Cloud-basierte Dienstleistungen im Licht der DSGVO

David Roth*

«Cloud Computing» verfügt (weiterhin) über disruptives Potenzial. Skaleneffekte infolge der ubiquitären Verarbeitung von «(big) data» sowie die effizientere Nutzung von Informations- und Kommunikationsinfrastrukturen führen nicht zuletzt auch zu Kosteneinsparungen, welche allen zugutekommen können. Hierbei darf indes die Privatsphäre des Individuums bzw. sein Grundrecht auf Personendatenschutz nicht aus den Augen verloren gehen. Der vorliegende Beitrag beschäftigt sich – aus der drittländischen Perspektive der Schweiz – mit den Anforderungen, welche die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) an die rechtmässige Erbringung und Inanspruchnahme von Cloud-basierten Dienstleistungen stellt.

Le « cloud computing » continue à disposer d'un potentiel disruptif. Les effets d'échelle générés par le traitement ubiquitaire des « big data » et l'utilisation plus efficiente des infrastructures informatiques et de communication ont notamment pour effet des économies de coûts qui peuvent bénéficier à tous. Cependant, il ne faut pas perdre de vue la sphère privée de l'individu ainsi que son droit fondamental à la protection de ses données personnelles. La présente contribution décrit les exigences juridiques qu'impose le Règlement général de l'Union européenne sur la protection des données (RGPD) à la fourniture et à l'utilisation de services en nuage, du point de vue d'un pays tiers (la Suisse).

Inhaltsübersicht

I. Einleitung

Dieser Beitrag führt zuerst in die technischen Grundlagen des «Cloud Computing» ein. Nach einer Darstellung des DSGVO-Anwendungsbereichs wendet er sich den Fragen zu, wie Cloud-Dienstleister in datenschutzrechtlicher Hinsicht zu qualifizieren sowie welche Vorgaben bei der Übermittlung personenbezogener Daten zu berücksichtigen sind. Der Beitrag taxiert in der Folge die besonderen Risiken der Inanspruchnahme von Cloud-basierten Dienstleistungen und zeigt auf, wie Cloud-Dienstleistungsnehmer ihrer datenschutzrechtlichen Verantwortung nachkommen können.

II. Technische Grundlagen

A. Begriffsklärung

Nach etablierter Definition bezeichnet «Cloud Computing» ein Modell, welches einen flexiblen und bedarfsori-

* David Roth, Dr. iur., Rechtsanwalt, Gerichtsschreiber am Bundesverwaltungsgericht (Abteilung II), Lehrbeauftragter für Handels- und Wirtschaftsrecht an der Universität Zürich sowie für Wettbewerbsrecht an der Kalaidos Fachhochschule. Beim vorliegenden Beitrag handelt es sich um eine teilweise Wiedergabe der schriftlichen Arbeit des Verfassers im Rahmen des CAS Finanzmarktrecht 2019 am Europa Institut an der Universität Zürich.

entierten Zugriff auf einen gemeinsam genutzten Pool von konfigurierbaren IT-Ressourcen ermöglicht, die grundsätzlich jederzeit und überall über ein Netzwerk abgerufen werden können.[1] Cloud-basierte Dienstleistungen sind für die vorliegenden Zwecke demnach zunächst einmal Dienstleistungen, welche von Personen (Dienstleistern) im Zusammenhang mit Cloud Computing für Personen (Dienstleistungsnehmer) erbracht werden.[2] Dienstleister können dabei sowohl Angestellte, beigezogene oder entsandte Mitarbeiter des Dienstleistungsnehmers, aber beispielsweise auch Unternehmen derselben Unternehmensgruppe oder unabhängige Unternehmen sein. Als «Cloud Banking» wird etwa die Bereitstellung und Erbringung von Bank- und Finanzdienstleistungen auf Grundlage der Cloud-Technologie definiert.[3] Nahezu alle informationstechnologischen Ressourcen (Daten sowie Hard- und Software) können in eine Cloud ausgelagert werden.[4] Es werden regelmässig drei grundlegende Dienstleistungsmodelle (service models) sowie sechs Bereitstellungsmodelle (deployment models) unterschieden.[5]

B. Dienstleistungsmodelle und (geteilte) technische Verantwortung

1. Server als Grundlage

Sämtliche Cloud-basierten Dienstleistungen werden jeweils auf Servern, d.h. auf vom Dienstleister zur Verfügung gestellter Hardware, erbracht.[6] Die nachfolgenden Dienstleistungsmodelle lassen sich auf diesen Servern auch kombiniert anbieten: Die Infrastruktur unterstützt eine Plattform, während eine Plattform zur Ausführung von Software genutzt werden kann.[7] Für die Integrität und Verfügbarkeit der Server ist jeweils der Cloud-Dienstleister verantwortlich.[8]

2. Infrastructure as a Service (IaaS)

Bei IaaS erhält der Dienstleistungsnehmer Zugang zu Hardware-Ressourcen. Als Grundmodell für Cloud-basierte Dienstleistungen ermöglicht IaaS die Verwendung von Software, welche nicht über ein «Software as a Service»-Dienstleistungsmodell angeboten wird, ohne dass die hohen Unterhaltskosten einer rechnergestützten Infrastruktur getragen werden müssen.[9] Die gesamte Konfiguration und das Management der Anwendungen sind im Verantwortlichkeitsbereich des Dienstleistungsnehmers. Der Cloud-Dienstleister hat zu gewährleisten, dass die Daten nicht von Unberechtigten abgerufen werden können sowie jederzeit verfügbar sind; sämtliche übrigen Anforderungen an die Vertraulichkeit und Integrität der Konfiguration liegen beim Dienstleistungsnehmer.[10]

3. Platform as a Service (PaaS)

Der Cloud-Dienstleister stellt bei PaaS seine Hardware sowie Softwareentwicklungstools wie Programmiersprachen, Programmbibliotheken und weitere Werkzeuge zur

---

1 Peter Mell/Timothy Grance, The NIST Definition of Cloud Computing, NIST Special Publication 800-145, September 2011, 2; Sebastian Lins/Ali Sunyaev, Klassifikation von Cloud-Services, in: Helmut Krcmar/Claudia Eckert/Alexander Rossnagel/Ali Sunyaev/Manuel Wiesche (Hrsg.), Management sicherer Cloud-Services, Wiesbaden 2018, 7 ff., 8; BaFin, Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter, Stand November 2018, 4; weiterf. Begriffsabgrenzungen finden sich bei W. Kuan Hon/Christopher Millard, Banking in the cloud: Part 1 – banks' use of cloud services, 34 CLSR 4–24 (2018), 6 f.

2 Bezieht sich die Cloud-basierte Dienstleistung auf die Verarbeitung personenbezogener Daten (weiterf. III.A. hiernach) und wird sie von Unternehmen derselben Unternehmensgruppe oder unabhängigen Unternehmen erbracht, wird der Dienstleister entweder als (Mit-)Verantwortlicher oder als Auftragsverarbeiter qualifiziert, weiterf. IV. hiernach.

3 Schweizerische Bankiervereinigung, Cloud-Leitfaden, Wegweiser für sicheres Cloud Banking, Version 1.0, März 2019, 8.

4 Christian Schwarzenegger/Florent Thouvenin/Burkhard Stiller, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Zürich 2019, 3.

5 Sebastian Lins/Stephan Schneider/Ali Sunyaev, Cloud-Service-Zertifizierung, Ein Rahmenwerk und Kriterienkatalog zur Zertifizierung von Cloud-Services, 2. A., Berlin 2019, 5 ff. m.Hinw. auf in der Praxis und Literatur zu findende weitere Dienstleistungsmodelle, welche den grundlegenden jeweils zuordenbar sind; vgl. Mell/Grance (FN 1), 2 f.; Lins/Sunyaev (FN 1), 9 ff.; s. II.B. f. hiernach.

6 Schwarzenegger/Thouvenin/Stiller (FN 4), 6.

7 Lins/Sunyaev (FN 1), 9.

8 Von der technischen Verantwortung im Sinne dieses Kapitels ist die datenschutzrechtliche Verantwortung für die Verarbeitung personenbezogener Daten zu unterscheiden, weiterf. VI.A. hiernach.

9 Schwarzenegger/Thouvenin/Stiller (FN 4), 8 f.; vgl. auch Artikel-29-Datenschutzgruppe, Stellungnahme 05/2012 zum Cloud Computing, 01037/12/DE WP 196, angenommen am 1. Juli 2012, 31.

10 Lins/Schneider/Sunyaev (FN 5), 10; Schwarzenegger/Thouvenin/Stiller (FN 4), 10 f.; vgl. BaFin (FN 1), 4; weiterf. zu den jeweiligen Einflussmöglichkeiten bei den verschiedenen Cloud-basierten Dienstleistungsmodellen s. NIST Cloud Computing Security Working Group, NIST Cloud Computing Security Reference Architecture, NIST Special Publication 500-299, Entwurf 2013, 110 ff.

Verfügung. Der Dienstleistungsnehmer kann die entwickelten Anwendungen verwalten und Veränderungen an ihnen vornehmen. Er spart wiederum Hardware- sowie Werkzeugkosten. Hingegen sind die Anwendungen oftmals bloss auf der Plattform des Cloud-Dienstleisters verwendbar, weswegen ein «lock in»-Effekt eintritt.[11] Im Hinblick auf die Sicherheit ist eine geteilte technische Verantwortung zwischen Dienstleister und Dienstleistungsnehmer zu konstatieren: Ersterer hat einerseits die Plattform zu entwickeln und zu betreiben sowie deren Verfügbarkeit zu gewährleisten und ist andererseits dafür verantwortlich, dass die Daten und Konfigurationen des Dienstleistungsnehmers vertraulich bleiben; Letzterer ist jedoch für die Konfiguration der Plattform und deren Sicherheitsaspekte verantwortlich.[12]

4. Software as a Service (SaaS)

Als endverbraucherfreundliches Dienstmodell kann der Dienstleistungsnehmer auf die SaaS-Anwendungen über ein Netzwerk zugreifen. Software und Daten werden auf der Infrastruktur zentral gespeichert, was das Cloud-Management und den Support für die Anwendungen erleichtert, hingegen den Dienstleistungsnehmer in seiner Kontrolle und bei gewünschten Anpassungen erheblich einschränkt.[13] In der alleinigen technischen Verantwortung des Cloud-Dienstleisters liegen die Vertraulichkeit der Daten, die Integrität des Netzwerks und die Verfügbarkeit der Dienste; der Dienstleistungsnehmer ist lediglich für die Sicherheit der Zugangsdaten sowie die sichere und konforme Nutzung verantwortlich.[14]

C. Bereitstellungsmodelle

Beim Bereitstellungsmodell Private-Cloud wird deren Infrastruktur nur von einer einzelnen Organisation und deren Mitgliedern benutzt. Sie kann sowohl von der besagten Organisation als auch von Dritten betrieben werden. Von einer Virtual-Private-Cloud wird gesprochen, wenn der Zugriff über ein Virtual Private Network realisiert wird. Eine Community-Cloud bezeichnet dementgegen eine Infrastruktur, welche durch eine Gruppe von Organisationen mit ähnlichen Anforderungen genutzt wird. Wiederum kann sie von einer oder mehreren beteiligten Organisationen betrieben werden oder auch durch einen Dritten. Durch die allgemeine Öffentlichkeit kann sodann die Public-Cloud genutzt werden. Die Hybrid-Cloud bezeichnet eine Kombination der vorgenannten Bereitstellungsmodelle u.a. zum Zwecke der Übertragung von Daten und Anwendungen. Schliesslich werden bei einer Multi-Cloud verschiedene Infrastrukturen aggregiert und zusammengefasst.[15]

III. Anwendungsbereich der DSGVO

A. Sachlicher Anwendungsbereich

Gemäss Art. 2 Abs. 1 DSGVO erstreckt sich der sachliche Anwendungsbereich der Verordnung einerseits auf die automatisierte Verarbeitung personenbezogener Daten. Unerheblich ist, ob eine vollständige oder bloss teilweise Automatisierung erfolgt.[16] Andererseits gilt die Verordnung für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Dies betrifft etwa Notizen oder Informationen aus Beobachtungen.[17] Die DSGVO gilt bereits ab der Datenerhebung, selbst wenn die Daten erst später automatisiert verarbeitet werden sollen.[18]

«Verarbeitung» ist der sehr weit auszulegende Oberbegriff für Handlungen mit personenbezogenen Daten;[19] Art. 4 Nr. 2 DSGVO benennt in einem nicht abschliessenden Beispielkatalog folgende Vorgänge als Verarbeitungen:

> «[D]as Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch

---

[11] Weiterf. Nelson Gonzalez/Charles Miers/Fernando Redigolo/Marcos Simplicio/Tereza Carvalho/Mats Näslund/Makan Pourzandi, A quantitative analysis of current security concerns and solutions for cloud computing, JCC 2012, 1:11, 3 f.; Schwarzenegger/Thouvenin/Stiller (FN 4), 8; Lins/Sunyaev (FN 1), 9.

[12] Lins/Schneider/Sunyaev (FN 5), 9 f.; Schwarzenegger/Thouvenin/Stiller (FN 4), 11.

[13] Mell/Grance (FN 1), 2; Schwarzenegger/Thouvenin/Stiller (FN 4), 7 f.; Lins/Sunyaev (FN 1), 9.

[14] Lins/Schneider/Sunyaev (FN 5), 8 f.; Schwarzenegger/Thouvenin/Stiller (FN 4), 11.

[15] Weiterf. nur Lins/Schneider/Sunyaev (FN 5), 10 ff. m.Hinw.; s. auch BaFin (FN 1), 5.

[16] Vgl. Erwägungsgrund 15 DSGVO.

[17] Zum Begriff s. III.B. hiernach.

[18] Tim Wybitul/Lukas Ströbel/Marian Ruess, Übermittlung personenbezogener Daten in Drittländer, Überblick und Checkliste für die Prüfung nach der DS-GVO, ZD 2017, 503 ff., 503.

[19] Philipp Reimer, in: Gernot Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. A., Baden-Baden/Wien/Zürich 2018, Art. 4 DSGVO N 43; Martin Esser, in: Martin Esser/Philipp Kramer/Kai von Lewinsky (Hrsg.), Auernhammer, DSGVO, BDSG Kommentar, 6. A., Köln 2018, Art. 4 DSGVO N 32 m.Hinw., dass grundsätzlich jeglicher Umgang mit personenbezogenen Daten eine Verarbeitung im Sinne der DSGVO darstelle.

> Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.»

Auch die Pseudonymisierung ist eine Verarbeitung, nämlich «in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können».[20] Die (Total-)Verschlüsselung ist die extremste Form der Pseudonymisierung.[21]

Personenbezogene Daten sind jegliche Informationen betreffend natürliche Personen.[22] Es genügt die Bestimmbarkeit der Person, d.h. eine methodische Möglichkeit der Identifizierung.[23] Hierbei sind sowohl die zum Zeitpunkt der Verarbeitung verfügbare Technologie als auch die technologische Entwicklung zu berücksichtigen sowie jegliche Mittel, soweit sie «nach allgemeinem Ermessen wahrscheinlich genutzt werden». Dementgegen sind anonyme Daten Informationen, welche keine Identifikation einer betroffenen Person (mehr) zulassen, entweder weil sie sich nicht auf eine Person beziehen oder die Identifizierbarkeit irreversibel beseitigt wurde.[24]

Besonders schützenswerte personenbezogene Daten sind jene, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung, Gesundheitsdaten oder Daten zum Sexualleben oder zur sexuellen Orientierung (auch als «sensible» oder «sensitive» Daten bezeichnet).[25]

Sowohl das Überführen personenbezogener Daten in eine Cloud als auch deren ebendortige Weiterverwendung eröffnen demnach den sachlichen Anwendungsbereich der DSGVO. Derweil bedarf der weiteren Klärung, inwieweit dies auch für die Verwendung pseudonymisierter Daten gilt.[26]

B. Räumlicher Anwendungsbereich

Der räumliche Anwendungsbereich orientiert sich am Niederlassungs- sowie am Marktortprinzip:[27] Die Verordnung gilt einerseits für jeden Verantwortlichen sowie Auftragsverarbeiter, der im Rahmen der Tätigkeit einer Niederlassung in der Union personenbezogene Daten verarbeitet (Art. 3 Abs. 1 DSGVO). Die Verordnung erlangt gemäss Art. 3 Abs. 2 DSGVO andererseits eine erhebliche Erweiterung ihres Anwendungsbereichs, indem sie zugleich für die Verarbeitung personenbezogener Daten gilt, wenn der Verantwortliche oder Auftragsverarbeiter über keine Niederlassung in der Union verfügt, seine Waren oder Dienstleistungen aber in der EU anbietet (lit. a) oder (alternativ) das Verhalten von betroffenen Personen in der Union beobachtet (lit. b). Art. 3 Abs. 3 DSGVO betrifft Fälle, in denen das Recht eines Mitgliedstaats aus völkerrechtlichen Gründen an einem Ort Anwendung findet, der ausserhalb der EU liegt.

Namentlich das Marktortprinzip ist auslegungsbedürftig, infolgedessen kann die Verordnung auch für Unternehmen gelten, welche über keine Niederlassung in der EU verfügen. Seiner Einführung lag die Überlegung zugrunde, die «Global Players» des Internets, welche oftmals ausserhalb Europas domiziliert sind, in den Anwendungsbereich des europäischen Datenschutzrechts einzubeziehen. Die Teilnahme am europäischen Binnenmarkt soll für Verantwortliche und Auftragsverarbeiter – ob in oder ausserhalb der EU domiziliert – mit datenschutzrechtlich «gleich langen Spiessen» erfolgen, d.h., eine Niederlassung in der EU soll keinen Wettbewerbsnachteil bedeuten.

Notabene reicht bereits ein bloss vorübergehender Aufenthalt des Betroffenen im EU-Raum (z.B. als Tou-

---

20 S. Art. 4 Nr. 5 DSGVO mit den weiteren Anforderungen, dass die fragliche Information gesondert aufbewahrt wird sowie «technische und organisatorische Massnahmen» zur Gewährleistung der Nichtzuordnung bestehen.

21 S. David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, Jusletter vom 11.6.2019, 39; eine abweichende Terminologie verwendet offenbar u.a. die Schweizerische Bankiervereinigung (FN 3), 13 f.

22 Während die DSGVO nicht für die personenbezogenen Daten verstorbener Personen gilt (Erwägungsgrund 27 DSGVO), sollten deren Betroffenenrechte (für Bearbeitungen zu Lebzeiten) nach richtiger Auffassung von ihren Erben geltend gemacht werden können; weiterf. Wolfgang Ziebarth, in: Gernot Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. A., Baden-Baden/Wien/Zürich 2018, Art. 4 DSGVO N 11; Mark-Oliver Mackenrodt, Der «digitale Nachlass» und die Verweigerung des Zugangs zu einem Internetaccount gegenüber Erben, ZUM-RD 2017, 540 ff.

23 S. Art. 4 Nr. 1 DSGVO m.Hinw.; hierzu zuletzt Jens Brauneck, DSGVO: Neue Anwendbarkeit durch neue Definition personenbezogener Daten?, EuZW 2019, 680 ff.; kritisch Tina Krügel, Das personenbezogene Datum nach der DS-GVO, Mehr Klarheit und Rechtssicherheit?, ZD 2017, 455 ff., 456, welche mit Blick auf *Big-Data*-Anwendungen eine potenziell uferlose Anwendung des Datenschutzrechts konstatiert.

24 S. Erwägungsgrund 26 DSGVO.

25 Art. 9 Abs. 1 DSGVO; David Kampert, in: Gernot Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. A., Baden-Baden/Wien/Zürich 2018, Art. 9 DSGVO N 1.

26 S. IV.B.2. hiernach.

27 S. nur Daniel Ennöckl, in: Gernot Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. A., Baden-Baden/Wien/Zürich 2018, Art. 3 DSGVO N 1 ff.

rist), um den Anwendungsbereich der Verordnung zu eröffnen.[28] Bei der Beurteilung, ob ein «Anbieten von Waren und Dienstleistungen» vorliegt, sind jedenfalls die tatsächlichen Inhalte des Angebots zu berücksichtigen, und es ist nicht bloss auf die Deklaration des Anbieters abzustellen.[29] Als Hinweise auf ein Angebot im Sinne von Art. 3 Abs. 2 lit. a DSGVO gilt etwa die Verwendung einer Sprache, die in der EU zwar gebräuchlich, im Land des Anbieters aber eine Fremdsprache ist, der Hinweis auf bestimmte Währungen (namentlich auf den Euro) oder wenn Kunden oder Nutzer in der EU erwähnt werden.[30] Eine «Beobachtung» im Sinne von Art. 3 Abs. 2 lit. b DSGVO stellt hingegen die Erhebung personenbezogener Daten zwecks Profilbildung (z.B. mittels *webtracking* etc.) insbesondere zu Werbezwecken dar, ohne dass (bereits) ein Angebot erfolgt.[31]

Es wird die Auffassung vertreten, ein schweizerisches (und damit ein drittländisch domiziliertes) Unternehmen falle nicht unter die DSGVO, wenn es als verantwortliche Stelle personenbezogene Daten durch einen Auftragsverarbeiter in der EU verarbeiten lasse oder umgekehrt als Auftragsverarbeiter personenbezogene Daten für einen Verantwortlichen in der EU verarbeite.[32] Diese Auslegungsfrage ist vorliegend insofern von Relevanz, als sie gerade auch die unionsgrenzüberschreitende Erbringung von Cloud-basierten Dienstleistungen betrifft.[33]

Meines Erachtens bedarf es einer differenzierten Betrachtung. Wohl sind die Anwendungsfälle des Marktortprinzips, wie sie in Art. 3 Abs. 2 DSGVO geregelt sind, abschliessend zu verstehen. Hingegen ist mit Blick auf die erste Konstellation jeweils zu fragen, wo sich die betroffene Person befindet und ob ein Angebot im Sinne von Art. 3 Abs. 2 lit. a DSGVO vorliegt. Dieselbe Bestimmung erfasst weiter den schweizerischen Auftragsverarbeiter für einen Verantwortlichen in der EU, sofern dieser einer betroffenen Person in der EU Waren oder Dienstleistungen anbietet. Auch der Auftragsverarbeiter als Auftragnehmer[34] des anbietenden Verantwortlichen untersteht nach Wortlaut und hiervor dargelegtem Zweck der Verordnung.[35] Seine Leistung wendet sich freilich nicht unmittelbar an die betroffene Person. Es genügt derweil nach dem Normwortlaut eine Datenverarbeitung «im Zusammenhang» mit dem Angebot,[36] was gegeben und weshalb eine Unterstellung zu bejahen ist.[37]

Schliesslich ist die Möglichkeit, die DSGVO anzurufen, freilich gerichtsstandsabhängig. Als Verordnung ist die DSGVO im EU-Raum in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat.[38] Darüber hinaus gilt sie für die EWR-Staaten Island, Liechtenstein und Norwegen qua Übernahme ins EWR-Abkommen.[39]

---

28 Philip Uecker, Extraterritorialer Anwendungsbereich der DS-GVO, Erläuterungen zu den neuen Regelungen und Ausblick auf internationale Entwicklungen, ZD 2019, 67 ff., 67 f.; Gerrit Hornung, in: Spiros Simitis/Gerrit Hornung/Indra Spiecker (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2019, Art. 3 DSGVO N 41 ff., je m.Hinw.

29 Philip Laue/Judith Nink/Sascha Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, Baden-Baden 2016, 56 f. m.Hinw., dass der Anwendungsbereich der Verordnung etwa eröffnet sei, wenn ein Unternehmen auf seiner Website erkläre, keine Waren oder Dienstleistungen in der EU anzubieten, hingegen eine Bestellung dorthin trotzdem möglich sei; die Autoren legen weiter in überzeugender Weise dar, dass bei der Auslegung – trotz autonomer Begrifflichkeit – auf die Judikatur zu Art. 6 Rom I-VO zurückgegriffen werden kann.

30 S. Erwägungsgrund 23 DSGVO; Emilie M. Praz, Responsabilités et outils de conformité selon la RGPD, AJP 2018, 609 ff., 610; weitere mögliche Konstellationen finden sich bei Lukas Bühlmann/Michael Reinle, Extraterritoriale Wirkung der DSGVO, digma 2017, 8 ff., 9, sowie Wolfgang Däubler, Das Kollisionsrecht des neuen Datenschutzes, RIW 2018, 405 ff., 408.

31 S. Erwägungsgrund 24 DSGVO.

32 David Vasella, Zum Anwendungsbereich der DSGVO, digma 2017, 220 ff., 221 f. m.Verw.; entsprechend Praz (FN 30), AJP 2018, 610; David Rosenthal/David Vasella, Erste Erfahrungen mit der DSGVO, Die Welt ist mit der Datenschutz-Grundverordnung der EU nicht untergegangen, aber komplizierter geworden, digma 2018, 166 ff., 169, wonach «heute überwiegend davon ausgegangen [werde], dass die DSGVO nicht anwendbar [sei], bspw. beim Outsourcing an (nicht konzernmässig kontrollierte) Dienstleister im EWR», ohne weitere Hinw.; abwägend Schwarzenegger/Thouvenin/Stiller (FN 4), 61 f.

33 Zur Qualifikation der Tätigkeit von Cloud-Dienstleistern weiterf. IV.B. hiernach.

34 S. Art. 4 Nr. 8 DSGVO; weiterf. IV.A. hiernach.

35 Im Ergebnis die Anwendbarkeit der Verordnung bejahend, allerdings mit anderer Begründung (Anwendbarkeit von Art. 3 Abs. 1 DSGVO, zumal der drittländische Auftragsverarbeiter «im Rahmen der Tätigkeiten» der Niederlassung des Verantwortlichen tätig werde): Stefan Ernst, in: Boris P. Paal/Daniel A. Pauly (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. A., München 2018, Art. 3 DSGVO N 12; ablehnend Vasella (FN 32), 221, Fn 5.

36 S. auch Europäischer Datenausschuss, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), adopted on 16 November 2018, 15.

37 Ähnlich Hornung (FN 28), Art. 3 DSGVO N 54; abweichend Manuel Klar, in: Jürgen Kühling/Benedikt Buchner (Hrsg.), Datenschutz-Grundverordnung, München 2017, Art. 3 DSGVO N 89; der Auftragsverarbeiter agiert als «verlängerter Arm» des Verantwortlichen, s. Bayerischer Landesbeauftragter für den Datenschutz, Auftragsverarbeitung, Orientierungshilfe, Version 2.0, 1. April 2019, 12, weiterf. IV. hiernach; weiterf. zur einheitlichen Behandlung von Verantwortlichem und Auftragsverarbeiter im Rahmen der Übermittlung von personenbezogenen Daten s. V.A. hiernach; s. auch Erwägungsgrund 22 DSGVO.

38 Art. 288 Abs. 2 AEUV.

39 Gemeinsamer EWR-Ausschuss, Decision No 154/2018 of July 2018 amending Annex XI (Electronic communication, audiovisual services and information society) and Protocol 37.

Vor Drittstaatsgerichten sei hier lediglich die Situation in der Schweiz skizziert: Im Bereich des öffentlichen Rechts richtet sich die Anwendbarkeit des schweizerischen Datenschutzrechts grundsätzlich nach dem Territorialitätsprinzip.[40] Vor einem schweizerischen Zivilgericht richtet sich die Anwendbarkeit der DSGVO bzw. die Geltendmachung von sich daraus ergebenden Ansprüchen nach den kollisionsrechtlichen Bestimmungen des schweizerischen internationalen Privatrechts.[41] Ein in der Schweiz domiziliertes Unternehmen kann nach Wahl des Geschädigten demgemäss gestützt auf die DSGVO belangt werden, wenn der Geschädigte in der EU seinen gewöhnlichen Aufenthalt hat oder der Erfolg der verletzenden Handlung dort eintritt, jeweils sofern das Unternehmen damit rechnen musste.[42]

C. Rechtsfolgen der Anwendbarkeit

Die Anwendbarkeit der DSGVO führt zur Verbindlichkeit sämtlicher ihrer Vorschriften, einschliesslich der Voraussetzungen für eine rechtmässige Übermittlung von personenbezogenen Daten in Drittländer.[43] In den Fällen gemäss Art. 3 Abs. 2 DSGVO hat der Verantwortliche oder der Auftragsverarbeiter weiter schriftlich einen Vertreter in der EU zu bestimmen.[44] Der Vertreter soll als Ansprechpartner für Aufsichtsbehörden zur Verfügung stehen sowie auf die Einhaltung der Verordnung durch den Vertretenen hinwirken.[45] Gemäss Art. 30 DSGVO hat der Vertreter das Verzeichnis der Verarbeitungstätigkeiten für den Verantwortlichen oder den Auftragsverarbeiter zu führen, sofern das vertretene Unternehmen nicht unter den Ausnahmetatbestand von Abs. 5 fällt.[46]

IV. Cloud-Dienstleister: Verantwortlicher oder Auftragsverarbeiter?

A. Funktionale Abgrenzung

Verantwortlicher ist gemäss Art. 4 Nr. 7 DSGVO eine Person oder Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Dementgegen ist Auftragsverarbeiter gemäss Art. 4 Nr. 8 DSGVO eine Person oder Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet. Verantwortlicher und Auftragsverarbeiter sind verpflichtet, sich schriftlich (durch Vertrag oder anderes unionsrechtliches oder mitgliedstaatliches Rechtsinstrument) zu binden, was auch in einem elektronischen Format geschehen kann.[47]

Als Empfänger der Datenübermittlung gemäss Art. 4 Nr. 9 DSGVO ist der Auftragsverarbeiter von den Dritten gemäss Art. 4 Nr. 10 DSGVO abzugrenzen.[48]

Der Auftragsverarbeiter sowie jede ihm unterstellte Stelle dürfen die personenbezogenen Daten ausschliesslich auf Weisung des Verantwortlichen bearbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.[49] Sie sind demnach grundsätzlich umfassend weisungsgebunden[50] und besitzen keine Entscheidungsbefugnis hinsichtlich des Zwecks oder der Mittel der Verarbeitung. Ein Auftragsverarbeiter entscheidet insbesondere nicht selbst, welche und wie datenschutzrechtlich relevante Parameter verarbeitet werden. Die Verwendung zu eigenen Zwecken ist begriffsdefinitorisch ebenso wenig zulässig, andernfalls die Person oder Stelle entweder als gemeinsam Verantwortlicher gemäss Art. 26 DSGVO[51] oder aber bei Überschreitung der Weisung des Verantwortlichen in Bezug auf diese Verarbeitung selbst als Verantwortlicher zu qualifizieren ist.[52]

---

40 Vgl. BVGer, A-7040/2009, 30.3.2011, E. 5.4, Google Street View, m.Hinw.

41 Ebenso Jacqueline Sievers/David Vasella, Bedeutung der DSGVO für die Treuhandbranche, TREX 2018, 330 ff., 331.

42 Art. 139 Abs. 1 lit. a und c i.V.m. Abs. 3 IPRG; ebenso Schwarzenegger/Thouvenin/Stiller (FN 4), 63 f. m.Hinw.

43 Zu Letzteren s. V.B. hiernach; Däubler (FN 30), 409.

44 S. Art. 27 Abs. 1 DSGVO; beachte die *De-minimis*-Ausnahmeregelung in Art. 27 Abs. 2 DSGVO (Gelegentliche, voraussichtlich risikofreie Verarbeitung von nicht «sensiblen» Daten) sowie die Befreiung der Behörden von Drittstaaten für die Datenverarbeitung zu öffentlichen Zwecken.

45 S. Erwägungsgrund 80 DSGVO; die unzulässige Nichtbenennung eines Vertreters kann als *ultima ratio* nach Art. 83 Abs. 4 lit. a DSGVO sanktioniert werden; vorgängig sollte eine Warnung bzw. Verwarnung gemäss Art. 58 Abs. 2 lit. a f. DSGVO erfolgen, s. Däubler (FN 30), 411.

46 Weiterf. Heiko Gossen/Marc Schramm, Das Verarbeitungsverzeichnis der DS-GVO, Ein effektives Instrument zur Umsetzung der neuen unionsrechtlichen Vorgaben, ZD 2017, 7 ff., 8 f.

47 S. Art. 28 Abs. 3 und Abs. 9 DSGVO.

48 Bartholomäus Regenhardt, in: Gernot Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. A., Baden-Baden/Wien/Zürich 2018, Art. 4 DSGVO N 155; zur mit dieser Unterscheidung einhergehenden Privilegierungswirkung s. V.A. hiernach.

49 Art. 29 DSGVO.

50 S. auch Art. 28 Abs. 3 lit. a DSGVO.

51 S. hierzu EuGH, 5.6.2018, Rs. C-210/16, *Facebook-Fanpage.*

52 Art. 28 Abs. 10 DSGVO; EuGH, 10.7.2018, Rs. C-25/17, N 68, *Zeugen Jehovas;* ausführlich Rosenthal (FN 21), 7 ff. m.Hinw.; Bayerischer Landesbeauftragter für den Datenschutz (FN 37), 11 f.; vgl. Artikel-29-Datenschutzgruppe, Stellungnahme 01/2010 zu den Begriffen «für die Verarbeitung Verantwortlicher» und «Auftragsverarbeiter», 00264/10/DE WP 169, angenommen am 16. Februar 2010, 30 ff.

Man kann die Einordnung eines Verarbeiters entweder als nach der DSGVO (Mit-)Verantwortlicher oder als Auftragsverarbeiter mit guten Gründen als «datenschutzrechtliche Gretchenfrage»[53] bezeichnen, zumal mit ihr die folgenreiche Zuordnung von empfindlich sanktionsbewehrten Pflichten einhergeht: Der Verantwortliche ist primär für die verordnungsgemässe Verarbeitung der personenbezogenen Daten verantwortlich und haftet im Aussenverhältnis umfassend.[54] Den Auftragsverarbeiter treffen derweil – lediglich, aber nun immerhin auch – Verzeichnisführungspflichten (Art. 30 DSGVO),[55] die Pflicht zur Zusammenarbeit mit der Datenschutzaufsicht sowie die Pflicht zur Bestellung eines Datenschutzbeauftragten (Art. 31 und Art. 37 Abs. 1 DSGVO), die Pflicht zu technischen und organisatorischen Massnahmen der Datensicherheit (Art. 32 DSGVO), die Pflicht zur Meldung von Datenpannen an den Verantwortlichen (Art. 33 Abs. 2 DSGVO) sowie gegebenenfalls die Pflicht zur Bestellung eines Vertreters[56] und Beschränkungen beim Datentransfer in Drittländer.[57]

B. Qualifikation von Cloud-Dienstleistern

1. Problemstellung

Angesichts der vorerwähnten, mit der Qualifikation einhergehenden Konsequenzen greift es kurz, wenn «Cloud Computing in den meisten Fällen als Auftragsverarbeitung im Sinne von Art. 28 DSGVO» eingestuft wird.[58] Fraglich ist zum einen, ob der Cloud-Dienstleister überhaupt personenbezogene Daten verarbeitet, andernfalls seine Tätigkeit nicht unter den sachlichen Anwendungsbereich der DSGVO fallen würde.[59] Bejaht man eine Verarbeitung personenbezogener Daten, ist festzustellen, ob der Cloud-Dienstleister als Auftragsverarbeiter oder Verantwortlicher tätig wird.

Die Unterscheidung kann hingegen vollends unterbleiben, wenn die Cloud-basierte Dienstleistung unter Aufsicht und auf Weisung des Dienstleistungsnehmers als Verantwortlicher im Sinne von Art. 29 DSGVO von natürlichen Personen wie Angestellten, beigezogenen oder entsandten Mitarbeitern erbracht wird. Sie sind dem Verantwortlichen zuzurechnen.[60] Ist der Cloud-Dienstleister aber eine andere Person – und dies gilt selbst bei Unternehmen, die derselben Unternehmensgruppe im Sinne von Art. 4 Nr. 19 DSGVO angehören[61] –, werden die nachfolgenden Abklärungen notwendig. In ersterem Fall (zurechenbare Personen) wie in letzterem, jedenfalls wenn das Unternehmen derselben Unternehmensgruppe angehört, wird es sich beim Bereitstellungsmodell im Übrigen regelmässig um entweder eine Private- oder eine Community-Cloud handeln.[62]

2. Personenbezogenheit pseudonymisierter Daten

Die Pseudonymisierung personenbezogener Daten kann zu deren relativer Unzuordenbarkeit führen und beschränkt damit die Identifizierbarkeit der betroffenen

---

53 S. Rosenthal (FN 21), 1; s. auch Rosenthal/Vasella (FN 32), 168.

54 Weiterf. VI.A.; Erwägungsgrund 74 DSGVO; Thomas Petri, in: Sprios Simitis/Gerrit Hornung/Indra Spiecker (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2019, Art. 24 DSGVO N 9; Nicolas Raschauer, in: Gernot Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. A., Baden-Baden/Wien/Zürich 2018, Art. 24 DSGVO N 9.

55 Vgl. III.C. hiervor.

56 Vgl. III.C. hiervor.

57 Weiterf. V.B. hiernach; vgl. Philipp-Christian Thomale, in: Martin Esser/Philipp Kramer/Kai von Lewinsky (Hrsg.), Auernhammer, DSGVO, BDSG Kommentar, 6. A., Köln 2018, Art. 28 DSGVO N 31 f.; s. auch Gossen/Schramm (FN 46), 11; Jens Eckhardt, DS-GVO: Anforderungen an die Auftragsdatenverarbeitung als Instrument zur Einbindung Externer, CCZ 2017, 111 ff., 115 f.; W. Kuan Hon, Open Season on Service Providers? The General Data Protection Regulation Cometh…, C&L 2015, August/September; Praz (FN 30), AJP 2018, 613 f.

58 Johanna M. Hofmann/Alexander Rossnagel, Rechtsverträgliche Gestaltung von Cloud-Services, in: Helmut Krcmar/Claudia Eckert/Alexander Rossnagel/Ali Sunyaev/Manuel Wiesche (Hrsg.), Management sicherer Cloud-Services, Wiesbaden 2018, 26 ff., 37; implizit von einer Auftragsverarbeitung ausgehend wohl auch Schwarzenegger/Thouvenin/Stiller (FN 4), 83 ff.; ebenso Christian Schwarzenegger/Florent Thouvenin/Burkhard Stiller/Damian George, Nutzung von Cloud-Diensten durch Anwältinnen und Anwälte, Anwaltsrevue 2019, 25 ff., 32; vgl. Gregor Schmid/Thomas Kahl, Verarbeitung «sensibler» Daten durch Cloud-Anbieter in Drittstaaten, Auftragsdatenverarbeitung nach geltendem Recht und DS-GVO, ZD 2017, 54 ff., 54; Privatim, Cloud-spezifische Risiken und Massnahmen, Merkblatt, 6. Februar 2019, 1; im Grundsatz zu Recht vorsichtig Albert Ingold, in: Gernot Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. A., Baden-Baden/Wien/Zürich 2018, Art. 28 DSGVO N 23, wonach sich eine pauschale Einordnung verbiete; ebenso Petri (FN 54), Art. 28 DSGVO N 19.

59 Zur fraglichen Personenbezogenheit pseudonymisierter Daten weiterf. IV.B.2. hiernach.

60 Weiterf. Rosenthal (FN 21), 43 f.

61 Peter Schantz, in: Spiros Simitis/Gerrit Hornung/Indra Spiecker (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2019, Art. 6 Abs. 1 DSGVO N 116; zumindest ist aber die Datenübermittlung an ein Unternehmen derselben Unternehmensgruppe zum Zwecke der Auftragsverarbeitung privilegiert und bedarf demnach grundsätzlich keiner weiteren Rechtfertigung, weiterf. V.A. hiernach.

62 Weiterf. II.C. hiervor.

Personen.[63] Ob die Weiterverwendung pseudonymisierter Daten durch einen Cloud-Dienstleister in den sachlichen Anwendungsbereich der DSGVO fällt, ist nach vorzugswürdiger Auffassung anhand der tatsächlichen Merkmale des Einzelfalls zu beurteilen.[64] Hierbei sollte – neben dem konkreten Verschlüsselungsgrad – nicht lediglich auf die «Mittel» bzw. durchsetzbaren Möglichkeiten des Cloud-Dienstleisters abgestellt werden,[65] sondern gleichsam seine jeweiligen (Offenlegungs-)Pflichten, namentlich gegenüber Behörden, in die Beurteilung einfliessen.[66]

Eine Totalverschlüsselung der personenbezogenen Daten vor deren Überführung in eine Cloud ist (bloss) dienstleistungsmodellabhängig möglich: Während IaaS- und regelmässig wohl auch PaaS-Modelle dem Dienstleistungsnehmer hinreichende Freiräume bei der Ausgestaltung der Anwendungen bieten, kann der Dienstleister beim SaaS-Modell die Softwareapplikationen grundsätzlich nur auf im Klartext gespeicherten, gegebenenfalls mässig pseudonymisierten Daten ausführen, was einer Totalverschlüsselung durch den Dienstleistungsnehmer entgegensteht. In solchen Fällen ist grundsätzlich von Identifizierbarkeit auszugehen.[67]

Die Personenbezogenheit sollte denn auch nicht leichthin verneint werden. Es ist unter Geltung der DSGVO tatsächlich ungeklärt, ob eine starke Pseudonymisierung, ja selbst eine Totalverschlüsselung nach dem letzten Stand der Technik,[68] die Personenbezogenheit überhaupt entfallen lässt.[69] Die sehr weiten Begriffsbestimmungen von Art. 4 Nr. 1 und Nr. 5 DSGVO sowie der zugehörige Erwägungsgrund 26 der Verordnung machen deutlich, dass der Verordnungsgeber «Verantwortlichkeitsketten» bei Datentransfer-Konstellationen generell aufrechterhalten möchte. Dies widerspiegelt sich zudem in den eigenständigen, auch die Auftragsverarbeiter treffenden Pflichten.[70] Cloud-Dienstleister und -Dienstleistungsnehmer tun im Ergebnis also gut daran, auch bei pseudonymisierten Daten den Vorgaben der DSGVO nach Möglichkeit zu entsprechen.

3. Abstellen auf die vertragliche Ausgestaltung

Soweit Cloud-basierte Dienstleistungen bloss von einer natürlichen Person für die eigenen personenbezogenen Daten in Anspruch genommen werden, ist der Dienstleister zwangsläufig Verantwortlicher: Der Dienstleistungsnehmer kann als betroffene Person nämlich definitionsgemäss nicht zugleich Verantwortlicher sein, und ohne beauftragenden Verantwortlichen kann es keinen Auftragsverarbeiter geben.[71]

Abgesehen vom vorerwähnten Spezialfall ist jeweils auf die konkrete vertragliche Ausgestaltung der zu erbringenden Cloud-basierten Dienstleistung abzustellen. Wohl enthält die Verordnung keine Beschränkungen der Auftragsverarbeitung mit Bezug auf gewisse Rechtsgebiete.[72] Die notwendige Weisungsgebundenheit des Auftragsverarbeiters[73] ist hingegen nur gewahrt, wenn es die Dienstleistungsnehmer bleiben, welche entscheiden können, welche Angebote sie in Anspruch nehmen wollen sowie welche Verarbeitungen durch den Dienstleister zulässig sind. Dem steht nicht entgegen, dass der Cloud-Dienstleister standardisierte Dienstleistungen anbietet.[74] Der Dienstleister darf auch einen Unterbeauftragten beiziehen – ohne zum Verantwortlichen zu mutieren –, solange er den Dienstleistungsnehmer hierüber informiert und Letzterer nicht kündigt («Notbremse»).[75] Voraussetzung hierfür ist derweil auf alle Fälle eine hinreichend bestimmte Klausel im ursprünglichen Vertragswerk, welche

---

63 S. III.A. hiervor m.Hinw.

64 Vgl. Schwarzenegger/Thouvenin/Stiller (FN 4), 66 f.

65 So EuGH, 19.10.2016, Rs. 582/14, N 49, *Breyer.*

66 Entsprechend Rosenthal (FN 21), 40; weiterf. zum US-amerikanischen CLOUD Act s. V.B.4. hiernach.

67 Entsprechend Jürgen Hartung, in: Jürgen Kühling/Benedikt Buchner (Hrsg.), Datenschutz-Grundverordnung, München 2017, Art. 28 DSGVO N 52; ähnlich Schwarzenegger/Thouvenin/Stiller (FN 4), 14 und 66 f.; weiterf. II.B. hiervor.

68 Wolfgang Straub, Cloud-Verträge – Regelungsbedarf und Vorgehensweise, AJP 2014, 905 ff., 913 m.Hinw., dass heute als unüberwindbar geltende kryptologische Verfahren in Zukunft ihre Wirksamkeit verlieren können; zur Terminologie s. III.A. hiervor.

69 In diesem Sinne Björn Steinrötter, Feuertaufe für die EU-Datenschutz-Grundverordnung – und das Kartellrecht steht Pate, EWS 2018, 61 ff., 64; zum Ganzen auch David Rosenthal, Personendaten ohne Identifizierbarkeit?, digma 2017, 198 ff.

70 S. IV.A. hiervor.

71 Vgl. Art. 4 Nr. 8 DSGVO; Rosenthal (FN 21), 11 f.

72 Bayerischer Landesbeauftragter für den Datenschutz (FN 37), 13.

73 S. IV.A. hiervor.

74 Ebenso Thomale (FN 57), Art. 28 DSGVO N 17; Rosenthal (FN 21), 18; entsprechend Hartung (FN 67), Art. 28 DSGVO N 44; ablehnend Ingold (FN 58), Art. 28 DSGVO N 23; überholt wohl die Auffassung von W. Kuan Hon, Killing Cloud Quickly, with GDPR…?, C&L 2016, February/March, wonach der Dienstleister von IaaS-Modellen nach der DSGVO durchwegs als Verantwortlicher gelte.

75 Rosenthal (FN 21), 18 f.; insgesamt kritisch Ingold (FN 58), Art. 28 DSGVO N 23, wonach die bisherige Vertragspraxis vieler Cloud-Anbieter für die Verantwortlichen faktisch keine hinreichenden Weisungs- und Kontrollmöglichkeiten eröffnet hätten und auch Dokumentationspflichten eingeschränkt realisierbar gewesen seien; entsprechend W. Kuan Hon/Christopher Millard, Banking in the cloud: Part 3 – contractual issues, 34 CLSR 595–614 (2018), 602, wonach sich Dienstleister üblicherweise das Recht ausbedingen würden, ihre Leistungen ohne vorgängige Ankündigung zu ändern.

den beschriebenen Vorgang als zulässig regelt.[76] Soweit der Dienstleister hingegen in Abweichung von den ursprünglichen Weisungen Verarbeitungen vornimmt, welche eigenmotiviert sind oder gar den nachweislichen Interessen des Dienstleistungsnehmers zuwiderlaufen, wird er zum Verantwortlichen.[77]

Bei Cloud-basierten Dienstleistungen innerhalb einer Unternehmensgruppe («Konzerndatenverarbeitungen») ist das Vorliegen einer Auftragsverarbeitung jedenfalls zweifelhaft, wenn die Muttergesellschaft der Dienstleister ist, zumal eine tatsächliche Weisungsgebundenheit dann kaum besteht.[78]

V. Anforderungen an die rechtmässige Übermittlung

A. Rechtfertigungsbedürftigkeit sowie Privilegierung bei Auftragsverarbeitung

Die Übermittlung von personenbezogenen Daten an einen Empfänger[79] stellt eine Verarbeitung dar.[80] Art. 6 Abs. 1 Satz 1 DSGVO statuiert für Verarbeitungen ein grundsätzliches Verbot mit Erlaubnisvorbehalt. Eine Erlaubnis – neben der Einwilligung der betroffenen Person etwa vertragliche oder rechtliche Pflichten – muss demzufolge im Grundsatz für jede Übermittlung bestehen. Dies gilt umso mehr für «sensible» Daten,[81] wobei hier die besonderen Erlaubnistatbestände von Art. 9 Abs. 2 DSGVO vorgehen.[82]

Nach mittlerweile wohl herrschender und auch hier vertretener Auffassung kann zumindest bei der Auftragsverarbeitung derweil auf eine zusätzliche Erlaubnis (zur Übermittlung an den Auftragsverarbeiter) verzichtet werden, sofern die Voraussetzungen gemäss Art. 28 DSGVO erfüllt sind. In datenschutzrechtlicher Hinsicht wird insoweit die Einheit von Verantwortlichem und Auftragsverarbeiter fingiert.[83] Ist ein Cloud-Dienstleister als Auftragsverarbeiter zu qualifizieren, ist mithin grundsätzlich keine weitere Rechtsgrundlage im Sinne von Art. 6 ff. DSGVO mehr erforderlich als diejenige, auf welche der Verantwortliche selbst die Verarbeitung stützt.[84]

Die Übermittlung personenbezogener Daten an Unternehmen derselben Unternehmensgruppe – z.B. wenn eine Konzernschwester die Cloud-basierten Dienstleistungen erbringt – kann zudem (nicht ausschliesslich) gestützt auf Art. 6 Abs. 1 lit. f DSGVO gerechtfertigt werden, zumal es «ein berechtigtes Interesse [begründen kann], personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschliesslich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln».[85]

B. Besondere Voraussetzungen bei der Übermittlung in Drittländer

Bei der Übermittlung von personenbezogenen Daten in Drittländer müssen hingegen – auch bei der Auftragsverarbeitung[86] – zusätzlich die Voraussetzungen des fünften Kapitels der Verordnung[87] eingehalten werden, welchen ein dreischrittiges Prüfprogramm zugrunde liegt:

- Vorliegen eines Angemessenheitsbeschlusses (Art. 45 DSGVO);
- Vorhandensein einer geeigneten Garantie oder von Binding Corporate Rules (Art. 46 f. DSGVO);
- Erfüllen einer Ausnahmevorschrift (Art. 49 DSGVO).

Sofern die Voraussetzungen einer Stufe erfüllt werden, erweist sich die Übermittlung als rechtmässig.[88] Keine

---

[76] Vgl. Art. 28 Abs. 2 DSGVO; Detlev Gabel/Holger Lutz, in: Jürgen Taeger/Detlev Gabel (Hrsg.), Kommentar DSGVO – BDSG, Frankfurt a.M. 2019, Art. 28 DSGVO N 63.

[77] S. IV.A. hiervor; weiterf. Rosenthal (FN 21), 20 ff., mit Abgrenzung zur gemeinsamen Verantwortung gemäss Art. 26 DSGVO; Bayerischer Landesbeauftragter für den Datenschutz (FN 37), 12.

[78] Petri (FN 54), Art. 28 DSGVO N 24 m.Hinw.

[79] S. Art. 4 Nr. 9 DSGVO, wovon auch der Auftragsverarbeiter erfasst wird, s. Regenhardt (FN 48), Art. 4 DSGVO N 155.

[80] S. III.A. hiervor; Wybitul/Ströbel/Ruess (FN 18), 504.

[81] S. III.A. hiervor.

[82] Kampert (FN 25), Art. 9 DSGVO N 63.

[83] Bayerischer Landesbeauftragter für den Datenschutz (FN 37), 7; gl.M. Bernd Schmidt/Bernhard Freund, Perspektiven der Auftragsverarbeitung, Wegfall der Privilegierung mit der DS-GVO?, ZD 2017, 14 ff. mit rigoroser Herleitung; Schwarzenegger/Thouvenin/Stiller (FN 4), 85; Schmid/Kahl (FN 58), 56 f.; Eckhardt (FN 57), 113; Rosenthal (FN 21), 4; im Ergebnis entsprechend Ingold (FN 58), Art. 28 DSGVO N 28 ff. m.Verw. auf a.M.; abweichend Regenhardt (FN 48), Art. 4 DSGVO N 155; ferner Barbara Schmitz/Jonas von Dall'Armi, Auftragsdatenverarbeitung in der DS-GVO – das Ende der Privilegierung?, Wie Daten künftig von Dienstleistern verarbeitet werden müssen, ZD 2016, 427 ff., 429 f.

[84] Damit ist zugleich gesagt, dass die Privilegierung auch für «sensible» Daten gilt, s. Schmid/Kahl (FN 58), 56.

[85] S. Erwägungsgrund 48 DSGVO.

[86] Schmidt/Freund (FN 83), 16; Petri (FN 54), Art. 28 DSGVO N 25.

[87] Art. 44 ff. DSGVO.

[88] Emanual V. Towfigh/Jacob Ulrich, in: Gernot Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. A., Baden-Baden/Wien/Zürich 2018, Art. 44 DSGVO N 7; grundlegend Kai von Lewinsky/Christoph Herrmann, Cloud vs. Cloud – Datenschutz im Binnenmarkt, Verantwortlichkeit und Zuständigkeit bei grenzüberschreitender Datenverarbeitung, ZD 2016, 467 ff., 472 ff.

Drittländer sind infolge ihrer Übernahme der DSGVO wie erwähnt die EWR-Staaten Island, Liechtenstein und Norwegen.[89]

1. Angemessenheitsbeschluss der Europäischen Kommission

Die Europäische Kommission kann beschliessen, dass ein Drittland ein angemessenes Schutzniveau bietet, sodass eine Datenübermittlung keiner besonderen Genehmigung bedarf.[90] Der hierdurch ermöglichte stete Datenfluss ist dem internationalen Handel sehr zuträglich. Die Kommission hat bei ihrer Beschlussfassung zu berücksichtigen, ob das Drittland über die rechtsstaatlichen Voraussetzungen sowie eine unabhängige Aufsichtsbehörde gemäss Art. 45 Abs. 2 DSGVO verfügt. Die Drittländer sind laufend zu überwachen, und es ist ein Mechanismus für eine regelmässige Überprüfung, die mindestens alle vier Jahre erfolgt, vorzusehen. Der Angemessenheitsbeschluss ist zu ändern, auszusetzen oder zu widerrufen, wenn das Drittland kein angemessenes Schutzniveau mehr gewährleistet.

Der Angemessenheitsbeschluss betreffend die Schweiz ist noch auf Grundlage von Art. 25 Abs. 6 der Richtlinie 95/46/EG erlassen worden und bleibt bis zur nächsten Überprüfung in Kraft.[91] Die Kommission wird das Schutzniveau der Schweiz voraussichtlich im Mai 2020 wieder überprüfen.[92] Der Ausgang wird wesentlich davon abhängen, ob die Revision des Datenschutzgesetzes rechtzeitig abgeschlossen und den inhaltlichen Anforderungen entsprechen wird.[93]

Als Nachfolger des vom EuGH in der Rechtssache *Schrems*[94] für unwirksam erklärten «Safe Harbor»-Abkommens mit den USA ist der sogenannte *EU–U.S. Privacy Shield* in Kraft getreten.[95] Es besteht aus einer Angemessenheitsentscheidung der Kommission mit einem Anhang, welcher die *Privacy Principles* und Briefe verschiedener US-Ministerien, die sich zur Anerkennung der Schutzstandards verpflichten, beinhaltet.[96] Unternehmen können sich zertifizieren lassen, wenn sie die besagten Prinzipien umsetzen und befolgen (tatsächliches Einhalten). Kontrollbehörden sind gemeinsam das US-Handelsministerium und die Kommission. Eine Datenübermittlung an zertifizierte Unternehmen in den USA bedarf demnach keiner besonderen Genehmigung.[97]

2. Weitere Möglichkeiten zur Legitimierung der Übermittlung

Falls kein Angemessenheitsbeschluss vorliegt, dürfen personenbezogene Daten – vorbehaltlich einer wirksamen Einwilligung oder sonstiger Ausnahmen gemäss Art. 49 DSGVO[98] – nur in ein Drittland übermittelt werden, sofern geeignete Garantien vorgesehen sind und den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen.[99]

Geeignete Garantien sind namentlich Standarddatenschutzklauseln *(standard contractual clauses)* gemäss Art. 46 Abs. 2 lit. c f. DSGVO. Sie werden entweder von der Kommission oder von einer mitgliedstaatlichen Aufsichtsbehörde erlassen, in letzterem Falle mit anschliessender Genehmigung durch die Kommission (Gewährleistung des DSGVO-Schutzniveaus). Weiter können verbindliche interne Datenschutzvorschriften *(binding corporate rules)* von der mitgliedstaatlichen Aufsichtsbehörde genehmigt werden, sodass jene als geeignete Garantien im Sinne von Art. 46 Abs. 2 lit. b DSGVO die Übermittlung von personenbezogenen Daten an entsprechende Unternehmen ohne weitere Genehmigung ermöglichen.[100] Auch genehmigte Verhaltensregeln *(codes of conduct)* nach Art. 40 DSGVO legitimieren zur Übermittlung, sofern die das Unternehmen vertretenden Verbände bzw. Vereinigungen solche Regeln aufgestellt und das Genehmigungsverfahren durchlaufen haben.[101] Schliesslich garantieren genehmigte Zertifizierungsmechanismen gemäss Art. 42 DSGVO ebenfalls ein angemessenes Schutzniveau. Die beiden letzten Möglichkeiten sollen

---

89 S. III.B. hiervor.

90 Art. 45 Abs. 1 DSGVO; zum Ganzen Jens Brauneck, EU-Handelshemmnis Datenschutz: Erleichterungen für Unternehmen durch DSGVO-Angemessenheitsbeschlüsse?, EWS 2019, 89 ff.

91 S. Art. 45 Abs. 9 DSGVO.

92 Lukas Mäder, Plötzlich soll es ganz schnell gehen – der Ständerat gibt beim Datenschutz Gas, NZZ vom 24.10.2019, 13 m.Hinw.

93 Vgl. Bundesrat, Stellungnahme vom 2. März 2018 zur Interpellation 17.4088 Fiala vom 13. Dezember 2017, Ziff. 1; s. auch Botschaft des Bundesrats vom 15. September 2017 zum Bundesgesetz über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz, BBl 2017 6943 ff., 6964 f.

94 EuGH, 6.10.2015, Rs. C-362/14, *Schrems*.

95 Zum Ganzen Fruzsina Molnár-Gábor/Laura Kaffenberger, EU-US-Privacy-Shield – Bedeutung des Angemessenheitsbeschlusses der EU-Kommission, Rechtsschutz bei der transatlantischen Verarbeitung personenbezogener Daten, ZD 2018, 162 ff.

96 Internet: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG (Abruf 15.11.2019).

97 Wybitul/Ströbel/Ruess (FN 18), 505 m.Hinw.; ferner Schmid/Kahl (FN 58), 54 f.; weiterf. zum US-amerikanischen CLOUD Act s. V.B.4. hiernach.

98 Weiterf. V.B.3. hiernach.

99 Art. 46 Abs. 1 DSGVO.

100 Towfigh/Ulrich (FN 88), Art. 47 DSGVO N 1.

101 S. Art. 46 Abs. 2 lit. e DSGVO.

die Privatwirtschaft zur «regulierten Selbstregulierung» bzw. «monitored self-regulation» animieren, sind derweil anspruchsvoll und aufwändig sowie als innovative Instrumente noch wenig erprobt.[102]

3. Wirksame Einwilligung und sonstige Ausnahmen

Eine wirksame Einwilligung muss freiwillig, informiert sowie ausdrücklich und konkret sein. Als Einwilligung zur Verarbeitung, welche die Übermittlung darstellt,[103] muss sie zugleich den (bloss streckenweise deckungsgleichen) Voraussetzungen von Art. 6 Abs. 1 bzw. Art. 9 Abs. 2 DSGVO genügen.[104]

Freiwilligkeit als Abwesenheit von Zwang bedingt Wahlfreiheit.[105] Keine Freiwilligkeit liegt vor, wenn ein «klares Ungleichgewicht» (in Form von Machtasymmetrien, besonderer Abhängigkeit oder übermässigen Anreizsystemen) zwischen der betroffenen Person und dem Verantwortlichen besteht.[106] Informiertheit bedingt die verständliche Aufklärung über alle relevanten Umstände der Übermittlung, namentlich auch über das Datenschutzniveau im Zielland.[107]

Sonstige Ausnahmen liegen vor, wenn die Datenübermittlung in Drittstaaten aus den in Art. 49 Abs. 1 lit. b–f DSGVO aufgeführten Gründen im konkreten Einzelfall erforderlich bzw. notwendig ist. Demnach muss die Übermittlung zur Erfüllung einer vertraglichen Leistungspflicht geboten und im Interesse der vertraglich begünstigten Person sein. Darüber hinaus können wichtige öffentliche, private oder lebenswichtige Interessen eine einzelfallweise Übermittlung rechtfertigen.[108]

4. Exkurs: Auskunftsbegehren gestützt auf den U.S. CLOUD Act

US-amerikanische Behörden können gestützt auf den U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act für strafrechtliche Zwecke auch ohne Rückgriff auf internationale Rechtshilfeabkommen (beziehungsweise unter deren Umgehung) Auskunftsbegehren betreffend personenbezogene Daten stellen, welche sich «within […] possession, custody, or control» eines in den USA domizilierten Unternehmens befinden. Dies gilt unabhängig davon, ob die personenbezogenen Daten «within or outside of the United States» liegen.[109] Dementgegen ist gemäss Art. 48 DSGVO eine Übermittlung oder Offenlegung von personenbezogenen Daten an ein Drittland grundsätzlich unzulässig, wenn sie nicht auf eine in Kraft befindliche internationale Übereinkunft wie ein Rechtshilfeabkommen zwischen dem ersuchenden Drittland und der Europäischen Union oder einem Mitgliedstaat gestützt ist. «Article 48 makes clear that a foreign court order does not in itself constitute a legal ground for transfer.»[110] Eine Verarbeitung und Übermittlung von personenbezogenen Daten aufgrund einer einseitigen Aufforderung von US-amerikanischen Behörden gestützt auf den CLOUD Act ist deswegen grundsätzlich nicht DSGVO-konform. Auch der *EU–U.S. Privacy Shield*[111] bietet hierfür keine Grundlage. Ausnahmsweise kommen nach gemeinsamer Auffassung des Europäischen Datenschutzbeauftragten und des Europäischen Datenschutzausschusses – in Abwesenheit einer ausdrücklichen Einwilligung der betroffenen Person[112] – lediglich Art. 6 Abs. 1 lit. d bzw. Art. 9 Abs. 2 lit. c i.V.m. Art. 49 Abs. 1 lit. f DSGVO als Rechtfertigung in Frage, wonach die Verarbeitung und Übermittlung der personenbezogenen Daten zum Schutz lebenswichtiger Interessen erforderlich ist und die betroffene Person aus physischen oder rechtlichen Gründen ausserstande ist, ihre Einwilligung zu geben.[113]

---

[102] Zum Ganzen Eric Lachaud, The General Data Protection Regulation and the rise of certification as a regulatory instrument, 34 CLSR 244–256 (2018); Towfigh/Ulrich (FN 88), Art. 46 DSGVO N 11 m.Hinw.

[103] S. V.A. hiervor.

[104] Wybitul/Ströbel/Ruess (FN 18), 507, Fn 77 m.Hinw.

[105] Ingold (FN 58), Art. 7 DSGVO N 26 und 29 m.Verw. auf Erwägungsgrund 42 DSGVO; es kommt massgeblich darauf an, ob die einwilligende Person «in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden».

[106] S. Erwägungsgrund 43 DSGVO.

[107] Wybitul/Ströbel/Ruess (FN 18), 507; zu den Anforderungen an die Ausdrücklichkeit und Konkretheit s. ebendort.

[108] Weiterf. Towfigh/Ulrich (FN 88), Art. 46 DSGVO N 6 ff.

[109] 18 U.S.C. § 2713; zur Vorgeschichte des CLOUD Act weiterf. Jennifer Daskal, Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0, 71(5) SLR 9–16 (2018); Tina Gausling, Offenlegung von Daten auf Basis des CLOUD Act, CLOUD Act und DS-GVO im Spannungsverhältnis, MMR 2018, 578 ff., 579; zur Legitimation des CLOUD Act aus US-amerikanischer Perspektive s. U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World, The Purpose and Impact of the CLOUD Act, White Paper, April 2019; vgl. Michael Rath/Axel Spies, CLOUD Act: Selbst für die Wolken gibt es Grenzen, CCZ 2018, 229 ff., 229; relativierend Christian Laux, Überwachung im Internet – das Superproblem unserer Zeit, Kolumne Lex Laux auf inside-it.ch (Internet: https://www.inside-it.ch/articles/52518 [Abruf 15.11.2019]).

[110] Europäische Kommission, Amicus Curiae brief in USA v. Microsoft corporation, 14.

[111] Weiterf. V.B.1. hiervor.

[112] Weiterf. V.B.3. hiervor.

[113] Europäischer Datenschutzbeauftragter/Europäischer Datenausschuss, Annex, Initial legal assessment of the impact of the US CLOUD Act on the EU legal framework for the protection of per-

VI. Verantwortung bei Cloud-basierten Dienstleistungen

A. Cloud-Dienstleistungsnehmer als Verantwortlicher

Während die Qualifikation des Cloud-Dienstleisters einige Schwierigkeiten bereitet,[114] verhält es sich beim Dienstleistungsnehmer klarer: Soweit er nicht bloss eigene personenbezogene Daten übermittelt und mithin betroffene Person ist,[115] handelt es sich um einen Verantwortlichen gemäss Art. 4 Nr. 7 DSGVO.[116]

Der Verantwortliche hat die Verarbeitung personenbezogener Daten gemäss der DSGVO sicherzustellen sowie hierfür den Nachweis zu erbringen.[117] Seine materiellen Pflichten beinhalten die Einhaltung der Grundsätze von Art. 5 Abs. 1 DSGVO, die Rechtfertigung der Verarbeitung gemäss Art. 6 ff. und Art. 44 ff. DSGVO[118] sowie die Gewährleistung der Rechte der betroffenen Person gemäss Art. 12 ff. DSGVO.[119]

Der Verantwortliche hat zu diesem Zweck geeignete technische und organisatorische Massnahmen (*technical and organisational measures,* TOMs) umzusetzen, welche gemäss Art. 24 Abs. 2 DSGVO unter Umständen auch «geeignete Datenschutzvorkehrungen» umfassen müssen.[120] Namentlich hat der Verantwortliche die Vorgaben der Verordnung zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Art. 25 DSGVO), zur Sicherheit der Datenverarbeitung (Art. 32 DSGVO) sowie zur Auftragsverarbeitung (Art. 28 DSGVO) zu berücksichtigen. Geeignete TOMs sind gemäss Art. 24 Abs. 1 DSGVO «unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen» festzulegen. Dies bedingt zuallererst eine Identifikation der besonderen Risiken, welche mit der Inanspruchnahme von Cloud-Dienstleistungen einhergehen.[121]

Bei Nichterfüllung drohen dem Verantwortlichen die Sekundärfolgen von Art. 82 ff. DSGVO (Schadenersatzansprüche, Geldbussen, mitgliedstaatliche Sanktionen). Darüber hinaus sollten die Reputationsschäden keinesfalls unterschätzt werden.[122]

B. Taxonomie der besonderen Risiken

1. Modellabhängigkeit

Die besonderen Risiken von Cloud-basierten Dienstleistungen sind sowohl dienstleistungsmodell- als auch bereitstellungsmodellabhängig:[123] Sie hängen einerseits mit der technischen Verantwortung zusammen, welche zwischen Cloud-Dienstleistungsnehmer und -Dienstleister aufgeteilt ist; sie liegen andererseits in der zur Verfügung stehenden Infrastruktur begründet. Hierbei können organisatorische, technische und rechtliche Risiken kategorisiert werden, wobei eine trennscharfe Zuteilung nicht durchwegs möglich ist.

2. Organisatorische Risiken

Ein bedeutendes organisatorisches Risiko besteht bei relativ unerfahrenen Cloud-Dienstleistungsnehmern darin, dass sie sich der Implikationen des «Cloud-Computing» zu wenig bewusst sind und infolgedessen unzureichende Schutzmechanismen einführen bzw. ungeeignete Sicher-

sonal data and the negotiations of an EU–US Agreement on cross-border access to electronic evidence, 3 ff.; s. auch Rath/Spies (FN 109), 229 f.; Gausling (FN 109), 581.

114 Weiterf. IV.B. hiervor.

115 S. IV.B.3. hiervor.

116 Zur Definition s. IV.A. hiervor.

117 Art. 24 Abs. 1 DSGVO; s. auch die Rechenschaftspflicht gemäss Art. 5 Abs. 2 DSGVO; hierzu Alexander Rossnagel, Wie zukunftsfähig ist die Datenschutz-Grundverordnung?, DuD 2016, 561 ff., 562; Alexander Jung, Datenschutz-(Compliance-)Management-Systeme – Nachweis- und Rechenschaftspflichten nach der DS-GVO, Praktikable Ansätze für die Erfüllung ordnungsgemässer Datenverarbeitung, ZD 2018, 208 ff., 208.

118 Weiterf. V. hiervor.

119 Raschauer (FN 54), Art. 4 DSGVO N 121; Petri (FN 54), Art. 24 DSGVO N 1; zum Ganzen Praz (FN 30), AJP 2018, 612 f.; Tim Hickman/Detlev Gabel, Rights of Data Subjects under the GDPR, C&L 2016, February/March; weiterf. Bob Duncan/Karen Renaud/Beverley Mackenzie, Investigating the Tension between Cloud-Related Actors and Individual Privacy Rights, in: Bob Duncan/Lee Young Woo/Magnus Westerlund/Andreas Assmuth (Hrsg.), Cloud Computing 2019, The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization, Venedig 2019, 19 ff.

120 Weiterf. zur umstrittenen eigenständigen Bedeutung der letzteren Vorgabe s. Petri (FN 54), Art. 24 DSGVO N 22 ff.; vgl. Kevin McGillivray, A right too far? Requiring cloud service providers to deliver adequate data security to consumers, 25 IJLIT 1–25 (2017).

121 Weiterf. VI.B. hiernach.

122 S. Bob Duncan/Yuan Zhao, Cloud Compliance Risks, in: Bob Duncan/Lee Young Woo/Magnus Westerlund/Andreas Assmuth (Hrsg.), Cloud Computing 2019, The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization, Venedig 2019, 31 ff., 35.

123 Ebenso Lins/Schneider/Sunyaev (FN 5), 13; zu den verschiedenen Dienstleistungs- und Bereitstellungsmodellen weiterf. II.B. f. hiervor.

heitsgarantien einfordern.[124] Dies kann zum Verlust der Kontrolle über die personenbezogenen Daten führen. Damit verbunden sind die Risiken, welche von nicht sorgfältig ausgewählten und fortlaufend geschulten Mitarbeitenden ausgehen.[125]

Weiter kann eine nicht hinlänglich klare Zuteilung von Verantwortlichkeiten zwischen Dienstleister und Dienstleistungsnehmer zu Sicherheitslücken führen. Auch besteht beim Beizug von Unterbeauftragten durch den Dienstleister das Risiko, dass jene unzureichend im Hinblick auf die Sicherheit und Verfügbarkeit der personenbezogenen Daten kontrolliert werden.[126]

Bereits hingewiesen wurde auf das organisatorische Risiko eines «lock in»-Effekts, welcher sich namentlich beim Beizug von PaaS-Dienstleistern ergeben kann.[127] Schliesslich hat der Dienstleistungsnehmer bei sämtlichen Dienstleistungsmodellen regelmässig keine eigentliche physische Kontrolle über die Infrastruktur eines unabhängigen Unternehmens als Cloud-Dienstleister, was Sicherheitsrisiken in sich birgt.[128]

3. Technische Risiken

Technische Risiken können sich bei Cloud-basierten Dienstleistungen insbesondere ergeben, wenn jene – wie etwa bei Public-Clouds und kombinierten Bereitstellungsmodellen üblich – über das (offene) Internet angeboten werden. «Distributed Denial of Service»-Angriffe können die Verfügbarkeit stark einschränken und hohe Kosten verursachen. Zudem besteht das Risiko von Angriffen während der Datenübertragung, und oftmals werden insbesondere SaaS-Dienste auf der Anwendungsebene attackiert.[129]

Der unberechtigte Zugriff sowie böswillige Veränderungen bzw. Löschungen sollten durch geeignete Authentifizierungs- und Identifizierungsverfahren verhindert oder zumindest mittels Protokollierungsmechanismen aufgezeichnet werden. Als «the elephant in the room» wird derweil die Tatsache bezeichnet, dass ein Eindringling in einer Cloud-basierten Infrastruktur mit hinreichenden Zugriffsmöglichkeiten gar seine Spuren «verwischen» kann, sodass der forensische Nachweis seines Angriffs unmöglich ist.[130]

Sowohl bei Public- als auch bei Community-Clouds und kombinierten Bereitstellungsmodellen besteht weiter die grundsätzliche Gefahr, dass andere Dienstleistungsnehmer – und seien es bloss Unternehmen derselben Unternehmensgruppe – unberechtigterweise Zugriff auf personenbezogene Daten erhalten. Bei SaaS-Dienstleistungsmodellen akzentuiert sich dies insofern, als eine Pseudonymisierung nur beschränkt möglich ist.[131]

Technische Risiken bestehen zugleich hinsichtlich der Rechte der betroffenen Person gemäss Art. 12 DSGVO: Ihre Ausübung kann unzulässiger Weise erschwert oder verunmöglicht werden, wenn die personenbezogenen Daten von Cloud-Dienstleistern verarbeitet werden. Namentlich die Rechte auf Löschung sowie (gegebenenfalls vorgängige) Datenübertragbarkeit (Art. 17 und Art. 20 DSGVO)[132] können hiervon betroffen sein. Es besteht das Risiko, dass der Cloud-Dienstleister bloss «logisch löscht», d.h. die Verknüpfung oder den Verweis im Dateisystem entfernt, wobei die personenbezogenen Daten schwieriger auffindbar sind, hingegen weiterhin erhalten bleiben.[133]

4. Rechtliche Risiken

Rechtliche Risiken sind einerseits die vorgenannten organisatorischen und technischen Risiken, jedenfalls so-

---

124 Europäischer Datenschutzbeauftragter, Leitlinien zur Nutzung von Cloud-Computing-Diensten durch die Organe und Einrichtungen der EU, 16. März 2018, 51.

125 S. auch Hon/Millard (FN 1), 8 f.

126 Lins/Schneider/Sunyaev (FN 5), 14 m.Hinw. auf die regelmässige Nutzung der Ressourcen eines PaaS-Dienstleisters durch SaaS-Dienstleister; weiterf. zum «layering» von Dienstleistungsmodellen s. Hon/Millard (FN 1), 6.

127 S. II.B.3. hiervor.

128 Europäischer Datenschutzbeauftragter (FN 124), 55 f.

129 Lins/Schneider/Sunyaev (FN 5), 15 m.Verw.; eine Darstellung verschiedener Angriffsformen findet sich bei Bob Duncan, EU General Data Protection Regulation Compliance Challenges for Cloud Users, in: Bob Duncan/Lee Young Woo/Magnus Westerlund/Andreas Assmuth (Hrsg.), Cloud Computing 2019, The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization, Venedig 2019, 25 ff., 26 f.

130 Bob Duncan, Can EU General Data Protection Regulation Compliance be Achieved When Using Cloud Computing?, in: Bob Duncan/Lee Young Woo/Aspen Olmsted (Hrsg.), Cloud Computing 2018, The Ninth International Conference on Cloud Computing, GRIDs, and Virtualization, Barcelona 2018, 1 ff., 3.

131 S. IV.B.2. hiervor.

132 Zum Verhältnis s. nur Alexander Dix, in: Spiros Simitis/Gerrit Hornung/Indra Spiecker (Hrsg.), Datenschutzrecht, DSGVO mit BDSG, Baden-Baden 2019, Art. 20 DSGVO N 16; zum Ganzen Paul de Hert/Vagelis Papakonstantinou/Gianclaudio Malgieri/Laurent Beslay/Ignazio Sanchez, The right to data portability in the GDPR: Towards user-centric interoperability of digital services, 34 (2018) CLSR 193–203.

133 S. Dix (FN 132), Art. 17 DSGVO N 5 m.Verw. auf Löschsoftware, welche eine physikalische Löschung nunmehr mit verhältnismässigem Aufwand erlauben soll; a.M. Enrico Peuker, in: Gernot Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, Handkommentar, 2. A., Baden-Baden/Wien/Zürich 2018, Art. 17 DSGVO N 32, welcher das Löschen von Verknüpfungen genügen lässt.

weit ihre Materialisierung nach der DSGVO sanktionsbeschwert ist oder Haftungsfolgen zeitigt. Andererseits sind in diesem Zusammenhang konfligierende Vorgaben anderer Jurisdiktionen zu erwähnen. Deren Anwendbarkeit setzt regelmässig einen (nach den Massstäben der jeweiligen Rechtsordnung) hinreichenden Bezug voraus. Letzterer kann mit der Verarbeitung bzw. blossen Speicherung personenbezogener Daten in einem bestimmten Hoheitsgebiet *(data residency)* oder gegebenenfalls gar schon bei Besitz, Gewahrsam oder Kontrolle über personenbezogene Daten in ausländischen Rechenzentren gegeben sein.[134] Rechtliche Risiken bestehen diesfalls namentlich, wenn unklar ist, wo die personenbezogenen Daten gespeichert werden oder wer in die Erbringung der Cloud-basierten Dienstleistung involviert ist. So kann etwa bei manchen SaaS-Dienstleistern der Speicherort in räumlicher Hinsicht nicht festgelegt werden,[135] oder der Dienstleistungsnehmer sieht sich im Falle einer nicht vorgängig bekanntgegebenen Unterbeauftragung plötzlich mit einem Verarbeiter konfrontiert, welcher einer anderen Jurisdiktion untersteht.

C. Geeignete Massnahmen

Der verantwortliche Dienstleistungsnehmer sollte den Umgang mit den vorerwähnten organisatorischen, technischen und rechtlichen Risiken alsdann in unternehmensinternen Datenschutzrichtlinien und konkretisierenden Arbeitsanweisungen festhalten.[136] In organisatorischer Hinsicht ist ausnahmslos sicherzustellen, dass die involvierten Unternehmenskreise die unternehmensinternen Vorgaben kennen sowie über das notwendige Know-how für die Inanspruchnahme von Cloud-basierten Dienstleistungen verfügen (Mitarbeiterschulungen, Beizug von externen Fachkräften).[137]

Von zentraler Bedeutung ist weiter, dass die technischen Verantwortungen, welche sich aus den jeweiligen Dienstleistungsmodellen ergeben,[138] in den schriftlichen Cloud-Dienstleistungsverträgen durchgängig klar zugeteilt werden. Für die Auftragsdatenverarbeitung enthält Art. 28 Abs. 3 DSGVO einen Katalog notwendiger Vertragskriterien.[139] Cloud-Dienstleister, die genehmigte Verhaltensregeln befolgen oder zertifiziert[140] sind, bieten eine erhöhte Gewähr für Datenschutzkonformität, auf welche die Dienstleistungsnehmer in begründeten Fällen vertrauen dürfen.[141] Eine vertragliche Regelung drängt sich gleichermassen auf, wenn der Dienstleister als Verantwortlicher zu qualifizieren ist.[142] In beiden Fällen sollten sich die Dienstleistungsnehmer zudem ausbedingen, dass sie die Infrastruktur des Dienstleisters vor der Datenübertragung sowie während der Vertragsdauer inspizieren dürfen.

In technischer Hinsicht sollten personenbezogene Daten vor der Übertragung und Auslagerung durch eine möglichst starke Pseudonymisierung geschützt werden.[143] Eine Auslagerung in SaaS-Dienstleistungsmodelle sollte demzufolge grundsätzlich nicht erfolgen, zumal diese besonders oft auf der Anwendungsebene attackiert werden und keine hinreichende Pseudonymisierung erlauben.[144] Auch sollten jeweils (vorzugsweise lokale) Sicherungskopien der ausgelagerten personenbezogenen Daten angefertigt werden, um deren endgültigem Verlust vorzubeugen.[145] Die Pseudonymisierung kann auch dem unberechtigten Zugriff anderer Dienstleistungsnehmer bei Public- und Community-Clouds entgegenwirken. Bei Community-Clouds sind zudem hinreichende *chinese walls* (Beschränkungen der Zugriffsrechte anderer Organisationen derselben Gruppe) vorzusehen. Ferner sind lediglich Cloud-Dienstleister zu beauftragen, welche die Betroffenenrechte, insbesondere das Recht auf Löschung der personenbezogenen Daten, tatsächlich zu gewährleisten vermögen (Verwendung tauglicher Löschsoftware).

Den rechtlichen Risiken ist insbesondere dadurch zu begegnen, dass der Cloud-Dienstleister einerseits anhand

---

134 Weiterf. zum US-amerikanischen CLOUD Act s. V.B.4. hiervor.

135 S. Hon/Millard (FN 75), 597; s. auch Europäischer Datenschutzbeauftragter (FN 124), 52 f.; zu den besonderen Voraussetzungen für eine zulässige Übermittlung personenbezogener Daten in Drittländer weiterf. V.B. hiervor.

136 Jung (FN 117), 212 f.; Duncan/Zhao (FN 122), 34; Petri (FN 54), Art. 24 DSGVO N 16.

137 Michael Wiedmann/Marco Greubel, Compliance Management Systeme – Ein Beitrag zur effektiven und effizienten Ausgestaltung, CCZ 2019, 88 ff., 91.

138 Weiterf. II.B. hiervor.

139 Ingold (FN 58), Art. 28 DSGVO N 51; weiterf. IV. hiervor; Bayerischer Landesbeauftragter für den Datenschutz (FN 37), 15 ff.; Eckhardt (FN 57), 113 ff.; s. auch Rosenthal (FN 21), 49 f.

140 Art. 28 Abs. 5 i.V.m. Art. 40 ff. DSGVO; Georg Borges, Cloud Computing und Datenschutz, Zertifizierung als Ausweg aus einem Dilemma, DuD 2014, 165 ff.; s. auch Art. 28 Abs. 1 DSGVO: Pflicht des Verantwortlichen, bloss mit Auftragsverarbeitern zusammenzuarbeiten, welche «hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Massnahmen» eingehalten werden; ein Überblick über die verschiedenen Zertifizierungsarten im Cloud-Service-Umfeld findet sich bei Lins/Schneider/Sunyaev (FN 5), 18.

141 S. Hofmann/Rossnagel (FN 58), 77 f.; Artikel-29-Datenschutzgruppe (FN 9), 27; vgl. Niklas Luhmann, Vertrauen, 5. A., Konstanz/München 2014, 31.

142 Ebenso Rosenthal (FN 21), 25 ff. m.w.Hinw.; weiterf. IV. hiervor.

143 Entsprechend Schweizerische Bankiervereinigung (FN 3), 13.

144 S. VI.B.3. u. II.B.4. hiervor.

145 Ebenso Duncan (FN 129), 28.

der Jurisdiktionen ausgewählt wird, denen er potenziell untersteht. Andererseits sind in den Dienstleistungsverträgen die zulässigen *data residencies* der personenbezogenen Daten – gerade auch im Falle einer vertraglich nicht ausgeschlossenen Unterbeauftragung[146] – ausdrücklich zu regeln. Soweit die besagten Festlegungen namentlich bei gewissen SaaS-Modellen verunmöglicht werden und infolgedessen auch die Rechtmässigkeit der Übermittlung in Drittländer[147] zu Zweifeln Anlass gibt, sollten auch deswegen keine personenbezogenen Daten in solche Dienste ausgelagert werden.

Namentlich in den Vereinigten Staaten domizilierte Cloud-Dienstleister versuchen dem Dilemma, entweder gegen die Bestimmungen des U.S. CLOUD Act oder der DSGVO verstossen zu müssen,[148] einerseits mit Abspaltungen von Unternehmensteilen und andererseits mit «Datentreuhand»-Modellen zu begegnen:[149] Beide Ansätze verfolgen die Auslagerung der personenbezogenen Daten zu rechtlich unabhängigen, der Gerichtsbarkeit der Vereinigten Staaten nicht unterstehenden Personen. Allerdings wird sich weisen müssen, inwieweit die US-amerikanischen Gerichte in solchen Fällen namentlich auf keine «control» mehr schliessen werden, welche hochgradig auslegungsbedürftig ist.[150]

Schliesslich können sowohl die skizzierten Cloud-relevanten TOMs als auch weitere unternehmensinterne Vorgaben längerfristig bloss eine wirksame Begrenzung datenschutzrechtlicher Risiken begründen, wenn ihre Wirksamkeit kontinuierlich überprüft und die Weisungen erforderlichenfalls überarbeitet sowie den involvierten Unternehmenskreisen wiederum zur Kenntnis gebracht werden.[151]

VII. Schlussbetrachtung

Cloud-basierte Dienstleistungen stellen eine datenschutzrechtliche Herausforderung dar. Kritische Faktoren sind insbesondere die Sicherheit und der Speicherort der personenbezogenen Daten. Die DSGVO enthält strikte und sanktionsbewehrte Vorgaben, deren Einhaltung nicht zuletzt aufgrund ihres breiten Anwendungsbereichs auch für in der Schweiz domizilierte Unternehmen generell geboten erscheint. Das Effizienzpotenzial des «Cloud Computing» kann infolgedessen nicht restlos ausgeschöpft werden: SaaS-Dienstleistungsmodelle erweisen sich etwa in mehrfacher Hinsicht als problematisch; tendenziell drängt das Unionsrecht die Cloud-Dienstleistungsnehmer in Community- und Private-Clouds. Diese «kleineren Wolken» sind derweil das Ergebnis eines gesellschaftspolitischen Diskurses bzw. dem normgeberischen Willen geschuldet, das Grundrecht auf Personendatenschutz auch im digitalen Zeitalter zu gewährleisten. Fortan werden es vermehrt Lehre und Rechtsprechung sein, welche im Rahmen der (Norm-)Auslegung die unternehmerischen, persönlichen und notabene geopolitischen Interessen austarieren müssen.

---

146 Art. 28 Abs. 4 DSGVO regelt die Pflichten des Auftragsverarbeiters bei der Unterbeauftragung (vertragliche Auferlegung der Datenschutzpflichten auf den Unterbeauftragten; Haftung für Verletzung der Datenschutzpflichten durch den Unterbeauftragten gegenüber dem Verantwortlichen).

147 Weiterf. V.B. hiervor.

148 S. V.B.4. hiervor; relativierend David Rosenthal, Banken & Co. in die Cloud, Präsentation anlässlich der 3. Datenschutzrechtstagung – Schweizer Forum für Kommunikationsrecht SFFS, 29. Mai 2019 (Folien abrufbar unter https://media.homburger.ch/karmarun/image/upload/homburger/BJ7qKhG0V-2019-05-29_Banken%20in%20die%20Cloud_ROD.pdf [Abruf 15.11.2019]), Folie 11: «zu Unrecht ein Schreckgespenst»; abwägend Europäischer Datenschutzbeauftragter/Europäischer Datenausschuss (FN 113), 2.

149 S. Gausling (FN 109), 581 f.; Rath/Spies (FN 109), 230, Giorgio V. Müller, Firmen gehen beim Cloud-Computing unkalkulierbare Risiken ein, NZZ vom 17.5.2019, 30, je m.Hinw.

150 Vgl. Art. 18 Abs. 1 des Übereinkommens über Computerkriminalität vom 23. November 2001 und den dazugehörigen Explanatory Report, N 173, wonach «a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not *necessarily* constitute ‹control› within the meaning of this provision» (Hervorhebung hinzugefügt); weiterf. zu den in den Vereinigten Staaten zur Beurteilung der «control» von den Gerichten angewandten «legal right»- und «practical ability»-Tests s. Tess Blair/Tara S. Lawler, Possession, Custody or Control: A Perennial Question gets more complicated, The Legal Intelligencer, 5. Februar 2018, 2 f.; Europäischer Datenschutzbeauftragter/Europäischer Datenausschuss (FN 113), 2.

151 S. Art. 24 Abs. 1 Satz 2 DSGVO; Petri (FN 54), Art. 24 DSGVO N 19 ff., Duncan/Zhao (FN 122), 34; weiterf. Alexander Jung, Key Performance Indicators zur Messung der Effizienz eines Datenschutz-Management-Systems, CCZ 2018, 224 ff.