchführung einer DSFA konnte bisher vom Erfordernis angemessener technischer und organisatorischer Maßnahmen abgeleitet werden, vgl. Art. 7 DSG.

30 Botschaft (o. Fußn. 5), S. 6970; *Piltz*, in: Gola (o. Fußn. 24), Art. 24 Rdnr. 19; zum risikobasierten Ansatz vgl. *Gordon*, SJZ 114/2018, 162 ff., 164, oder *Veil*, ZD 2015, 447 ff., 448, oder *Löschhorn/Fuhrmann*, NZG 2019, 161 ff., 167.

31 Immerhin enthalten die Erwägungsgründe der DS-GVO gewisse Hinweise, vgl. Erwägungsgrund 75 und 76 sowie 89 DS-GVO. Im Weiteren finden sich in der Lit. auch Hilfestellungen zur Risikoskalierung, z.B. *Witt*, in: Koreng/Lachenmann, Formularhdb. Datenschutzrecht, 2. Aufl. 2018, S. 207 ff.; anders als in der EU liegt ein hohes Risiko in der Schweiz namentlich vor, wenn es zu einer umfangreichen Bearbeitung besonders schützenswerter Personendaten, zu einem Profiling oder zu einer systematischen Überwachung öffentlicher Bereiche kommt. In der EU sind dies lediglich Hinweise auf ein hohes Risiko, vgl. *Rosenthal* (o. Fußn. 23), Rdnr. 49.

32 Die Bedeutung der Listen ist aber zu relativieren (können jederzeit geändert werden, keine Gewissheit auf Vollständigkeit), *Hansen*, in: Wolff/Brink, BeckOK DatenschutzR, 26. Aufl. 2018, Art. 35 Rdnr. 34.

33 Derzeit ist der *EDSA* noch mit den Stellungnahmen zu den nationalen Listen beschäftigt, die indes zur Festlegung der Kriterien für eine einheitliche EU-Liste beitragen werden, vgl. Medienmitteilung des *EDSA* zur fünften Plenartagung v. 5.12.2018; die *Art. 29-Datenschutzgruppe*, Vorgänger des *EDSA*, hatte Risikogruppen definiert und empfiehlt die Durchführung einer DSFA, wenn mindestens zwei Gruppen einschlägig sind, vgl. Leitlinie der *Art. 29-Datenschutzgruppe* zu Datenschutz-Folgenabschätzungen v. 4.10.2017, S. 12.

34 Der Datenschutzberater überwacht die Einhaltung der Datenschutzvorschriften innerhalb eines Unternehmens und berät den Datenverantwortlichen in Datenschutzbelangen, wobei allerdings stets der Verantwortliche die alleinige Verantwortung für die datenschutzkonforme Bearbeitung trägt. Das E-DSG geht weniger weit als das europäische Recht, das in gewissen Fällen eine Pflicht zur Ernennung eines internen oder externen Datenschutzbeauftragten vorsieht, vgl. Botschaft (o. Fußn. 5), S. 7031 und Art. 37 DS-GVO.

b) Pflicht zur Meldung einer Datenschutzverletzung

Die Pflicht, Datenschutzverletzungen so rasch wie möglich der Aufsichtsbehörde zu melden, soll neu auch in der Schweiz eingeführt werden (Art. 22 E-DSG). Bislang erfolgten Meldungen in der Schweiz auf freiwilliger Basis. Eine Meldung soll gem. E-DSG fortan zwingend sein, wenn die Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt (Art. 22 Abs. 1. E-DSG). Die Schweizer Meldepflicht soll allerdings weniger weit gehen als jene der DS-GVO, da sie nur bei Vorliegen eines hohen Risikos vorgesehen ist (anders in der EU, wo jedes Risiko die Meldepflicht auslöst, vgl. Art. 33 Abs. 1 DS-GVO). Ähnlich wie hinsichtlich der Pflicht, eine DSFA durchzuführen (vgl. unter III.1.), wird auch hier die Schwierigkeit darin bestehen, das Vorliegen des (hohen) Risikos zu konkretisieren. In der EU muss zudem die betroffene Person bereits benachrichtigt werden, wenn die Verletzung ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat (Art. 34 Abs. 1 DS-GVO), wohingegen sie gemäß E-DSG in der Schweiz nur benachrichtigt werden muss, wenn dies zu ihrem Schutz erforderlich erscheint oder die Aufsichtsbehörde es verlangt (Art. 22 Abs. 4 E-DSG).

Auch betreffend die Meldefristen weicht die geplante neue Schweizer Regelung von der DS-GVO ab, da Verletzungen künftig bloß so rasch wie möglich zu melden sein sollen und keine maximale Frist vorgesehen ist (Art. 22 Abs. 1 E-DSG). Die DS-GVO verlangt indes eine unverzügliche Meldung, die spätestens innerhalb von 72 Stunden zu erfolgen hat (Art. 33 Abs. 1 DS-GVO).[35]

Obschon die Befugnisse der Schweizer Aufsichtsbehörde *(Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter – EDÖB)* im E-DSG gestärkt werden und mit den Befugnissen der europäischen Kontrollbehörden vergleichbar sind, wird ein Verstoß gegen die Meldepflicht in der EU mit Bußgeldern bestraft (83 Abs. 6 DS-GVO). In der Schweiz soll hingegen ein Verstoß nicht direkt sanktioniert werden (vgl. zum Schweizer Sanktionsansatz unter III.1.), der Aufsichtsbehörde soll nur die Möglichkeit eingeräumt werden, den säumigen Meldepflichtigen im Rahmen ihrer Ermittlungs- und Eingriffsbefugnisse unter Strafandrohung zur Einführung und Befolgung eines entsprechenden Meldeprozesses zu zwingen (vgl. Art. 44 E-DSG i.V.m. Art. 57 E-DSG). Zudem kann die Aufsichtsbehörde seine Verfügung unter Androhung einer Strafandrohung aussprechen (Art. 58 E-DSG).

Im Zusammenhang mit der Frage der zuständigen Aufsichtsbehörde ist der eingangs erwähnte extraterritoriale Geltungsbereich der DS-GVO und des (E-)DSG von besonderer Bedeutung (s. unter I.3.): Grundsätzlich gilt bei grenzüberschreitenden Datenbearbeitungen innerhalb der EU das sog. One-Stop-Shop-Prinzip (Art. 33 Abs. 1 i.V.m. Art. 56 DS-GVO). Dieses hat zur Folge, dass für Meldungen bei Datenschutzverletzungen ausschließlich die Aufsichtsbehörde der EU-Hauptniederlassung oder der einzigen EU-Niederlassung des Verantwortlichen als sog. federführende Behörde zuständig ist.[36] Im Verhältnis zu einem Verantwortlichen, der in der Schweiz und somit in einem Drittstaat niedergelassen ist, greift das Prinzip mangels (Haupt-)Niederlassung in der EU aber gerade nicht. In diesem Fall ist die Meldung nicht etwa der Schweizer Aufsichtsbehörde, sondern der Aufsichtsbehörde desjenigen Mitgliedstaats zu machen, in dem der EU-Vertreter gem. Art. 27 DS-GVO des Schweizer Datenverantwortlichen seinen Sitz hat.[37]

Im umgekehrten Fall, d.h. wenn ein EU-Datenverantwortlicher mit seinen Datenbearbeitungen (auch) dem Schweizer Recht untersteht, ist ebenfalls zu fragen, ob die Meldung an die eigene EU-Behörde oder an den *EDÖB* zu machen ist. Eine Pflicht zur Benennung eines Datenschutz-Vertreters analog zu Art. 27 DS-GVO existiert in der Schweiz nicht (weder nach altem noch nach neuem Recht).[38] Trotzdem ist auf Grund der extraterritorialen Wirkung des (E-)DSG (s. unter I.3.) der EU-Datenverantwortliche verpflichtet, die Datenschutzverletzungen im Anwendungsbereich der Schweizer Datenschutzgesetzgebung dem *EDÖB* zu melden. In beiden Fällen ist indes die Vollstreckung der Sanktionen problematisch, so kann die eine Aufsichtsbehörde (z.B. der *Schweizer EDÖB*) keine direkten Untersuchungshandlungen im Hoheitsgebiet der EU durchführen (und umgekehrt, vgl. Territorialitätsprinzip und Vollstreckung, unter I.3. und III.4.).

3. Betroffenenrechte

Der Ausbau und die Ausgestaltung der Betroffenenrechte orientieren sich im neuen Schweizer E-DSG an den Vorgaben der revidierten Europarats-Konvention (SEV-108) und decken sich größtenteils mit deren Ausgestaltung in der DS-GVO.

Anders als bisher und in Angleichung an das europäische Recht soll das neue Schweizer Datenschutzrecht nur noch für die Bearbeitung von Daten natürlicher Personen gelten, Daten von juristischen Personen[39] sollen künftig vom Anwendungsbereich des E-DSG ausgenommen sein (Art. 1 E-DSG).

Allerdings haben im EU-Raum Betroffene das Recht auf Datenübertragbarkeit (Art. 20 DS-GVO). Der *Bundesrat* hat dieses Recht nicht in den E-DSG aufgenommen. Er ist der Ansicht, dass die Datenübertragbarkeit in erster Linie darauf ausgerichtet sei, den betroffenen Personen die Wiederverwendung ihrer Daten zu ermöglichen (und so den Wettbewerb zu fördern), und nachgeordnet ihre Persönlichkeit zu schützen.[40] Es handle sich also aus Schweizer Perspektive vielmehr um einen verbraucherrechtlichen als einen datenschutzrechtlich begründeten Anspruch. Es ist allerdings nicht ausgeschlossen, dass das Recht auf Datenübertragbarkeit in der Schweiz zu einem späteren Zeitpunkt eingeführt wird. Der *Bundesrat* hat in diesem Zusammenhang ausdrücklich festgehalten, die Erfahrungen innerhalb der EU abwarten zu wollen.[41]

I.Ü. sind die Betroffenenrechte des (E-)DSG mit denjenigen in der DS-GVO vergleichbar, so z.B. das Berichtigungsrecht, das bisher vom Grundsatz der Richtigkeit der Daten (Art. 5 Abs. 2 DSG) abgeleitet wurde (wobei die Berichtigung stets auch die Löschung oder den Widerspruch beinhalten konnte) und neu bei den Rechtsansprüchen (Art. 28 Abs. 1 E-DSG) verankert ist. Das im Kontext der DS-GVO viel zitierte Recht auf Vergessenwerden war dem DSG schon implizit bekannt (es wurde vor al-

---

35 Die Überschreitung der Frist führt dazu, dass diese ggü. der Aufsichtsbehörde begründet werden muss, vgl. 33 Abs. 1 DS-GVO.

36 *Jandt*, in: Kühling/Buchner (o. Fußn. 13), Art. 33 Rdnr. 11; *Selmayr*, in: Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 56 Rdnr. 5-13.

37 Vgl. zur Zuständigkeit des EU-Vertreters die Leitlinien der *Art. 29-Datenschutzgruppe* für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der VO (EU) 2016/679, zuletzt überarbeitet und angenommen am 6.2.2018 (WP250rev.01), S. 18; *Selmayr* (o. Fußn. 36), Art. 56 Rdnr. 11.

38 Der *Bundesrat* hat sich zwar überlegt, eine solche Pflicht einzuführen (Erläuternder Bericht zum Vorentwurf für das Bundesgesetz über die Totalrevision des Datenschutzgesetzes und die Änderung weiterer Erlasse zum Datenschutz, 41), letztlich jedoch darauf verzichtet, weil andere gesetzliche Grundlagen die Benennung eines Zustellungsempfängers bereits zulassen (z.B. Art. 11b des Bundesgesetzes über das Verwaltungsverfahren (VwVG) v. 20.12.1968, SR 172.021 sowie Art. 140 Schweizerische Zivilprozessordnung (ZPO) v. 19.12.2008, SR. 272).

39 Vgl. zu den sich daraus im geltenden Recht ergebenden Konsequenzen bei der Qualifikation und Verarbeitung von IP-Adressen *Bühlmann/Schüepp* (o. Fußn. 19), S. 53 f.

40 Zur Datenportabilität vgl. *Kratz*, InTer 2019, 26 ff.; ob es nun ein wettbewerbsrechtliches oder datenschutzrechtliches Recht sei, wird in der Lit. krit. diskutiert, vgl. für den wettbewerbsrechtlichen Charakter z.B. *Dehmel/Hullen*, ZD 2013, 147, 153 und *Herbst*, in: Kühling/Buchner (o. Fußn. 13), Art. 20 Rdnr. 4; für den datenschutzrechtlichen Charakter, vgl. z.B. *Hennemann*, PinG 2017, 5 ff., 8; Botschaft (o. Fußn. 5), S. 6984.

41 Botschaft (o. Fußn. 5), S. 6984.

lem aus dem zivilrechtlichen Persönlichkeitsschutz abgeleitet[42]) und wird nunmehr explizit genannt (Anspruch auf Löschung, Art. 28 Abs. 2 lit. c E-DSG).[43]

4. Verbesserung grenzüberschreitenden Datenverkehrs

In Zukunft dürfen in der Schweiz Daten ins Ausland übermittelt werden, wenn der *Bundesrat* per Verordnung festgestellt hat, dass das empfangende Land oder das internationale Organ einen angemessenen Datenschutz gewährleisten (Art. 13 Abs. 1 E-DSG). Der *Bundesrat* wird die Situation periodisch evaluieren (ähnlich wie die *EU-Kommission*, Art. 45 DS-GVO).[44] Die vom *Bundesrat* erstellte Verordnung wird als Positiv-Liste zu verstehen sein, d.h. sie wird nur jene Staaten aufzählen, die über einen angemessenen Datenschutz verfügen (ebenso in der EU, Art. 45 DS-GVO).[45] Im Umkehrschluss bedeutet dies, dass ein Staat, der auf der Liste nicht genannt wird, entweder (noch) keiner Evaluation unterzogen wurde oder der *Bundesrat* zum Schluss gekommen ist, dass die Gesetzgebung des fraglichen Staats den Anforderungen der Gewährleistung eines angemessenen Schutzes nicht entspricht.[46]

Liegt kein solcher Beschluss vor, sieht der E-DSG, in Erweiterung zum aktuellen Recht[47] und in Angleichung an die DS-GVO, verschiedene Möglichkeiten vor, mit denen ein geeigneter Datenschutz gewährleistet werden kann, sodass die Weitergabe ins Ausland dennoch möglich ist (Art. 13 E-DSG). So kann angemessener Schutz durch einen völkerrechtlichen Vertrag gewährleistet werden[48] oder durch Ad-hoc- und standardisierte Garantien (Art. 13 Abs. 2 lit. b-d E-DSG). Andererseits kann die Bekanntgabe von Daten ins Ausland auch gestützt auf verbindliche unternehmensinterne Datenschutzvorschriften erfolgen (Art. 13 Abs. 2 lit. e E-DSG). Gleich wie in der EU müssen die Garantien bzw. die unternehmensinternen Datenschutzvorschriften in der Schweiz den Behörden mitgeteilt oder gar zur Genehmigung im Voraus vorgelegt werden.[49] Zuständig für die Genehmigung und den Erhalt der Mitteilung ist der *EDÖB* (Art. 13 Abs. 2 lit. b und d E-DSG).

III. Sanktionen und deren Vollstreckung

Verstöße gegen das Datenschutzrecht werden in der Schweiz privat-, straf- und aufsichtsrechtlich sanktioniert. Dies war bereits unter dem alten, aktuell noch geltenden DSG so und wird sich auch mit der laufenden Totalrevision nicht ändern. Im Nachfolgenden soll insbesondere auf die im E-DSG vorgesehene Ausgestaltung der straf- und aufsichtsrechtlichen Sanktionen näher eingegangen werden. Die privatrechtliche Durchsetzung erfolgt über Ansprüche aus zivilrechtlichem Persönlichkeitsschutz und erscheint rechtsvergleichend weniger bemerkenswert.

1. Keine Bußgelder analog zur DS-GVO – der Schweizer Sanktionsansatz

In Bezug auf die Sanktionierung und Durchsetzung des revidierten Datenschutzrechts enthält der E-DSG einen grundlegend anderen Weg als die DS-GVO. Zwar sollen die Sanktionen im Vergleich mit dem bisherigen Recht deutlich verschärft werden, das neue Schweizer Recht soll aber auch nach der Totalrevision des Datenschutzgesetzes keine (direkten) finanziellen Verwaltungssanktionen vorsehen.[50] Der Grund liegt darin, dass finanzielle Verwaltungssanktionen mit strafendem Charakter in der Schweizer Rechtsordnung grundsätzlich eine Ausnahme darstellen.[51] Auf Grund ihres Strafcharakters bedingen finanzielle Verwaltungssanktionen materielle und verfahrensrechtliche Garantien, welche das für die Durchsetzung des Datenschutzrechts maßgebliche Verwaltungsverfahren bislang nicht vorsieht.[52] Die Einführung von finanziellen Verwaltungssanktionen im E-DSG würde – so der Schweizer Gesetzgeber – den strafrechtlichen Grundsatzentscheid, wonach die Unternehmensstrafbarkeit eine subsidiäre sein soll (vgl. Art. 102 Schweizerisches Strafgesetzbuch – schweizStGB[53]), durch die Hintertüre des Verwaltungsrechts (zu) stark relativieren.[54] Der *Bundesrat* will deshalb an seiner bisherigen Praxis festhalten, wonach verwaltungsrechtliche Pflichten weiterhin mit dem Verwaltungsstrafrecht bzw. dem Nebenstrafrecht sicherzustellen sind.[55] Daraus ergibt sich eine deutlich schärfere Sanktionierung als in der DS-GVO, da sich die Schweizer Sanktionen gegen die handelnden, natürlichen Personen richten und nicht gegen die Unternehmen[56]. Dieser Grundsatzentscheid i.R.d. Totalrevision wurde im Vernehmlassungsverfahren breit kritisiert, da es nicht sachgerecht erscheint, die Sanktionierung datenschutzrechtlicher Vorgaben im Unternehmensalltag den handelnden Mitarbeitern anzudrohen. Der *Bundesrat* betont zwar bei jeder Gelegenheit, dass sich die Sanktionen nicht gegen die einzelnen Mitarbeiter richten sollen, sondern primär die Leitungspersonen treffen werden (Art. 29 schweizStGB i.V.m. Art. 6 des Bundesgesetzes über das Verwaltungsstrafrecht – schweizVStR[57]).[58] Dies ist jedoch umstritten und es kann nicht davon ausgegangen werden, solange die Sanktionierung auch datenschutzrechtliche Pflichten betrifft, die nicht nur den Verantwortlichen treffen, sondern jede an einer Datenbearbeitung mitwirkende Person.[59] Es ist anzunehmen, dass entsprechend auch Mitarbeiter unterer Stufen, die aber mit selbstständiger Entscheidungsbefugnis ausgestattet sind, strafbar gemacht werden.[60]

Zuständig für Strafverfahren sollen die kantonalen Strafbehörden sein (Art. 59 Abs. 1 E-DSG). Immerhin – und das ist neu – kann der *EDÖB* unter Strafandrohung Verwaltungsmaßnahmen verfügen (mit Bußen von bis zu CHF 250.000,–, vgl. Art. 57 E-DSG, zur verwaltungsrechtlichen Durchsetzung s. unter III.3.). Darüber hinaus kann der *EDÖB* der kantonalen Strafverfolgungsbehörde eine Anzeige erstatten (und im Verfahren die Rechte einer Privatklägerschaft wahrnehmen, vgl. Art. 59 Abs. 2 E-DSG).

---

42 BGE 109 II 353; 111 II 209 sowie 122 III 449; Botschaft (o. Fußn. 5), S. 7077.
43 Botschaft (o. Fußn. 5), S. 7077.
44 Botschaft (o. Fußn. 5), S. 7038.
45 Botschaft (o. Fußn. 5), S. 7038.
46 Nach aktuellem DSG existiert zwar ebenfalls eine Liste des Datenschutzbeauftragten, diese dient indes nur der Hilfestellung, vgl. Art. 7 VDSG (o. Fußn. 29); Botschaft (o. Fußn. 5), S. 7038.
47 Bereits nach aktuellem DSG bestehen verschiedene Möglichkeiten, vgl. Art. 6 Abs. 2 DSG.
48 Dazu zählt jedes internationale Abkommen, das einen Datenaustausch zwischen den Vertragsparteien vorsieht und materiell den Anforderungen der Europarats-Konvention entspricht, vgl. Botschaft (o. Fußn. 5), S. 7039.
49 Die Standarddatenschutzklauseln sowie die unternehmensinternen Datenschutzvorschriften müssen vorgängig genehmigt werden, vgl. Art. 13. Abs. 2 lit. b-d E-DSG.
50 Botschaft (o. Fußn. 5), S. 7092.
51 Die Ausnahmen bestehen z.B. im Schweizer Kartellrecht.
52 Botschaft (o. Fußn. 5), S. 7098.
53 Schweizerisches Strafgesetzbuch v. 21.12.1937 (schweizStGB), SR.311.0.
54 Botschaft (o. Fußn. 5), S. 7098.
55 Ausf. zur Qualifikation von finanziellen Verwaltungssanktionen *Niggli/Riedo*, in: Amstutz (et al.), Die Praxis des Kartellgesetzes im Spannungsfeld von Recht und Ökonomie, Quasi-Strafrecht, 2011, S. 91 ff.; Botschaft (o. Fußn. 5), S. 7098.
56 *Rosenthal* (o. Fußn. 23), Rdnr. 121 sowie insgesamt zum Schweizer Sanktionsansatz, Rdnr. 115 ff.
57 Bundesgesetz über das Verwaltungsstrafrecht v. 22.3.1974 (schweizVStR), SR.313.0
58 Botschaft (o. Fußn. 5), S. 7098 f.
59 *Rosenthal* (o. Fußn. 23), Rdnr. 122.
60 Nach hier vertretener Auffassung ist davon auszugehen, dass dies nicht gelingt und auch Mitarbeiter tieferer Stufen strafbar sein werden: Es ist allg. anerkannt, dass Art. 29 schweizStGB auch Mitarbeiter erfasst, die, ohne Organ zu sein, eine selbstständige Entscheidungsbefugnis in ihrem Tätigkeitsbereich haben, so z.B. der Mitarbeiter, der für die Beantwortung der Auskunftsgesuche als zuständig ernannt wird, vgl. statt vieler *Trechsel*, in: Trechsel/Pieth, Schweizerisches Strafgesetzbuch, Praxiskomm., 2. Aufl. 2018, Art. 39 Rdnr. 4; *Rosenthal* (o. Fußn. 23), Rdnr. 122.

2. Strafrechtliche Durchsetzung

Im Zuge der Revision wird die strafrechtliche Durchsetzung im Vergleich zur noch geltenden Rechtslage deutlich ausgebaut und verschärft. Im Vorentwurf war das strafrechtliche Sanktionssystem allerdings noch sehr viel weitgehender geplant. Auf Grund der breiten Kritik im Vernehmlassungsverfahren wurde nun aber der Katalog an sanktionierten Pflichtverletzungen eingeschränkt und insbesondere auf die Strafbarkeit fahrlässigen Verhaltens verzichtet.

Wie bereits nach geltendem Recht soll die Verletzung von Informations-, Auskunfts- und Mitwirkungspflichten strafbewehrt sein (Art. 34 DSG, Art. 54 E-DSG). Obwohl dies also nichts wirklich Neues ist, wird die Bedeutung stark zunehmen. Dies einerseits auf Grund des im Vergleich zum bisherigen Recht massiv ausgebauten Katalogs an Informationspflichten und andererseits auf Grund des stark erhöhten Bußgeldrahmens. Der Bußgeldrahmen liegt hier (sowie bei allen anderen Strafrechtsbestimmungen des E-DSG) bei CHF 250.000,– und ist somit massiv tiefer als in der EU (dort liegen die Bußen bei Verletzung der Auskunfts- und Mitwirkungspflichten bei 4% des weltweiten Umsatzes oder € 20 Mio., je nachdem, welcher Betrag höher ist, vgl. Art. 83 i.V.m. Art. 15 DS-GVO). Die Verletzung der Informations- und Auskunftspflichten ist nur auf Antrag strafbar (antragsberechtigt sind die betroffenen Personen).[61]

Neu soll sodann die Verletzung gewisser „Sorgfaltspflichten" unter Strafe gestellt werden (ebenfalls nur auf Antrag, Art. 55 E-DSG). Die Auswahl der entsprechend sanktionierten Pflichten erscheint etwas willkürlich. Zentrale Pflichten wie die Führung eines Verfahrensverzeichnisses, die Meldung von Datenschutzverstößen (Data Breach Notification) oder die Durchführung einer DSFA sind nicht erfasst. Die unter Strafe gestellten Sorgfaltspflichten umfassen hingegen die Pflichten im Zusammenhang mit dem grenzüberschreitenden Datenverkehr (Art. 13 Abs. 1-2 und 14 E-DSG), die Pflichten im Kontext von Auftragsdatenbearbeitungsverhältnissen (Art. 8 Abs. 1-2 E-DSG) und die Pflicht zur Einhaltung der Vorgaben des *Bundesrats* zur Datensicherheit (Art. 7 Abs. 3 E-DSG).[62]

Sodann soll die Verletzung der beruflichen Schweigepflicht neu umfassend unter Strafe gestellt werden (auf Antrag, Art. 56 E-DSG). Die neue Bestimmung soll alle geheimen Personendaten anderer schützen, die jemand auf Grund seines Berufs erfahren hat. Die Schweigepflicht soll weder eine vertragliche Geheimhaltungspflicht voraussetzen, noch müssen die Daten ein Geschäftsgeheimnis darstellen. Die Tatsache, dass die sich aus den Daten ergebenden Informationen nicht allgemein bekannt oder zugänglich sind, soll ausreichend sein, solange die betroffene Person ein schützenswertes Interesse hat und mit der Kundgabe nicht einverstanden ist.[63] Der Anwendungsbereich dieses neuen Berufsgeheimnisses ist enorm weit, es wird jedermann betreffen, der mit Personendaten im beruflichen Kontext in Berührung kommt. Eine Entbindungsmöglichkeit, analog zu den klassischen Berufsgeheimnissen (z.B. Anwaltsgeheimnis gem. Art. 321 schweizStGB) soll nicht bestehen. Der Bußgeldrahmen soll auch hier CHF 250.000,– betragen.

Schließlich ist festzuhalten, dass die Verletzung der Bearbeitungsgrundsätze in der Schweiz – anders als in der EU (vgl. Art. 83 Abs. 5 DS-GVO) – strafrechtlich nicht (direkt) sanktioniert sein soll. Die Zuständigkeit zur Rechtsdurchsetzung soll hier alleine bei der Aufsichtsbehörde liegen. Der *EDÖB* wird die Einhaltung der Bearbeitungsgrundsätze nur – aber immerhin – unter Strafandrohung verfügen können (Art. 57 E-DSG).

3. Verwaltungsrechtliche Durchsetzung

Die Befugnisse der Aufsichtsbehörde, d.h. des *EDÖB*, sollen im E-DSG gestärkt werden und sind künftig mit den Befugnissen der europäischen Kontrollbehörden vergleichbar.[64] Obschon er – wie bereits erwähnt – keine Bußen wird verhängen können, wird er immerhin ermächtigt, Verfügungen mit Strafandrohung zu erlassen (Art. 57 E-DSG). Der *EDÖB* erhält entsprechend neu umfassendere Untersuchungs- (Art. 43 und Art. 44 E-DSG) und Verfügungsbefugnisse (Art. 45 E-DSG), einschließlich der Befugnis, vorsorgliche Maßnahmen anzuordnen (Art. 44 Abs. 2 E-DSG). Bisher konnte der *EDÖB* nur Empfehlungen abgeben und musste beim *Schweizer Bundesverwaltungsgericht* den Erlass einer Verfügung beantragen (Art. 29 Abs. 4 DSG). Die neu vorgesehenen Interventionsmöglichkeiten des *EDÖB* sind im Vergleich zum bisherigen Recht also durchaus abschreckend.

4. Vollstreckung(sprobleme)

Obschon sowohl der (E-)DSG als auch die DS-GVO extraterritoriale Wirkung haben (s. unter I.3.), bedeutet dies noch nicht, dass die entsprechenden datenschutzrechtlichen Verfügungen oder Sanktionen gegen Unternehmen mit Sitz im Ausland ohne weiteres vollstreckt werden können.[65] Für die Frage der Vollstreckung im internationalen Verhältnis ist jeweils die Rechtsnatur der betreffenden Maßnahme bzw. Sanktion maßgeblich.[66]

Zivilrechtliche Entscheide können im Ausland auf Grund von völkerrechtlichen Verträgen oder anhand international-privatrechtlicher Bestimmungen des jeweiligen Vollstreckungslands vollstreckt werden (im Verhältnis zwischen der EU und der Schweiz ist hier insbesondere das Lugano-Übereinkommen maßgebend).[67]

Verwaltungsmaßnahmen einer Behörde können indes nur im eigenen Hoheitsgebiet Wirkung entfalten, weshalb ohne internationales Abkommen Verfügungen ausländischer Behörden grundsätzlich im internationalen Verhältnis nicht vollstreckt werden können.[68] Weder besteht derzeit ein solches Abkommen, noch ist wahrscheinlich, dass ein solches in naher Zukunft zu Stande kommen wird.[69] Immerhin ist es indes denkbar, dass der *Schweizer EDÖB* auf Information einer EU-Aufsichtsbehörde hin zum Schluss kommt, dass (auch) eine Verletzung nach Schweizer Recht vorliegt. Dies ermöglicht es dem *EDÖB* sodann, selbst aktiv zu werden.[70] Hinzuweisen ist in diesem Zusammenhang auf die Pflicht der Benennung eines EU-Vertreters gem. Art. 27 DS-GVO, sofern eine Datenbearbeitung im EU-Ausland auf Grund von Art. 3 DS-GVO vom Anwendungsbereich der Verordnung erfasst ist. Diese Pflicht relativiert die Vollstreckungsproblematik einseitig zu Gunsten der EU-Aufsichtsbehörden, denn weder das bisherige noch das geplante neue Schweizer Datenschutzrecht kennen eine vergleichbare Pflicht.

---

61 Der *EDÖB* hat zwar ein Anzeigerecht, vgl. Art. 59 Abs. 2 E-DSG, aber kein Strafantragsrecht, vgl. *Rosenthal* (o. Fußn. 23), Rdnr. 118.

62 Wie *Rosenthal* zutreffend ausführt, erscheint die Auswahl der unter Strafe gestellten Sorgfaltspflichten zufällig, vgl. *Rosenthal* (o. Fußn. 23), Rdnr. 118.

63 Botschaft (o. Fußn. 5), S. 7102.

64 Die Befugnisse sind im Hinblick auf die europäische Gesetzgebung ein entscheidendes Element, um sicherzustellen, dass die *EU-Kommission* den Angemessenheitsbeschluss ggü. der Schweiz erneuert bzw. bestätigt; Botschaft (o. Fußn. 5), S. 7092.

65 *Bühlmann/Reinle* (o. Fußn. 17), S. 10 f.

66 *Bühlmann/Reinle* (o. Fußn. 17), S. 11; *Benhamou/Jacot-Guillarmod,* digma 2018, 142 ff., 145.

67 *Bühlmann/Reinle* (o. Fußn. 17), S. 11.

68 Immerhin wurde beim *Parlament* eine Motion eingereicht „Gegen Doppelspurigkeiten im Datenschutzrecht", woraufhin der *Bundesrat* ausdrücklich festhielt, diesbezüglich Gespräche mit der EU „zu gegebener Zeit" aufnehmen zu wollen, vgl. zum Ganzen die Motion von Doris Fiala v. 28.9.2016; *Bühlmann/Reinle* (o. Fußn. 17), S. 11, insb. mit Hinweisen auf die Lit. zur Vollstreckung von ausländischen Straßenverkehrsmaßnahmen.

69 In Frage käme ein Abkommen ähnl. dem zwischen der Schweiz und der EU über die Zusammenarbeit bei der Anwendung ihres Wettbewerbsrechts, abgeschlossen am 17.5.2013. Das Abkommen sieht weitreichende Möglichkeiten des Informationsaustauschs vor; *Benhamou/Jacot-Guillarmod* (o. Fußn. 66), S. 145.

70 *Bühlmann/Reinle* (o. Fußn. 17), S. 11.

IV. Schlussbemerkungen

Die Schweiz hat guten Grund, den datenschutzrechtlichen Entwicklungen in der EU Rechnung zu tragen. Die Annäherung an die europäische Datenschutzgesetzgebung ist sowohl völkerrechtlich als auch auf Grund der engen wirtschaftlichen Verknüpfung mit der EU und ihren Mitgliedstaaten geboten. Die Annäherung ist eines der zentralen Kriterien, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt. Obwohl die laufende Revision des Schweizer Datenschutzrechts diese Annäherung zum zentralen Anliegen hat, werden datenbearbeitende Unternehmen dies- und jenseits der Grenze sich auf unterschiedliche Vorgaben einstellen müssen. Dies stellt insb. für Schweizer KMU eine große Herausforderung dar, wenn sie ihre Geschäftstätigkeit auch auf Kunden in der EU ausrichten.

Lukas Bühlmann, LL.M.,
ist Rechtsanwalt und leitet als Partner die Praxisgruppe Digital, Data Privacy & E-Commerce in der Kanzlei Meyerlustenberger Lachenal AG in Zürich.

Hatun Metin, MLaw,
ist Rechtsanwältin in der Praxisgruppe Digital, Data Privacy & E-Commerce in der Kanzlei Meyerlustenberger Lachenal AG in Zürich.

RECHTSPRECHUNG

BVerfG: Anspruch einer Partei auf Entsperren eines gesperrten Facebook-Accounts

GG Art. 2 Abs. 1, 3, 5 Abs. 1, 19 Abs. 4, 21 Abs. 1 Satz 1, 38; BVerfGG § 32 Abs. 1
Beschluss vom 22.5.2019 – 1 BvQ 42/19

Leitsätze der Redaktion

1. Es ist in der Rechtsprechung noch nicht geklärt, ob und ggf. welche rechtlichen Forderungen sich aus der mittelbaren Drittwirkung der Grundrechte im Verhältnis zwischen Privaten auch für Betreiber sozialer Netzwerke im Internet ergeben; etwa in Abhängigkeit vom Grad deren marktbeherrschender Stellung, der Ausrichtung der Plattform, des Grads der Angewiesenheit auf eben jene Plattform und den betroffenen Interessen der Plattformbetreiber und sonstiger Dritter.

2. Die Nutzung eines Facebook-Accounts ist für eine Partei – jedenfalls im Vorfeld von Wahlen – für die Verbreitung ihres politischen Programms von wesentlicher Bedeutung.

Anm. d. Red.: Der Volltext ist abrufbar unter: BeckRS 2019, 9558.

Sachverhalt

Die Ast. greift zum Zweck der Stellungnahme zum aktuellen politischen Tagesgeschehen und der Berichterstattung über ihre Parteiarbeit auf das in Deutschland weit verbreitete soziale Netzwerk Facebook (Ag.) zurück. Mit ihrem Eilantrag wendet sie sich gegen die Löschung eines ihrer Beiträge und die anschließende Sperrung ihres Nutzeraccounts durch die Ag. Am 21.1.2019 veröffentlichte die Ast. unter dem in ihrem Namen betriebenen Nutzeraccount einen Link zu einem Artikel auf ihrer Internetseite, der den Titel „Winterhilfestand in Zwickau-Neuplanitz" trägt. Darin heißt es u.a.:

Accountentsperrung
Politischer Diskurs
Privatautonomie
Strafbare Äußerungen

„Im Zwickauer Stadtteil Neuplanitz gibt es zahlreiche Menschen, die man landläufig wohl als sozial und finanziell abgehängt bezeichnen würde. Während nach und nach immer mehr art- und kulturfremde Asylanten in Wohnungen in den dortigen Plattenbauten einquartiert wurden, die mitunter ihrer Dankbarkeit mit Gewalt und Kriminalität Ausdruck verleihen, haben nicht wenige Deutsche im Viertel kaum Perspektiven ..."

Unmittelbar nach der Veröffentlichung teilte die Ag. der Ast. mit, dass der Beitrag als „Hassrede" gegen die Gemeinschaftsstandards verstoße. Die Sichtbarkeit des Beitrags sei daher eingeschränkt und das Veröffentlichen von Beiträgen für 30 Tage gesperrt worden. Auf Einspruch der Ast., der unter Verweis auf die Meinungsfreiheit der Ast. begründet wurde, erfolgte am 30.1.2019 die Löschung des Nutzerkontos, dessen Inhalt seitdem nicht mehr verfügbar ist.

Nach erfolgloser Abmahnung beantragte die Ast. sodann vor dem *LG* den Erlass einer einstweiligen Verfügung mit dem Inhalt, die Ag. unter Androhung von Ordnungsmitteln zu verpflichten, den Auftritt der Ast. zu entsperren und ihr die Nutzung wieder einzuräumen sowie der Ag. zu untersagen, den Auftritt wegen des Teilens des genannten Beitrags zu sperren, die Nutzung der Funktionen von Facebook vorzuenthalten oder den Beitrag zu löschen bzw. dessen Sichtbarkeit einzuschränken. Das *LG* wies den Antrag mit B. v. 8.3.2019 zurück. Mit B. v. 17.4.2019 wies das *OLG* die sofortige Beschwerde der Ast. zurück. Mit ihrem Antrag auf Erlass einer einstweiligen Anordnung verfolgt die Ast. ihr Begehr fort.

Aus den Gründen

11 1. Gem. § 32 Abs. 1 BVerfGG kann das *BVerfG* im Streitfall einen Zustand durch einstweilige Anordnung vorläufig regeln, wenn dies zur Abwehr schwerer Nachteile, zur Verhinderung drohender Gewalt oder aus einem anderen wichtigen Grund zum gemeinen Wohl dringend geboten ist. ...

14 a) Eine ggf. noch zu erhebende Vb ist weder von vornherein unzulässig noch offensichtlich unbegründet. Es erscheint vielmehr nicht ausgeschlossen, dass die angegriffene Entscheidung des *OLG* mit dem GG unvereinbar ist, soweit dieses den Antrag auf Erlass einer einstweiligen Anordnung mit dem Ziel der Ermöglichung einer weiteren Nutzung des Internetangebots www.facebook.com durch die Ast. verneint hat.

15 Die angegriffenen Entscheidungen betreffen die Gewährung von einstweiligem Rechtsschutz in einem Rechtsstreit zwischen sich als Private gegenüberstehenden Parteien über die Reichweite der zivilrechtlichen Befugnisse des Betreibers eines sozialen Netzwerks, das innerhalb der Bundesrepublik Deutschland über