Astrid Epiney

Datenschutz in der EU und die Schweiz

Zur Bedeutung des Datenschutzrechts der EU für die Schweiz

Das Datenschutzrecht in der EU ist mittlerweile sehr differenziert und umfasst sowohl primär- als auch sekundärrechtliche Vorgaben, welche auch für die Schweiz von Bedeutung sind. Nachfolgend werden die Rechtsgrundlagen in der EU skizziert, bevor die Mechanismen der Implikationen des EU-Rechts für die Schweiz aufzeigt werden und auf die von der Rechtsprechung des EuGH bislang erörterten Themata hingewiesen wird. Deutlich wird damit, dass die Schweiz sehr wohl von den Rechtsentwicklungen in der Union durchaus in bedeutender Weise betroffen ist.

La législation applicable à la protection des données dans l'UE est désormais très diversifiée et comprend des dispositions, tant de droit primaire que de droit dérivé, qui revêtent également une importance pour la Suisse. Le présent article esquisse ci-après les bases juridiques au sein de l'UE, avant d'illustrer par quels mécanismes le droit de l'UE a des implications pour la Suisse et d'évoquer, enfin, les thèmes abordés jusqu'ici par la jurisprudence de la CJUE. Il apparaît ainsi clairement que la Suisse est bel et bien concernée de manière significative par les développements juridiques au sein de l'Union européenne.

I. Einleitung

Die Europäische Union ist bereits relativ früh mit dem Erlass der RL 95/46 im Jahr 1995 im Bereich des Datenschutzes tätig geworden, und seitdem haben sich die Rechtsgrundlagen nicht nur weiterentwickelt, sondern auch in beachtlicher Form ausdifferenziert. Meilenstein ist hier zweifellos der Erlass der sog. Datenschutzgrundverordnung (VO 2016/679); zu beachten sind aber auch die zahlreichen sektoriellen Regelungen, z.B. im Bereich der polizeilichen Zusammenarbeit oder des SIS.[1] Auch die Rechtsprechung des Europäischen Gerichtshofs (EuGH) hat sich mittlerweile in zahlreichen Urteilen mit grundlegenden datenschutzrechtlichen Fragen befasst und mitunter in seiner in ihrer Bedeutung weit über die EU hinausreichenden Rechtsprechung eine Reihe grundsätzlicher Fragen thematisiert und (teilweise) geklärt.

Astrid Epiney, Prof. Dr. iur., Institut für Europarecht, Universität Freiburg/CH.

Die Schweiz ist zwar als Nicht-EU-Mitglied weder an das EU-Recht als solches gebunden, noch entfalten die Urteile des EuGH für sie verbindliche Wirkung. Nichtsdestotrotz sind die Rechtsentwicklungen in der Union (auch) in diesem Bereich für die Schweiz aus verschiedenen Gründen von zentraler Bedeutung.

Vor diesem Hintergrund will der vorliegende Beitrag – auf der Grundlage der Skizzierung der Rechtsgrundlagen in der EU (II.) – die Implikationen des EU-Rechts für die Schweiz aufzeigen (III.), bevor auf die von der Rechtsprechung des EuGH bislang erörterten Themata hingewiesen wird (IV.) und der Beitrag mit einer kurzen Schlussbemerkung (V.) schliesst.[2]

II. Datenschutzrecht in der EU im Überblick

Im Unionsrecht finden sich den Datenschutz betreffende Regelungen sowohl im Primärrecht (1.) als auch im Sekundärrecht (2.). Ausgespart werden soll im Folgenden allerdings eine Erörterung der Kompetenzgrundlagen. Ebenso wenig wird auf einige neuere und zukunftsweisende Tendenzen im Sekundärrecht – wobei es insbesondere um einen allgemeinen Regelungsrahmen für Daten (unabhän-

1 Vgl. für einen Überblick über das EU-Datenschutzrecht – neben den einschlägigen Kommentaren zur Datenschutzgrundverordnung – C. Copain-Héritier, Le cadre européen de la protection des données entre forces et faiblesses intrinsèques, RUE 2021, 163 ff.; C. de Terwangne, La nouvelle loi suisse de protection des données dans le contexte international (Convention 108+ et RGPD), in: A. Epiney/S. Moser/S. Rovelli (Hg.), Die Revision des Datenschutzgesetzes des Bundes, Zürich 2022, 47 ff., jeweils m.w.N.

2 Die nachfolgenden Ausführungen greifen teilweise bereits früher durchgeführte Untersuchungen auf. S. insbesondere A. Epiney/N. Frei, Die Datenschutzgrundverordnung: Grundsätze und ausgewählte Aspekte, in: A. Epiney/S. Rovelli (Hg.), Datenschutzgrundverordnung (DSGVO): Tragweite und erste Erfahrungen, Zürich 2020, 1 ff.

gig davon, ob es sich um Personendaten handelt) sowie um Künstliche Intelligenz geht – eingegangen; die diesbezüglichen Arbeiten sind noch nicht abgeschlossen, wenn auch die Kommission bereits diverse Initiativen ergriffen hat.[3]

1. Primärrecht

In der Union wird der Persönlichkeitsschutz der Betroffenen (nunmehr) in Art. 7 und 8 GRCh geregelt: Während Art. 7 GRCh das Recht auf Achtung des Privat- und Familienlebens verankert und insoweit Art. 8 EMRK entspricht, enthält Art. 8 GRCh das Recht auf Schutz personenbezogener Daten. Der Gerichtshof prüft beide Bestimmungen in der Regel zusammen, und seine bisherige Rechtsprechung illustriert die Bedeutung dieser Grundrechte – die bei der Auslegung des Sekundärrechts zu beachten sind – trefflich.

So prüfte der EuGH verschiedentlich Sekundärrechtsakte am Massstab dieser Grundrechte:[4]

- In der Rs. C-293/12[5] erklärte der EuGH die sog. Vorratsdatenspeicherungs-Richtlinie[6] für ungültig, da der Eingriff nicht erforderlich sei, wobei der EuGH auch die besondere Bedeutung des Schutzes personenbezogener Daten für das Grundrecht auf Achtung des Privatlebens betonte und angesichts des Ausmasses und der Schwere des vorgesehenen Eingriffs in diese Grundrechte davon ausgeht, dass der Gestaltungsspielraum des Unionsgesetzgebers eingeschränkt sei.
- Auch in den verb. Rs. C-203/15 und C-658/15[7] ging es um die Vorratsdatenspeicherung, dies jedoch in Bezug auf eine mitgliedstaatliche Vorschrift. Im Anschluss an sein Urteil in der Rs. C-293/12 hielt der Gerichtshof fest, es stehe nicht mit Art. 15 Abs. 1 RL 2002/58 (Datenschutzrichtlinie im Bereich der elektronischen Kommunikation)[8] in Einklang, zum Zweck der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten vorzusehen.
- In der Rs. C-207/16[9] betonte der Gerichtshof im Zusammenhang mit der Auslegung des eine Beschränkung der Persönlichkeitsrechte ermöglichenden Art. 15 Abs. 1 RL 2002/58, die Verpflichtung, öffentlichen Stellen Zugang zu Daten zu gewähren, anhand derer die Identität der Inhaber von SIM-Karten, die mit einem gestohlenen Mobiltelefon aktiviert wurden, festgestellt wurde (wie Name, Vorname und ggf. Adresse der Karteninhaber), stelle zwar einen Eingriff in Art. 7 und 8 GRCh dar; dieser lediglich die Ermittlung der Identität betreffende Eingriff wiege aber nicht so schwer, dass er nur zur Bekämpfung schwerer Kriminalität zulässig wäre. Im Umkehrschluss – was der Gerichtshof auch ausdrücklich betont – können schwere Eingriffe nur durch die Bekämpfung schwerer Kriminalität gerechtfertigt werden, wobei in Bezug auf die Telekommunikation ein solcher schwerer Eingriff jedenfalls dann vorliege, wenn die Daten Schlüsse auf das Privatleben der Betroffenen erlauben, was wohl bei einem «umfassenden» Zugang zu Daten im Zusammenhang mit dem Mobiltelefon (neben Kommunikationsinhalten wohl auch schon die Ortung) zu bejahen ist.
- In der Rs. C-362/14[10] («Safe-Harbor») hielt der Gerichtshof insbesondere fest, auch im Falle der Übermittlung von Daten in einen Drittstaat sei ein hohes Schutzniveau zu gewährleisten, das zwar nicht identisch mit demjenigen der RL 95/46 sein, jedoch einen gleichwertigen Schutz bieten müsse. In den USA könne das Konzept des Safe Harbour kein solches angemessenes Schutzniveau gewährleisten.
- In dem auf Antrag des Europäischen Parlaments erstellten Gutachten 1/15[11] ging es um das geplante Abkommen zwischen Kanada und der EU über die Übermittlung und Verarbeitung von Fluggastdatensätzen. Die in dem Abkommen vorgesehene Übermittlung von Fluggastdatensätzen (die recht umfangreiche Informationen über die Fluggäste beinhalten) an die zuständige kanadische Behörde sowie deren Speicherung und Verwendung (unter Einschluss der Weiterleitung an andere Behörden in Kanada, in der EU oder in Drittstaaten) stelle einen Eingriff in Art. 7 und 8 GRCh dar. Dieser könne grundsätzlich gerechtfertigt werden, dies allerdings nicht durch die Einwilligung der Fluggäste (haben diese ihre Daten doch lediglich mit Blick auf die Abwicklung ihrer Flugreise bekanntgegeben), sondern durch das Abkommen selbst, das eine gesetzliche Grundlage im Sinne der Art. 8 II und 52 I GRCh darstelle. Auch würden im Allgemeinwohl liegende Ziele verfolgt, denn die vorgesehene Datenverarbeitung diene der öffentlichen Sicherheit (Bekämpfung terroristischer Aktivitäten und schwerer grenzüberschreitender Kriminalität). Der Wesensgehalt der Art. 7 und 8 GRCh sei nicht betroffen, da nur gewisse Aspekte des Privatlebens erfasst würden und die Datenverarbeitung nur zur bestimmten, im Abkommen umschriebenen Zwecken erfolgen dürfe und zudem Regelungen zur Sicherheit, Vertraulichkeit und Integrität der Daten vorgesehen seien. Allerdings lasse es das geplante Abkommen auch zu, dass sensible Daten (die im Abkommen definiert sind und z.B. die rassische oder ethnische Herkunft, die Religion oder das Sexualleben erfassen) übermittelt und verwendet werden. Eine Massnahme, die auf der Annahme beruht, dass eines dieser sensiblen Merkmale unabhängig vom konkreten Verhalten des Betroffenen für das Ziel des Schutzes der öffentlichen Sicherheit relevant sein könnte, verstosse jedoch gegen Art. 7, 8 und 21 GRCh (andere Rechtferti-

3 Vgl. hierzu A. Müller, Der Artifical Intelligence Act der EU: Ein risikobasierter Ansatz zur Regulierung von künstlicher Intelligenz, EuZ 1/2022; R. Weber, Künstliche Intelligenz: Regulatorsiche Überlegungen zum «Wie» und «Was», EuZ 1/2022; M. Hennemann/B. Steinrötter, Data Act – Fundament des neuen Datenwirtschaftsrechts?, NJW 2022, 1481 ff.
4 Vgl. insoweit ausführlich Epiney/Frei (Fn. 2), 2 ff.
5 EuGH vom 8. April 2014, C-293/12, «Digital Rights Ireland».
6 RL 2006/24/EG über die Vorratsspeicherung von Daten, ABl. 2006 L 105/54.
7 EuGH vom 21. Dezember 2016, C-203/15 und C-658/15, «Tele2 Sverige».
8 ABl. 2002 L 201, 37.
9 EuGH vom 2. Oktober 2018, C-207/16, «Ministerio Fiscal».
10 EuGH vom 6. Oktober 2015, C-362/14, «Schrems».
11 Gutachten 1/15 vom 26. Juli 2017.

gungsgründe seien vorliegend nicht ersichtlich). Weiter sei der Umfang der zu übermittelnden Daten teilweise nicht hinreichend bestimmt. Schliesslich formuliert der Gerichtshof eine Reihe von Voraussetzungen, denen das Abkommen Rechnung tragen müsse, damit die Übermittlung von Fluggastdatensätzen mit Art. 7 und 8 GRCh vereinbar ist, so u.a. in Bezug auf die Präzision der zu übermittelnden Daten, die automatisierte Verarbeitung, die verfahrensrechtlichen Gewährleistungen, die Speicherung der Daten nach der Ausreise (die nur bei Anhaltspunkten, dass von den Betroffenen eine Gefahr ausgeht, zulässig sei), die Weitergabe an Empfänger in Drittstaaten (hinreichendes Datenschutzniveau), die Information der Betroffenen und der Einbezug einer unabhängigen Kontrollstelle.

2. Sekundärrecht: die Datenschutzgrundverordnung

Die 2016 erlassene und seit 2018 massgebliche sog. Datenschutzgrundverordnung (VO 2016/679),[12] welche die aus dem Jahr 1995 stammende Datenschutzrichtlinie RL 95/46[13] ablöste, führte zu einer grundlegenden Revision der datenschutzrechtlichen Vorgaben in den EU-Mitgliedstaaten, wobei diese auch für Drittstaaten relevant sind.[14] Die VO 2016/679 knüpft zwar an die bestehenden Regelungen an, so dass insbesondere auch die bisherige, zur RL 95/46 ergangene Rechtsprechung[15] im Wesentlichen nach wie vor relevant ist; jedoch sind sowohl in struktureller als auch in inhaltlicher Hinsicht durchaus bedeutende Weiterentwicklungen zu konstatieren, die auch Implikationen für und in der Schweiz entfalten.

Auch beim Anwendungsbereich – sieht man von der neu geregelten extraterritorialen Anwendung ab[16] – knüpft die VO 2016/679 weitgehend an die RL 95/46 an, so dass sie insbesondere auch in Bezug auf Sachverhalte, die als solche keinerlei grenzüberschreitenden Bezüge aufweisen, anwendbar ist und somit umfassend auch Vorgaben für das rein innerstaatliche Datenschutzrecht enthält, dies z.B. im Zusammenhang mit der Veröffentlichung des Jahreseinkommens von Angestellten der öffentlichen Verwaltung[17] oder betreffend die Verarbeitung öffentlicher Daten durch öffentliche Stellen für die Anwendung aufenthaltsrechtlicher Vorschriften und statistische Zwecke.[18]

Allerdings griff der Unionsgesetzgeber bei der Revision der datenschutzrechtlichen Vorgaben nicht mehr auf das Instrument der Richtlinie, sondern – letztlich mit Blick auf eine weitergehende Harmonisierung (vgl. Erw. 9 f. VO 2016/679)[19] – auf dasjenige der Verordnung zurück. Verordnungen entfalten nach Art. 288 AEUV unmittelbare Geltung in den Mitgliedstaaten, so dass die Bestimmungen der Verordnung als solche in den Mitgliedstaaten anzuwenden sind und somit keiner Umsetzung bedürfen. Dies impliziert auch, dass die Verordnung Behörden und Einzelne berechtigen und verpflichten kann. Freilich ist damit nicht ausgeschlossen, dass gewisse Bestimmungen der Verordnung der mitgliedstaatlichen Durchführung bedürfen oder eine solche zumindest sachdienlich sein kann. Denn Verordnungen können Vorgaben sehr unterschiedlicher Art enthalten, so – neben direkt anwendbaren Bestimmungen – auch solche, die es den Mitgliedstaaten aufgeben bzw. erlauben, bestimmte Massnahmen zu ergreifen.[20] Ein Beispiel in der Datenschutzgrundverordnung ist die in Art. 51 ff. DGVO enthaltene Verpflichtung der Mitgliedstaaten, eine oder mehrere unabhängige Aufsichtsbehörden vorzusehen, denen bestimmte Befugnisse zukommen müssen.

Wie bereits die RL 95/46,[21] stellt die VO 2016/679 (wie sich schon aus ihrer Zielsetzung, (auch) den freien Datenverkehr sicherzustellen, ergibt) eine sog. Vollharmonisierung dar, die in ihrem Anwendungsbereich den Schutzstandard abschliessend regelt, so dass auch eine Abweichung «nach oben» nicht zulässig ist. Allerdings enthalten verschiedene Bestimmungen der Verordnung die Harmonisierungswirkung der Richtlinie relativierende «Erlaubnisvorbehalte», wonach es den Mitgliedstaaten offensteht, in der betreffenden Frage und im vorgesehenen Ausmass ggf. auch ein erhöhtes Schutzniveau anzulegen bzw. dieses zu spezifizieren. Beispielhaft erwähnt seien das Einwilligungsalter bei Kindern, Datenschutz im Zusammenhang mit Arbeitsverhältnissen oder gewisse Aspekte der Meldepflicht bei Datenschutzverletzungen.

Die Relevanz bzw. die Bedeutung des abschliessenden Charakters der Verordnung kann – noch mit Bezug auf die RL 95/46 – durch die Rs. C-582/14[22] illustriert werden. Der Gerichtshof hielt hier zunächst fest, dass auch eine dynamische IP-Adresse ein personenbezogenes Datum darstelle,

12 VO 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. 2016 L 119, 8. Die Literatur zur Datenschutzgrundverordnung ist mittlerweile kaum noch überschaubar; insbesondere existiert eine Reihe von Kommentaren. Vgl. schon die Nachweise in Fn. 1, 2.

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

14 S. insoweit auch noch unten III.

15 S. die Nachweise unten IV.

16 Hierzu noch unten III.

17 Mit Bezug zur RL 95/46 EuGH vom 20. Mai 2003, C-465/00, C-138/01 und C-139/01, «Österreichischer Rundfunk».

18 Mit Bezug zur RL 95/46 EuGH vom 16. Dezember 2008, C-542/06, «Huber».

19 Wobei anzumerken ist, dass das «Harmonisierungsdefizit» der RL 95/46 weniger auf dem Instrument der Richtlinie, denn auf den in dieser eingeräumten Spielräumen beruhte; da auch die VO 2016/679 zahlreiche «Öffnungsklauseln» enthält, die es den Mitgliedstaaten erlauben, in bestimmten Bereichen bzw. in Bezug auf gewisse Fragen die Vorgaben der Verordnung zu konkretisieren, zu spezifizieren, zu ergänzen oder/und zu verschärfen, ist denn auch die Harmonisierungswirkung der Verordnung zumindest in gewissen Bereichen weniger weitgehend als häufig angenommen. Vgl. in diesem Zusammenhang F. Detmering/A. Splittgerber, DSGVO und nationale Umsetzungsgesetze, digma 2018, 172 ff., die insgesamt rund 70 Öffnungsklauseln zählen.

20 Zur Zulässigkeit solcher Bestimmungen auch in Verordnungen z.B. EuGH vom 1. November 2001, C-403/98, «Azienda Agricola Monte Arcosu», Rn. 26; zur Zulässigkeit bzw. Notwendigkeit mitgliedstaatlicher Durchführungsmassnahmen z.B. EuGH, Rs. C-541/16 (Kommission/Dänemark).

21 S. EuGH vom 12. April 2018, C-468/10 und C-469/10, «ASNEF».

22 EuGH vom 19. Oktober 2016, C-582/14, «Breyer».

dies soweit der Nutzer anhand von Zusatzinformationen bestimmbar sei und diese Informationen aus tatsächlicher und rechtlicher Sicht zugänglich seien. Weiter sehe Art. 7 RL 95/46 eine erschöpfende und abschliessende Liste derjenigen Fälle vor, in denen eine Verarbeitung personenbezogener Daten als rechtmässig anzusehen sei, so dass die Mitgliedstaaten weder neue bzw. weitere Zulässigkeitsgründe einführen noch zusätzliche Bedingungen stellen dürften, welche die Tragweite einer der in dieser Bestimmung enthaltenen Grundsätze modifizieren würde.[23] Daher sei es nicht mit der RL 95/46 vereinbar, wenn ein Anbieter von Online-Mediendiensten ohne Einwilligung des Nutzers dessen personenbezogene Daten nur verarbeiten dürfe, um die Inanspruchnahme der Dienstleistungen zu ermöglichen und die Abrechnung sicherzustellen (mit der Folge, dass z.B. eine Verarbeitung zur Gewährleistung der generellen Funktionsfähigkeit eines Online-Mediendienstes nicht zulässig wäre), stehe Art. 7 lit. f RL 95/46 doch einer mitgliedstaatlichen Regelung entgegen, die kategorisch und ganz allgemein die Verarbeitung bestimmter personenbezogener Daten ausschliesse, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen, so dass ein Mitgliedstaat das Ergebnis der Abwägung dieser Rechte und Interessen nicht abschliessend vorschreiben dürfe, ohne es zu ermöglichen, dass das Ergebnis aufgrund besonderer Umstände des Einzelfalls anders ausfalle.

Inhaltlich betreffen die wesentlichen Neuerungen der Datenschutzgrundverordnung den Anwendungsbereich, die Rechte der Betroffenen, die Pflichten der Datenverarbeiter sowie Durchsetzung und Sanktionen. In unserem Zusammenhang von besonderer Bedeutung ist die neu in Art. 3 Abs. 2 VO 2016/679 vorgesehene extraterritoriale Anwendung: Danach findet die Verordnung auch auf die Verarbeitung der Daten von Personen («betroffene Personen»), die sich in der Union befinden, Anwendung, wenn die Datenverarbeitung «im Zusammenhang damit steht», dass den Personen Waren oder Dienstleistungen in der Union angeboten werden (unabhängig von Zahlungsflüssen) oder dass ihr Verhalten in der Union beobachtet wird. Eine Niederlassung des Datenverarbeiters oder des Auftragsverarbeiters in der Union ist in dieser Konstellation nicht notwendig. Angestrebt wird damit ein umfassenderer Schutz der Persönlichkeitsrechte der sich im Hoheitsgebiet der Union bzw. ihrer Mitgliedstaaten aufhaltenden Personen vor potentiellen Eingriffen durch ausserhalb der Union niedergelassene Datenverarbeiter. Diese neue Bestimmung bringt eine Ausdehnung des Anwendungsbereichs der Datenschutzgrundverordnung auf Personen und Sachverhalte mit sich, die vollumfänglich ausserhalb des Hoheitsgebiets der Union bzw. ihrer Mitgliedstaaten angesiedelt sind, so dass es insofern um Normen mit extraterritorialer Wirkung geht, was unter gewissen Voraussetzungen – die hier vorliegen dürften – völkerrechtlich zulässig ist.

Diese mit der neuen Bestimmung einhergehende beträchtliche Ausweitung des Anwendungsbereichs der Datenschutzgrundverordnung – die letztlich impliziert, dass viele Wirtschaftsteilnehmer und öffentliche Stellen in Drittstaaten die Vorgaben der Verordnung bei zahlreichen ihrer Datenverarbeitungen einhalten müssen – wirft jedoch auch einige Fragen auf, so insbesondere diejenigen nach den genauen Voraussetzungen, bei deren Vorliegen davon ausgegangen werden kann, dass Waren oder Dienstleistungen in der Union angeboten werden, wie der geforderte Zusammenhang ausgestaltet sein muss und was genau unter «Dienstleistungen» zu verstehen ist.[24]

Hingewiesen sei weiter darauf, dass die VO 2016/679 – wie bereits bislang die RL 95/46 – auf die Verarbeitung personenbezogener Daten Anwendung findet, soweit diese «im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt» (Art. 3 Abs. 1 DGVO), wobei die Verarbeitung selbst nicht in der Union stattfinden muss. Entscheidender Anknüpfungspunkt ist somit einerseits die Niederlassung in der Union, wobei eine feste Einrichtung mit einer gewissen Stabilität ausreichend sein dürfte; andererseits muss die Verarbeitung im Rahmen dieser Niederlassung erfolgen, wobei es genügt, dass die Verarbeitung im Zusammenhang mit einer effektiven und tatsächlichen Tätigkeit der Niederlassung steht. Die Tätigkeit der Niederlassung kann dabei nur geringfügig sein und auch der Zusammenhang kann eher lose ausfallen. Die Anforderungen sind daher eher gering, wie auch die Rechtsprechung des EuGH illustriert.[25]

III. Implikationen des EU-Datenschutzrechts für die Schweiz

Die Schweiz ist über die sog. Schengen- und Dublinassoziierung[26] auch an datenschutzrechtliche Vorgaben des EU-Rechts gebunden,[27] soweit diese in den Anhängen der Abkommen entsprechend vermerkt sind, womit die entsprechenden Rechtsakte Teil des sog. Schengen- und Dublin-Be-

23 S. insoweit auch schon EuGH vom 12. April 2018, C-468/10 und C-469/10, «ASNEF».

24 Vgl. im Einzelnen zum Problemkreis z.B. S. Métille/A. Ackermann, RGPD: application territoriale et extraterritoriale, in: A. Epiney/S. Rovelli (Hg.), Datenschutzgrundverordnung (DSGVO): Tragweite und erste Erfahrungen, Zürich 2020, 77 ff.

25 Vgl. EuGH vom 13. Mai 2014, C-131/12, «Google Spain und Google Inc.» (im Zusammenhang mit einer Suchmaschine); EuGH vom 1. Oktober 2015, C-230/14, «Weltimmo» (in Bezug auf den Betrieb von Webseiten).

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

27 Vgl. schon A. Epiney, Datenschutz und «Bilaterale II», SJZ 2006, 121 ff.; S. Füzesséry Minelli/S. Brunner, La protection des données et les Accords Schengen/Dublin, in: C. Kaddous/M. Jametti Greiner (Hg.), Bilaterale Abkommen II Schweiz – EU und andere neue Abkommen, 2006, 426 (428 ff.).

sitzstands sind.[28] Sowohl die RL 95/46 als auch der Rahmenbeschluss 2008/977 (betreffend die Strafverfolgung) figurieren in den Anhängen. Da die erwähnten Assoziierungsabkommen in den «Übernahmemechanismen» eine dynamische Übernahme der Weiterentwicklungen des Schengen- und Dublin-Besitzstands vorsehen, könnte man auf den ersten Blick annehmen, die Schweiz werde im Zuge der Anwendung dieser Mechanismen[29] nach der Übernahme der neuen Rechtsakte in die Anhänge der genannten Abkommen im Ergebnis auch die Vorgaben der Datenschutzgrundverordnung und der neuen Richtlinie zum Datenschutz bei der Strafverfolgung zu beachten haben.

Dieser Schluss gilt jedoch nur für die Richtlinie zum Datenschutz in der Strafverfolgung (RL 2016/680),[30] nicht hingegen für die Datenschutzgrundverordnung: Interessanterweise fehlt in dieser jeglicher Hinweis darauf, dass sie Teil des Schengen-Besitzstandes ist bzw. sein soll, was insofern überrascht, als dies bei der RL 95/46 – die ja durch die Datenschutzgrundverordnung aufgehoben wird – der Fall ist. Dies und der Umstand, dass sich im Rahmen von «Schengen» und «Dublin» zahlreiche datenschutzrechtliche Fragen stellen, sprechen – im Gegensatz zur Ansicht des Unionsgesetzgebers – dafür, dass auch die Verordnung als Teil des Schengen-Besitzstandes hätte angesehen werden müssen. Die Frage, ob ein Rechtsakt Teil des Schengen-Besitzstandes ist oder nicht, ist im Übrigen durchaus eine Rechtsfrage, die Gegenstand der gerichtlichen Überprüfung durch den EuGH ist bzw. sein kann. Allerdings unterliegt es einigen Zweifeln, ob es zu einem entsprechenden Verfahren kommen wird: Eine Nichtigkeitsklage (Art. 263 AEUV) wäre hier zwar grundsätzlich denkbar gewesen; die Klagefrist ist aber abgelaufen. Darüber hinaus kann die Gültigkeit eines Rechtsakts auch im Rahmen des Art. 267 AEUV (Vorabentscheidungsverfahren) geprüft werden; hierfür müsste jedoch gerade diese Frage für die Entscheidung einer bei einem mitgliedstaatlichen Gericht anhängigen Streitsache relevant sein, was theoretisch möglich ist, sich aber wohl kaum in absehbarer Zeit realisieren dürfte (wenn dies auch nicht ausgeschlossen ist). Vor diesem Hintergrund bleibt es in Bezug auf die Schweiz dabei, dass für diese nach wie vor die RL 95/46 massgeblich ist, während in den EU-Mitgliedstaaten die Datenschutzgrundverordnung gilt. Dieses Ergebnis steht in einem gewissen Spannungsverhältnis zur Zielsetzung der Schengen- und Dublinassoziierung, im Verhältnis zur Schweiz in den betroffenen Bereichen eine möglichst parallele Rechtslage sicherzustellen.

Dieser Befund ändert jedoch nichts daran, dass die Datenschutzgrundverordnung und die diesbezügliche Rechtsprechung des EuGH für die Schweiz von Bedeutung sind, wobei in erster Linie auf vier Aspekte hinzuweisen ist:

- Erstens knüpft die Verordnung – trotz aller Neuerungen – in zahlreichen Bereichen an bereits in der RL 95/46 enthaltene Regelungen an. Soweit also z.B. Rechtsprechung des EuGH zu solchen übernommenen oder ggf. auch präzisierten Regelungen ergeht, kann diese durchaus auch für die Auslegung der RL 95/46 und damit für die Schweiz von Bedeutung sein. Im Einzelfall sind hier aber schwierige Abgrenzungsfragen zu gewärtigen.
- Zweitens sind in der Schweiz tätige Unternehmen aufgrund des weiten Anwendungsbereichs der Datenschutzgrundverordnung insofern betroffen, als sie sich bei Vorliegen der skizzierten Voraussetzungen der extraterritorialen Anwendung[31] an die Vorgaben der Verordnung zu halten haben.
- Drittens sind die Vorgaben der VO 2016/679 auch im Zusammenhang mit dem von der Kommission nach Art. 45 VO 2016/679 anzunehmenden «Gleichwertigkeitsbeschluss» – welcher mit Blick auf die Kommunikation von Personendaten aus der EU in einen Drittstaat die Gleichwertigkeit des Datenschutzniveaus in letzterem feststellt – von Bedeutung. Es ist zu erwarten, dass dieser Beschluss in Bälde gefasst werden wird, wobei hier die nach wie vor nicht geklärten «institutionellen Fragen» zwischen der Schweiz und der EU dazu führen könnten, dass dieser Entscheid der Kommission negativ ausfällt, dies trotz des Umstands, dass die Gleichwertigkeit des Datenschutzniveaus in der Schweiz auf der Grundlage des totalrevidierten Datenschutzgesetzes grundsätzlich zu bejahen ist. Allerdings gibt es keine Rechtspflicht, einen derartigen Beschluss zu fassen.[32]
- Schliesslich ist es auch darüber hinaus sinnvoll, im Bereich des Datenschutzrechts die unionsrechtlichen Entwicklungen zumindest zur Kenntnis zu nehmen und in die Betrachtungen einzubeziehen, zumal gewisse Aspekte auch im Rahmen der Revision der Datenschutzkonvention des Europarates – die nach ihren erklärten Zielsetzungen inhaltlich mit den Entwicklungen auf EU-Ebene

28 Streitig ist dabei die genaue Reichweite der Bindungswirkung der RL 95/46 für die Schweiz, in Bezug auf welche es sich fragt, ob sie lediglich für die von der Schengen-/Dublin-Assoziierung erfassten Bereiche verbindlich ist oder allgemein auch darüber hinaus zu beachten ist, ähnlich wie für einen EU-Mitgliedstaat, vgl. für die zuletzt genannte Ansicht Epiney (Fn. 27), SJZ 2006, 121 (122 ff.); C. Langhanke, Datenschutz in der Schweiz. Reichweite der europarechtlichen Vorgaben, ZD 2014, 621 ff.; a.A. S. Brunner, Zur Umsetzung von «Schengen» und «Dublin» im Bereich des Datenschutzes: Drei Thesen, in: A. Epiney/P. Hobi (Hg.), Die Revision des Datenschutzgesetzes, Zürich 2009, 139 (140 ff.); B. Rudin/B. Baeriswyl, «Schengen» und der Datenschutz in den Kantonen: Anforderungen – Beurteilung – Handlungsbedarf, in: A. Epiney/S. Theuerkauf (Hg.), Datenschutz in Europa und die Schweiz/La protection des données en Europe et la Suisse, Zürich 2006, 169 (175 f.).

29 Vgl. im Einzelnen zu diesen A. Epiney/B. Metz/B. Pirker, Zur Parallelität der Rechtsentwicklung in der EU und in der Schweiz, Zürich 2012, 140 ff.

30 RL 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, ABl. 2016 L 119, 89. Diese wurde auch inzwischen in der Schweiz umgesetzt. Vgl. hierzu B. Rudin, Datenschutzreform in der Schweiz, digma 2018, 194 ff.

31 Oben II. 2.

32 Vgl. im Einzelnen hierzu A. Epiney, Les implications de l'échec des négociations d'un Accord-cadre entre la Suisse et l'UE, Fribourg 2022, Rn. 42 ff.

abgestimmt werden sollte[33] und durch die Schweiz ratifiziert wurde – relevant sein dürften. Hier könnte es gar zu einer Art «Harmonisierung» der in der Union einerseits und in der Schweiz andererseits geltenden rechtlichen Vorgaben aufgrund des Abschlusses eines sowohl für die Union als auch für die Schweiz verbindlichen völkerrechtlichen Vertrages kommen, dies soweit davon auszugehen ist, dass das Unionsrecht im Ergebnis und zumindest in weiten Teilen insbesondere durch die Datenschutzgrundverordnung die Vorgaben der revidierten Datenschutzkonvention des Europarates umsetzen will. Denn diesfalls wären im Ergebnis auch die Datenschutzgrundverordnung (bzw. Teile derselben) sowie die zu ihr ergehende Rechtsprechung für die Schweiz relevant, stellt doch die Praxis der Vertragsparteien ein bei der Auslegung eines völkerrechtlichen Vertrages zu berücksichtigendes Element dar (vgl. Art. 31 Abs. 3 lit. b VRK).[34]

IV. Rechtsprechung des EuGH

Die Rechtsprechung des EuGH hatte sich mittlerweile in zahlreichen Urteilen mit Fragen des Datenschutzes zu befassen. Die Problemstellungen sind dabei mitunter parallel wie in der Schweiz gelagert, so dass die Urteile – abgesehen von den unter III. erwähnten Aspekten – auch ganz grundsätzlich eine gewisse Aufmerksamkeit verdienen. Es ist hier nicht der Ort, diese Rechtsprechung im Einzelnen darzustellen und zu bewerten; allerdings vermag die folgende Auflistung mit den zentralen Stichworten der Urteile die Vielfalt der von der Rechtsprechung erörterten Fragen zu illustrieren:

- EuGH vom 20. Mai 2003, C-465/00, C-138/01 und C-139/01, «Österreichischer Rundfunk»: Veröffentlichung des Einkommens von öffentlichen Angestellten;
- EuGH vom 16. Dezember 2008, C-542/06, «Huber»: Datenbearbeitung für aufenthaltsrechtliche und statistische Zwecke;
- EuGH vom 9. März 2010, C-518/07, «Kommission/Deutschland»; EuGH vom 16. Oktober 2012, C-614/10, «Kommission/Österreich»; EuGH vom 8. April 2014, C-288/12, «Kommission/Ungarn»: Unabhängigkeit der Aufsichtsbehörden;
- EuGH vom 8. April 2014, C-293/12, «Digital Rights Ireland»; EuGH vom 21. Dezember 2016, C-203/15 und C-658/15, «Tele2 Sverige»; EuGH vom 6. Oktober 2020, C-511/18 u.a., «La Quadrature du cercle»; EuGH vom 2. März 2021, C-746/18, «H K»; EuGH vom 6. Oktober 2020, C-623/17, «Privacy International»: Vorratsdatenspeicherung;
- EuGH vom 13. Mai 2014, C-131/12, «Google Spain»; EuGH vom 24. September 2019, C-136/17, «GC/CNIL»; EuGH vom 24. September 2019, C-507/17, «Google/CNIL»: «Recht auf Vergessen»;
- EuGH vom 11. Demeber 2014, C-212/13, «Rynes»; EuGH vom 11. Dezember 2019, C-708/18, «TK»: Videoüberwachung;
- EuGH vom 1. Oktober 2015, C-201/14, «Bara»; EuGH vom 2. Oktober 2018, C-207/16, «Ministerio Fiscal»: Bekanntgabe von Personendaten;
- EuGH vom 1. Oktober 2015, C-230/14, «Weltimmo»: Voraussetzungen einer Niederlassung;
- EuGH vom 6. Oktober 2015, C-362/14, «Schrems»; EuGH vom 16. Juli 2020, C-311/18, «Schrems II»: Datenübermittlung in die USA;
- EuGH vom 19. Oktober 2016, C-582/14, «Breyer»: IP-Adresse als Personendatum, Unzulässigkeit strengerer Datenschutzanforderungen;
- Gutachten 1/15 vom 26. Juli 2017: Verarbeitung von Fluggastdatensätzen;
- EuGH vom 20. Dezember 2017, C-434/16, «Nowak»: Personendatum bei Prüfungen;
- EuGH vom 5. Juni 2018, C-210/16, «Wirtschaftsakademie»; EuGH vom 10. Juli 2018, C-25/17, «Zeugen Jehovas»; EuGH vom 29. Juli 2019, C-40/17, «Fashion ID»: Begriff des Verantwortlichen;
- EuGH vom 14. Februar 2019, C-345/17, «Buivids»: journalistische Tätigkeit;
- EuGH vom 1. Oktober 2019, C-673/17, «Planet49»; EuGH vom 11. November 2020, C-61/19, «Orange Romania»: Rechte Einzelner;
- EuGH vom 15. Juni 2021, C-645/19, «Facebook Ireland»: Zuständigkeit der Aufsichtsbehörde.
- EuGH vom 22. Juni 2021, C-439/19, «Latvijas Republikas Saeima»: Datenbank über Verstösse gegen Verkehrsregeln.

V. Schluss

Auch im Bereich des Datenschutzes ist die Schweiz – trotz der fehlenden «formellen» Bindung an die Datenschutzgrundverordnung – in vielfältiger Weise von der Rechtsentwicklung in der Union (sowohl in Bezug auf die Gesetzgebung als auch die Rechtsprechung) betroffen. Schon aufgrund der bedeutenden Datenflüsse zwischen der Union und der Schweiz sowie der Perspektive bzw. der Notwendigkeit eines neuen «Gleichwertigkeitsbeschlusses» der Europäischen Kommission lohnt sich somit das Verfolgen der Rechtslage in der Union. Der Bundesgesetzgeber hat denn

33 Vgl. hierzu, m.w.N., C. de Terwangne, La modernisation de la Convention 108 du Conseil de l'Europe, in: A. Epiney/T. Fasnacht (Hg.), Die Entwicklung der europarechtlichen Vorgaben im Bereich des Datenschutzes und Implikationen für die Schweiz, Zürich 2012, 23 ff.; J.-Ph. Walter, La révision de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108) et les répercussions pour la Suisse, in: A. Epiney/D. Nüesch (Hg.), Die Revision des Datenschutzes in Europa und die Schweiz, Zürich 2016, 77 ff.

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

auch mit der Totalrevision des Datenschutzgesetzes[35] diesem Befund Rechnung getragen. Insofern und vor dem Hintergrund der «Harmonisierung durch Völkerrecht» ist damit zu rechnen, dass sich die Entwicklungen in der Schweiz und der EU auch in Zukunft weitgehend parallel gestalten werden, was freilich nichts daran ändert, dass es in (möglicherweise bedeutenden) Einzelbereichen – wie z.B. bei den Sanktionen – ins Gewicht fallende Unterschiede gibt bzw. geben kann.

Zusammenfassung

Das Datenschutzrecht der EU ist sehr ausdifferenziert, sowohl in Bezug auf die Rechtsetzung als auch die Rechtsprechung. Von besonderer Bedeutung sind im Primärrecht die Vorgaben der Grundrechtecharta, welche der Datenbearbeitung Grenzen setzen und durch den EU-Gesetzgeber und den nationalen Gesetzgeber (letzterer bei der Durchführung des EU-Rechts) zu beachten sind, sowie die Datenschutzgrundverordnung. Die Schweiz ist – trotz ihres Status als Nicht-EU-Mitglied – zwar nicht an diese rechtlichen Vorgaben gebunden; jedoch sind diese aufgrund verschiedener Mechanismen auch für die und in der Schweiz von grosser Bedeutung. Insofern ist es zentral, die Rechtsentwicklungen in der EU auch in diesem Gebiet aufmerksam zu verfolgen und ihre Relevanz für die Schweiz zu analysieren.

Résumé

Le droit de l'UE en matière de protection des données est très diversifié, tant au niveau de la législation que de la jurisprudence. Dans le droit primaire, les dispositions de la Charte des droits fondamentaux, qui fixent des limites au traitement des données et doivent être respectées aussi bien par le législateur de l'UE que par le législateur national (lorsque ce dernier met en œuvre le droit de l'UE), ainsi que le Règlement général sur la protection des données, revêtent une importance particulière. Bien que la Suisse ne soit pas tenue de respecter ces dispositions juridiques, celles-ci sont d'une grande portée aussi bien pour la Suisse qu'en Suisse en raison de divers mécanismes – et ce malgré son statut de pays non membre de l'UE. Il est donc essentiel de suivre attentivement les développements juridiques en cours au sein de l'UE dans ce domaine et d'analyser leur pertinence pour la Suisse.

35 Vgl. zu diesem, m.w.N., S. Métille, La (nouvelle) Loi fédérale sur la protection des données du 25 septembre 2020: des principes, des droits et des obligations, in: A. Epiney/S. Moser/S. Rovelli (Hg.), Die Revision des Datenschutzgesetzes des Bundes, Zürich 2022, 1 ff.