Christina Rost/Dr. Stefan Brink/Tobias Birk

Cloud Computing und Datenschutz

Datenschutz ist technologisch agnostisch – und er muss es sein, denn staatliche Vorgaben zur Datenverarbeitung können Ziele und Standards vorgeben, aber grundsätzlich nicht komplette Technologien festlegen oder ausschließen. Trotzdem fordert uns jede neue Technologie heraus, sie mit den Vorgaben des Datenschutzes in Einklang zu bringen. Cloud Computing ist dafür ein besonders wichtiges Beispiel.

I. Die gespaltene Wirklichkeit

Cloud Computing in verschiedensten Ausprägungen ist heute Stand der Technik. Ähnlich wie der Verbrennungsmotor im späten 19. Jahrhundert andere mögliche Energiequellen im Individualverkehr ablöste, ist Cloud Computing im 21. Jahrhundert zur Grundlage von Digitalisierung schlechthin geworden: keine Fortschritte bei der Digitalisierung ohne Cloud Computing.

Völlig untechnisch formuliert ist Cloud Computing nichts anderes als die Idee, Ressourcen, in diesem Fall IT-Ressourcen, auf Knopfdruck und in Echtzeit zur Verfügung stellen zu können. Ob es um einen Abruf aus der Kundendatenbank geht, ob es die Verwaltung von Mitarbeiterdaten betrifft, Texte bzw. Dokumente in Echtzeit mehreren zur Verfügung gestellt werden sollen oder der Arbeitsplatz auf verschiedenen Endgeräten zur Verfügung gestellt werden soll – Cloud Computing macht dies ohne Zeitverlust von einer beliebigen Basisstation möglich. Die Nutzung von Kalenderfunktionen oder die Kommunikation via E-Mail von verschiedenen Endgeräten aus ist selbstverständlich – man ist heute immer auf dem aktuellsten Stand. Fast genauso selbstverständlich nutzen wir Dienste wie GoogleDocs, Dropbox, S3 Buckets und vergleichbare Angebote. Cloud Computing macht im Jahr einen weltweiten Markt von 197 Milliarden Dollar,[1] in Deutschland 12, 1 Mrd. Euro[2] aus, aber vor allem ist Cloud Computing die Basis von Wirtschaftswachstum und digitalem Fortschritt.

In Deutschland allerdings herrscht beim Thema Cloud Computing eine eher zögerliche Stimmung. Anders als in anderen EU-Ländern haben einige potentielle Nutzer von Cloud-Dienstleistern im öffentlichen Sektor und in der Privatwirtschaft offenbar das Gefühl, sie könnten wegen vermeintlicher (datenschutz-)rechtlicher Risiken Cloud Computing nicht ohne weiteres einsetzen. Das führt bei den betreffenden Unternehmen bzw. Behörden zu einer faktischen „No Cloud Policy" und bremst Innovationen „Made in Germany" aus, da solche heutzutage in großen Teilen auf der Basis von Cloud-Lösungen entwickelt werden, z.B. bei künstlicher Intelligenz, in der Medizintechnik und im Maschinenbau. Wir haben es also mit einer Spaltung zu tun, nämlich der wachsenden Bedeutung von Cloud Computing für Innovationen einerseits und der zögerlichen Haltung in Wirtschaft und Verwaltung andererseits. Diese Unsicherheit gefährdet dabei nicht nur die Innovationsfähigkeit und digitale Zukunftsfähigkeit unseres Landes, sondern auch das Vertrauen in den Datenschutz als technologisch offenes, zukunftsfähiges Schutzinstrument.

In der COVID-19 Krise zeigte sich der Bedarf nach Cloud Computing besonders nachdrücklich – und wurde unter dem Druck der Pandemie gegen vorhandene Bedenken zügig umgesetzt. Schnell und konsequent nutzte die deutsche Verwaltung die Möglichkeiten der Cloud, um die eigene Handlungs- und Gestaltungsfähigkeit aufrecht zu erhalten bzw. zu verbessern. Ob bei spontanen Video-Konferenzen, beim Skalieren von Soforthilfe, bei virtuellen Rechenzentren, bei der Verlegung der Schulen ins Digitale oder bei der Integration von KI in die Pandemie-Forschung. Aber das was in der Krise spontan und außerhalb der normalen Prozesse funktionieren kann, ist in einer Welt der „No-Cloud-Policies" möglicherweise nur schwer aufrecht zu halten. Deshalb braucht es einen Plan, die positiven Erfahrungen der letzten Wochen zu „normalisieren" und in den Regelbetrieb zu überführen.

All dies verdeutlicht die Notwendigkeit, die Debatte um Cloud Computing und Datenschutz nochmals zu reflektieren. Die Datenschutzgrundverordnung (DS-GVO) soll kein industriepolitisches Instrument sein, das spezifische Technologien verbietet, sondern versteht sich als ein wichtiges und mächtiges Rahmenwerk für Datenschutz in unserer Zeit.

Ziel dieses Beitrags ist es, die Diskussion zum Thema Datenschutz im Bereich des Cloud Computings fortzuführen und mehr Klarheit in diesem von Missverständnissen und Unklarheiten geprägten Feld zu fördern. Dabei wird die DS-GVO reflektiert und eingeordnet, zudem werden kurz- und mittelfristige Wege für eine Konkordanz gegenläufiger Aspekte aufgezeigt.

Folgende Fragen sollen dabei unter den folgenden Punkten reflektiert werden:

- Welche Herausforderung stellt ein Auftragsverarbeitungsvertrag nach Art. 28 DS-GVO? Verhindern datenschutzrechtliche Vorgaben die Nutzung von Clouddiensten? Sind bestehende Bedenken berechtigt? Wie kann bestehende Unsicherheit „gemanagt" werden?
- Welche Rolle spielt Art. 48 DS-GVO in diesem Kontext? Wird Art. 48 DS-GVO missverstanden oder zu restriktiv ausgelegt? Welche Reichweite hat der CLOUD Act tatsächlich und verdient er überhaupt die Aufmerksamkeit, die ihm entgegengebracht wird?
- Welche Lösungsmöglichkeiten bestehen für den scheinbaren Konflikt? Welche Hilfestellung würde Entscheidern zugutekommen?

1 www.de.statista.com.

2 www.de.statista.com.

II. Auftragsverarbeitungsvertrag nach Art. 28 DS-GVO

Der Auftragsverarbeitungsvertrag (AVV) nach Art. 28 DS-GVO ist einer der zentralen Dreh- und Angelpunkte[3] im Kontext der Verarbeitung von personenbezogenen Daten in der Cloud. Der Vertrag beinhaltet die Vorgaben und Anforderungen an den Auftragnehmer über die Verarbeitung und Speicherung von personenbezogenen Daten auf dem Schutzniveau der DS-GVO. Damit scheint er auf den ersten Blick sehr komplex, da er umfassend die Regelungen der DS-GVO aufgreift. Aber da inzwischen ein großer Teil der Auslegungsfragen durch den Europäischen Datenschutzausschuss (EDSA) geklärt wurde,[4] ist Art. 28 DS-GVO als gelungene Hilfestellung für die Gestaltung eines Auftragsverarbeitungsvertrag zu sehen. Im Vordergrund steht die Klärung der Verantwortlichkeiten zwischen den Vertragspartnern und die Umsetzung der Pflichten aus der DS-GVO zur Vermeidung von Verstößen.[5] Verantwortlicher i. S. d. DS-GVO ist und bleibt in erster Linie der Nutzer der Cloud. Daher hat der Nutzer als Verantwortlicher mit dem CLOUD-Dienstleister einen AVV zu schließen, der den Anforderungen des Art. 28 DS-GVO gerecht wird.[6]

In einem solchen AVV sind nach Art. 28 DS-GVO mindestens die folgenden Punkte zwingend zu regeln:

- Gegenstand und Dauer der Verarbeitung, auch im Hinblick auf einen Transfer in ein Drittland,
- Art und Zweck der Verarbeitung,
- Art der personenbezogenen Daten und Kategorien von betroffenen Personen (z.B. Mitarbeiter oder Nutzer),
- Umfang der Weisungsbefugnisse,
- Verpflichtung der zur Verarbeitung befugten Personen zur Vertraulichkeit,
- Sicherstellung von technischen und organisatorischen Maßnahmen i.S.v. Art. 32 DS-GVO,
- Hinzuziehung von Subunternehmen unter Einhaltung von Art. 28 Abs. 2 und 3 DS-GVO,
- Unterstützung des für die Verarbeitung Verantwortlichen bei Anfragen und Ansprüchen Betroffener sowie bei der Meldepflicht bei Datenschutzverletzungen nach Art. 33 DS-GVO,
- Rückgabe oder Löschung personenbezogener Daten nach Abschluss der Auftragsverarbeitung,
- Kontrollrecht des für die Verarbeitung Verantwortlichen, z.B. Einholen von Informationen über technisch-organisatorische Maßnahmen mittels Fragebögen oder Inspektionen vor Ort.

Hierzu sollten die Verantwortlichen bereits in einer frühen Phase der Überlegungen und Planungen eine Check-Liste erstellen, damit keiner der o. g. Punkte in der Umsetzung untergeht. Früh bedeutet in diesem Fall, VOR dem Ausschreibungsverfahren, zumal die Entscheidung über die Ausgestaltung der Punkte sich nicht unwesentlich auf die Vertragsgestaltung auswirken kann.[7]

In der Summe verhindern die datenschutzrechtlichen Vorgaben aus der Auftragsverarbeitung nicht die Cloudnutzung, sie ermöglichen eine Cloudnutzung unter Wahrung des Schutzes personenbezogener Daten und fördern das Vertrauen der Nutzerinnen und Nutzer der Dienste in Cloud Computing. Die bestehende Unsicherheit kann durch Transparenz und optimales Projektmanagement deutlich reduziert werden. Art. 28 DS-GVO stellt für die Fragen um die erforderlichen Regelungen in der Auftragsverarbeitung die Roadmap.[8]

III. Übermittlung in Drittländer

Bei den rechtlichen Risiken im Zusammenhang mit der Cloud ist die größte Unsicherheit die Frage der Übermittlung von personenbezogenen Daten in Drittländer. Dadurch, dass die Cloud eben nicht nur „deutsch"[9] oder europäisch ist, sondern die Cloud Solution Provider (CSP) global agieren, unterliegen die CSP gesetzlichen Bestimmungen verschiedener Länder – ggf. auch denen eines Drittlandes. Aufgrund dieser Tatsache kann es dazu kommen, dass für den Cloud-Nutzer und den CSP auf den ersten Blick konkurrierende Regelungen zur Anwendung kommen können, bspw. wenn etwa ausländisches Recht in bestimmten Fällen die Offenlegung gewisser Daten verlangt, das europäische Recht hingegen Offenlegungen in Drittländern enge Grenzen setzt.

Die Rahmenbedingungen für die Übermittlung von personenbezogenen Daten in Drittländer sind in Art. 44-50 DS-GVO geregelt.[10] Die eine Fragestellung betrifft die befugte Verarbeitung von personenbezogen Daten mittels Drittlandtransfer. Die andere Problematik in dem Kontext ist die Forderung nach Offenlegung von Daten in der Cloud gegenüber dem Drittland wegen krimineller Vorkommnisse (Art. 48 DS-GVO). Während Verständnis und Auslegung der Art. 44 ff. DS-GVO sich nun an der Schrems II Entscheidung des EuGHs vom 16.7.2020 (Az. C 311/18) teilweise neu orientieren müssen, wird im Kontext mit Art. 48 DS-GVO insbesondere der Cloud Act diskutiert. Dieser Beitrag kann die hierbei auftauchenden Fragen nicht in der gebotenen Tiefe

3 Die zivilrechtlichen Vereinbarungen werden an dieser Stelle nicht behandelt, für den Überblick Spindler/Sein, MMR 2019, 488 ff.; Heydn, MMR 2020, 435 ff., Lehmann GRUR Int. 2015, 677 ff.; Wicker, MMR 2012, 783; Nägele/Jacobs, ZUM 2010, 281 ff.

4 Zu den bereits erlassenen Leitlinien gehören u.a. WP 250 rev.01, 243 rev.01, 24 2rev.01, 260 rev.01 sowie die Guidelines 1/2018, 2/2018, 4/2019, 5/2019 und 2/2020, s. https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de.

5 S. vor allem Art. 83 Abs. 4, lit. a u. Abs. 5 lit. a und c DS-GVO; s.a. Möllenkamp/Ortmann, ZD 2019, 445, 446 ff.

6 Dazu Möllenkamp/Ortmann, ZD 2019, 445 ff.; Hofmann, ZD-Aktuell 2017, 05488; Eckhardt, CCZ 2017, 111 f.

7 S. Dahmen, BKR 2019, 533 ff.; Funke/Wittmann, ZD 2013, 221 ff.

8 Für weitere Informationen gibt es Hinweise in dem Kurzpapier Auftragsverarbeitung Nr. 13 der DSK, https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf.

9 Zum Thema deutsche Cloud Wischner am 28.08.2019, in: https://www.heise.de/newsticker/meldung/Microsoft-startet-neuen-Cloud-Versuch-in-Deutschland-4508151.html; Benrath, in: FAZ v. 04.10.2019, https://www.faz.net/aktuell/wirtschaft/digitec/cloud-aus-deutschland-die-suche-nach-dem-hyperscaler-16411233.html; Schüler am 31.08.2018, in: https://www.heise.de/newsticker/meldung/Auslaufmodell-Microsoft-Cloud-Deutschland-4152650.html; Benrath, in: FAZ am 31.01.2020, https://www.faz.net/aktuell/wirtschaft/digitec/digitale-technik/digitale-infrastruktur-waechst-der-aufstieg-der-cloud-16575213.html.

10 Dazu Piltz, K&R 2016, 777 ff.

betrachten und auch nicht umfassend diskutieren, er soll und kann aber zur Diskussion anregen.

IV. Übermittlungsmöglichkeiten von personenbezogenen Daten in Drittländer

Grundsätzlich besteht ein allgemeines Verbot der Übermittlung von personenbezogenen Daten an Drittländer ohne angemessenes Datenschutzniveau (Art. 44 DS-GVO). In jedem Fall sind Datenübermittlungen an Drittländer oder eine andere internationale Organisation nur unter strikter Einhaltung der DS-GVO zulässig. Eine Datenübermittlung kann nur dann stattfinden, wenn die in der DS-GVO festgelegten Bedingungen zur Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen vorbehaltlich der übrigen Bestimmungen der DS-GVO von dem Verantwortlichen oder dem Auftragsverarbeiter erfüllt werden.[11] Diesen Spagat hat der Vertrag über die Auftragsverarbeitung nach Art. 28 Abs. 3 lit. a DS-GVO ebenfalls zu bewältigen.

Anerkannte Schutzgarantien nach Art. 46 Abs. 2 lit. a bis f DS-GVO sind insbesondere ein Angemessenheitsbeschluss der EU-Kommission für bestimmte Drittstaaten (Art. 45 DS-GVO),[12] Standard-Datenschutzklauseln der EU-Kommission (Art. 46 Abs. 2 lit. c DS-GVO),[13] verbindliche interne Datenschutzvorschriften für konzerninterne Datenübermittlung (Binding Corporate Rules [BCR]) gem. Art. 47 DS-GVO (Art. 46 Abs. 2 lit. b DS-GVO),[14] von einer Aufsichtsbehörde angenommene Standard-Datenschutzklauseln, die von der Kommission genehmigt wurden, genehmigte Verhaltensregeln von Branchenverbänden gemäß Art. 40 DS-GVO (Art. 46 Abs. 2 lit. e DS-GVO) oder ein genehmigter Zertifizierungsmechanismus gemäß Art. 42 DS-GVO (Art. 46 Abs. 2 lit. f DS-GVO).

V. Unzulässige Übermittlung oder Offenlegung

Die Art. 44 ff. DS-GVO zeigen die Optionen auf, nach denen die Übermittlung personenbezogener Daten durch einen Verantwortlichen oder Auftragsverarbeiter in Drittländer zulässig ist. Darüber hinaus können sich der Verantwortliche und der Auftragsverarbeiter mit Art. 48 DS-GVO konfrontiert sehen. Art. 48 DS-GVO erfährt in der Praxis bislang recht wenig Aufmerksamkeit. Wenn er in Erscheinung tritt, dann wird er bisweilen mit vergleichbaren Regelungen in den Drittländern in Verbindung gebracht. Daher sollte ein Blick auf diese Norm geworfen werden. Zumal der Verstoß gegen die Vorschrift gem. Art. 83 Abs. 5 lit. c DS-GVO mit einem Bußgeld von bis zu 20 Mio Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes verhängt werden kann, je nachdem welcher der Beträge höher ist.

1. Die Regelung

Der Verordnungsgeber hat mit Art. 48 DS-GVO für die Fälle eine Regelung getroffen, in denen in Drittländern ansässige Gerichte oder Verwaltungsbehörden die Übermittlung bzw. Offenlegung durch in der EU ansässige Stellen verlangen können.[15] Art. 48 DS-GVO stellt eine besondere Form des grundsätzlichen Verbots der Datenübermittlung ohne entsprechende Rechtfertigung dar und ist eine gesetzgeberische Reaktion auf die Vorbehalte gegenüber den Aktivitäten außereuropäischer Dienste, deren Folge die ungehinderte Exposition von personenbezogenen Daten europäischer Bürger gegenüber Drittstaaten zur Folge hatte.[16] Die Übermittlung und die Offenlegung sind von dem Verarbeitungsbegriff nach Art. 4 Nr. 2 DS-GVO umfasst.[17] Die Regelung beinhaltet einen speziellen Erlaubnistatbestand der Verarbeitung für den Fall des Vorliegens einer in Kraft befindlichen internationalen Übereinkunft, die eine Datenübermittlung auf Basis gerichtlicher oder behördlicher Entscheidung im Drittland abdeckt.[18] Normadressaten des Art. 48 DS-GVO sind sowohl Verantwortliche als auch Auftragsverarbeiter. Diesen ist eine Preisgabe der gewünschten personenbezogenen Daten nunmehr explizit nur gestattet, wenn die Voraussetzungen nach Art. 48 DS-GVO oder einem anderen in Art. 44 ff. DS-GVO beschriebenen Tatbestand vorliegen.[19]

2. Die Herausforderung

Diese Regelung kann ein Unternehmen gegenüber dem Nutzer der Cloud in Konflikte bringen. Im Eilfall stellt sich die Situation für das Unternehmen so dar, dass ein Unternehmen als Adressat des ausländischen Urteils oder einer Verwaltungsentscheidung in der Regel in kurzer Frist aufgefordert wird, dem Urteil oder der Verwaltungsentscheidung Folge zu leisten. Also muss das Unternehmen binnen oft sehr kurzer Frist prüfen und entscheiden, ob das Herausgabeverlangen auf eine Art. 48 DS-GVO entsprechende Grundlage gestützt werden kann.

Art. 48 DS-GVO bezieht sich auf das Übermitteln und Offenlegen von personenbezogenen Daten im Zusammenhang mit gerichtlichen oder behördlichen Anordnungen aus Drittländern. Voraussetzung für eine Übermittlung nach Art. 48 DS-GVO ist eine Internationale Übereinkunft, z.B. ein Rechtshilfeabkommen zwischen ersuchendem Drittland und der Union oder einem Mitgliedstaat.

11 S. Erwägungsgrund 104 zur DS-GVO.

12 Zur aktuellen Lage s. EuGH-Urteil vom 16.07.2020, Rechtssache C-311/18 https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf; vor dem 16.07.2020 EDSA WP 254 rev.01.

13 Siehe dazu EDSA-Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies unter https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_nl.

14 EDSA-Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies unter https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_nl; EDSA WP 264; EDSA WP 265; EDSA WP 256 rev. 01; EDSA WP 257 rev. 01; sowie Register of approved binding corporate rules https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_de.

15 Vgl. Gola/Klug, DS-GVO Art. 48 Rn. 1; Klein, HK-DS-GVO/BDSG, Art. 48, Rn. 2 f.

16 Vgl. Albrecht/Jotzo, Das neue Datenschutzrecht der EU, S. 111; Klein, HK-DS-GVO/BDSG Art. 48 Rn. 1.

17 Vgl. Gola/Klug, DS-GVO Art. 48 Rn. 3.

18 Vgl. Gola/Klug, DS-GVO Art. 48 Rn. 2.

19 Vgl. Gola/Klug, DS-GVO Art. 48 Rn. 1.

Allerdings stellt sich der Weg über bestehende Rechtshilfeabkommen gerade bei eiligen Ermittlungen, z.B. im Kontext mit Cyberkriminalität, häufig als langsam, aufwändig und deshalb im Ergebnis nicht zielführend dar. Deswegen ermöglichen es die einschlägigen Gesetze in verschiedenen Ländern, dass Ermittlungsbehörden von einem Anbieter die Offenlegung ermittlungsrelevanter Daten unabhängig von einem Rechtshilfeabkommen auch dann verlangen können, wenn die Daten in einem anderen Land gespeichert sind.[20] Aber genügen diese Abkommen den Anforderungen des europäischen Datenschutzrechts, den Anforderungen nach Art. 48 DS-GVO?

In einem solchen Fall sollte es dem betroffenen Unternehmen möglich sein, einen Interessenausgleich zwischen europäischem und dem einschlägigen Recht des jeweiligen Drittlands herzustellen. Ein einseitiger und absoluter Vorrang des europäischen Datenschutzrechts, der in einem solchen Fall jegliche Abwägung von vorneherein ausschließen und per se zu einer Verletzung des ausländischen Rechts führen würde, schlösse international agierende CSP de facto vom europäischen Markt aus.

3. Die Konkordanz

Eine Konkordanz der widerstreitenden gesetzlichen Anforderungen kann u.a. auf verschiedene rechtliche Aspekte gestützt werden.

Art. 48 DS-GVO, der sich speziell auf Rechtshilfeabkommen bezieht, hat keine Sperrwirkung gegenüber den anderen Tatbeständen des Art. 44 ff. DS-GVO, die eine Übermittlung personenbezogener Daten in Länder außerhalb des EEA rechtfertigen können. Diese Rechtfertigungstatbestände können somit auch im Zusammenhang mit Behördenanfragen zur Anwendung kommen. Dementsprechend kann die Datenübermittlung z.B. auch auf Grundlage der von der EU-Kommission erlassenen EU-Standardvertragsklauseln erfolgen, vgl. Art. 46 Abs. 2 lit. c, Abs. 5 DS-GVO.[21]

Im Übrigen ergibt sich auch unmittelbar aus den EU-Standardvertragsklauseln die Möglichkeit eines Offenlegungsverlangen einer Verarbeitung – auch außerhalb der EU. Denn die Standardvertragsklauseln[22] enthalten in Klausel 5 d) eine explizite Regelung für den Zugriff von Sicherheitsbehörden, worunter gerade auch Sicherheitsbehörden im Land des Datenimporteurs (z.B. USA) fallen können.

Bei der Gesamtbewertung sollte auch berücksichtigt werden, wie der CSP auf etwaige Herausgabeverlangen reagiert. Eine Konkordanz zwischen den rechtlichen Verpflichtungen der DS-GVO einerseits und ausländischen Sicherheitsgesetzen andererseits kann z.B. dadurch gefördert werden, dass der Anbieter das Datenoffenlegungsverlangen einer Prüfung unterzieht, weitgehenden Anordnungen im Rahmen des Zumutbaren widerspricht und den Cloud-Nutzer – im Rahmen des gesetzlich Zulässigen – über das Datenoffenlegungsverlangen informiert. Letzteres ermöglicht dem Cloud-Nutzer, frühzeitig etwaige eigene rechtliche Abwehrmöglichkeiten bzw. Einschränkung des Offenlegungsverlangens zu prüfen (z.B. eine sog. „Protective Order").

Selbst wenn im Einzelfall ein Offenlegungsverlangen einer ausländischen Sicherheitsbehörde im Lichte des Art. 48 DS-GVO problematisch werden könnte, ist dies im konkreten Einzelfall primär das Risiko des betroffenen CSPs. Vor der Schrems II Entscheidung des EuGHs v. 16.7.2020[23] wäre indes nicht gerechtfertigt gewesen, die Zusammenarbeit zwischen einem in der EU ansässigen Cloud-Nutzer und dem CSP aufgrund dieses abstrakten Risikos von vorneherein als datenschutzwidrig anzusehen. Das EU/US-Privacy-Shield-Abkommen versprach den Schutz der personenbezogenen Daten im Drittland USA. Mit der Schrems II Entscheidung hat sich das gewandelt. Wie die Lage nun zu beurteilen ist und wie das in die Überlegungen einfließt, wird in den nächsten Monaten noch zu klären sein. Vorerst wird die Entscheidung breit diskutiert, der EDSA hat FAQ zu den am häufigsten gestellten Fragen herausgeben.[24]

Fehlt also ein Abkommen i.S.d. Art. 48 DS-GVO, ist im Falle des Falles zu prüfen, ob der Drittlandtransfer ggf. auch im Rahmen von anderen oben genannten Transfermöglichkeiten in Betracht kommen könnte.

VI. US-CLOUD Act im Zusammenhang mit Art. 48 DS-GVO?

Im Kontext von gerichtlichen bzw. behördlichen Datenoffenlegungsverlangen wird insbesondere der Clarifying Lawful Overseas Use of Data Act (CLOUD Act) und dessen (angebliche) Unvereinbarkeit mit der DS-GVO diskutiert.

1. CLOUD Act

Der US-Kongress hat den CLOUD Act am 23. August 2018 verabschiedet.[25] Hintergrund war ein Streit aus dem Jahr 2013 über ein Datenherausgabeverlangen von US-Strafverfolgungsbehörden auf bei Microsoft in Irland gespeicherten Daten bzw. E-Mails eines (vermeintlichen) US-Drogenhändlers. Microsoft hatte die Herausgabe der auf einen in Irland stehenden Server abgelehnt. Infolge dieses Rechtsstreits kam es zur Überarbeitung des bereits seit 1996 geltenden Rechtsrahmens für solche Datenherausgabeverlangen (dem „Stored Communications Act" – „SCA") und der CLOUD Act wurde als erläuterndes Gesetz („clarifying") zum SCA verab-

20 Zu den Herausforderungen der Strafverfolgungsbehörden durch Cloud Computing, Obenhaus, NJW 2010, 651 ff.

21 Art. 48 DS-GVO von „unbeschadet anderer Gründe für die Übermittlung gemäß dem Kapitel (V)".

22 Beschluss der Kommission vom 05.02.2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates (ABL. 2010, L39, S. 5) in der Fassung des Durchführungsbeschlusses (EU) 2016/2297 der Kommission vom 16.12.2016 (ABl. 2016, L334, S. 100) weitere Links z.B. unter https://www.gdd.de/links.

23 Https://edpb.europa.eu/our-work-tools/our-documents/other/statement-court-justice-european-union-judgment-case-c-31118-data_en.

24 Https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_en.

25 S. Spieß, ZD-Aktuell 2018, 04291; Cording/Götzinger, CR 2018, 636; Gausling, MMR 2018, 579, m.w.N.

schiedet.[26] Ein weiterer Grund für diese Entwicklung waren die seit längerem bestehenden Bedenken, dass die bisherigen Rechtshilfeverfahren zu schwerfällig wären, um den wachsenden Bedarf an dieser Art von elektronischen Beweisen mit verhältnismäßigem Zeitaufwand decken zu können.

Aufgrund der Unsicherheiten rund um den CLOUD Act hat das US-Justizministerium im April 2019 ein White Paper mit dem Titel "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act"[27] sowie FAQ dazu herausgegeben. Diese kann man den Verantwortlichen und Auftragsverarbeitern als wichtiges Medium an die Hand geben.

Alleine schon die Abkürzung CLOUD Act könnte den einen oder anderen dazu verleiten, dieses Gesetz als Cloud-spezifische Reglung zu verstehen, die nur für CLOUD-Dienstleister gelte. Dies wäre jedoch ein Irrtum. Der CLOUD Act ist auf alle Anbieter elektronischer Kommunikations- oder Remote-Computing-Services anwendbar, die in den USA aktiv sind, unabhängig davon, wo deren Sitz liegt. Dies umfasst zwar auch Cloud-Services, jedoch treffen die Vorgaben des CLOUD Acts vorrangig klassische Telekommunikationsanbieter wie z.B. Mobilfunk- und E-Mail Provider, denn der CLOUD Act modifiziert den Stored Communications Act (sozusagen das amerikanische Telekommunikationsgesetz) und bezieht sich auf Inhalte oder Metadaten von „electronic communication", soweit diese für die Ermittlungen im Zusammenhang mit einer Straftat (einschließlich Terrorismus) erforderlich sind. Der Originalwortlaut der § 2713 Chapter 121 USC lautet: "A provider of electronic communication service or remote computing service (...)".

Kommunikationsdaten wie bspw. Standorte bei Mobilfunkgesprächen und Bewegungsprofile sehen die US-Ermittlungsbehörden am ehesten als für die Aufklärung von Verbrechen relevante Informationen an. Die Fragestellungen rund um den CLOUD Act sind bezüglich einer Cloudnutzung daher die gleichen, denen man sich auch bei der Nutzung anderer elektronischer Kommunikationsdienste stellen muss. Im Wesentlichen ist vom Auftragsverarbeiter zu prüfen, mit wem man eine Geschäftsbeziehung eingeht und welche Informationen im Rahmen dieser Geschäftsbeziehung fließen. Dies beginnt schon bei „kleinen" bzw. kostenlosen Dienstleistungen wie bspw. der Nutzung von Messengerdiensten, die in ihren AGBs regeln, dass sie regelmäßig Zugriff auf gespeicherte Adressdaten fordern.

2. CLOUD Act und Art. 48 DS-GVO

Bemerkenswert ist im Rahmen der Diskussionen um den CLOUD Act[28] – und dies wird im Zuge vorhandener Unsicherheit mit der Materie häufig übersehen –, dass sich Art. 48 DS-GVO nicht auf US-Auskunftsverlangen beschränkt, sondern für alle Entscheidungen einer Verwaltungsbehörde eines Drittlandes gilt, das einschlägige Gesetze, Vorschriften und sonstige Rechte erlassen hat.[29]

Außerdem wird verkannt, dass Begehren nach dem CLOUD Act sich an Art. 48 DS-GVO messen lassen müssen. Er stellt die Anforderungen für eine Übermittlung aus der Sicht der USA, des Drittlandes, auf. Demgegenüber stellen Art. 44 ff. DS-GVO die europäischen Anforderungen an ein solches Begehren dagegen. Der CLOUD-Act ist sicherlich eine prominente Regelung, welche über die Medien in den letzten Jahren viel Aufmerksamkeit in der Öffentlichkeit erfahren hat – alleine maßgeblich ist er aber nicht.

Allein basierend auf den Aussagen des o.g. Whitepapers des US-Justizministeriums wird deutlich, dass die allgemein beschriebenen Mutmaßungen um den CLOUD-Act sich mit der tatsächlichen Zielsetzung des CLOUD-Acts nicht ausreichend auseinandersetzen. Wie dargestellt ist der CLOUD-Act auf die Beweiserlangung bei schweren Verbrechen anwendbar. Es sollte daher unter Einhaltung der DS-GVO gelingen, eine Vereinbarkeit zwischen beiden Interessenlagen, der US-amerikanischen und der europäischen, herzustellen.

Dass eine solche Regelung notwendig ist, zeigt allein schon die neue Qualität, welche die Verbrechen im digitalen Zeitalter erlangt haben. Die Bearbeitung von Rechtshilfeersuchen erfordern hohen Zeitaufwand und komplexe Prozesse.

Der CLOUD-Act darf im Zusammenhang mit der Cloud Nutzung daher nicht als unüberwindliches Hemmnis verstanden werden. Ein erster Schritt sollte die Transparenz über die Zielsetzung des CLOUD Acts sein und ein zweiter Gedanke der Frage folgen, unter welchen Umständen der CLOUD Act überhaupt zum Einsatz kommt.

VII. Welche Lösungsmöglichkeiten bestehen für den scheinbaren Konflikt? Welche Hilfestellung würde Entscheidern zugutekommen?

Die in diesem Beitrag herausgegriffenen Herausforderungen für den Verantwortlichen und den Auftragsverarbeiter i.S.d. Art. 28 DS-GVO sind durchaus lösbar. Aber es bedarf weiterer Aktivitäten, um zur Bewältigung der Herausforderungen Hilfe zu leisten.

Kurzfristig ist die eine klare Kommunikation zwischen den Unternehmen bzw. Behörden und den Datenschützern erforderlich. Mittelfristig wäre es wertvoll, ein Papier vergleichbar der Orientierungshilfe der DSK „Cloud Computing" (Version 2.0 (Stand 09.10.2014)[30]) zur Verfügung zu stellen. Langfristig sind sicherlich die Gesetzgeber gefordert, ggf. die bestehenden gesetzlichen Rahmenbedingungen anzupassen und aufeinander abzustimmen. Aber dafür braucht es naturgemäß erst die Praxiserfahrungen mit den geltenden Vorschriften.

26 S. Cording/Götzinger, CR 2018, 636 ff.

27 S. unter https://www.justice.gov/opa/press-release/file/1153446/download.

28 Dazu Cording/Götzinger, CR 2018, 636 ff.; Rath/Spies, CCZ 2018, 229 ff.; Metz/Spittka, ZD 2017, 361 ff.; Pauly/Dieckhoff, CCZ 2017, 270 ff.

29 S. Gola/Klug, DS-GVO Art. 48, Rn. 1.

30 Orientierungshilfe Cloud Computing der Arbeitskreise „Technik und Medien" wurde von der 88. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zustimmend zur Kenntnis genommen (Stand: 09.10.2014), https://www.datenschutzkonferenz-online.de/media/oh/20141009_oh_cloud_computing.pdf; zur Entstehung der OH, Richter, ZD 2020, 84, 86.

VIII. Conclusio

Eine sich im Umbruch befindliche Informationsgesellschaft, die sich auch noch ganz neuen Herausforderungen wie bspw. aktuell einer Pandemie zu stellen hat, kann es sich nicht leisten, per se eine Möglichkeit zur Weiterentwicklung auszuschließen.

Die in diesem Zusammenhang auftretenden Fragen sind umfassend und müssen – unabhängig von Cloud-Computing – auf dem Weg zu einer mündigen und digitalen Gesellschaft diskutiert werden. Nur ein informierter Bürger kann eine bewusste und gut informierte Entscheidung treffen und damit die Digitalisierung sinnvoll und zielführend begleiten.

Dies wäre dann sicherlich auch im Sinne der „Begründer Europas", die schon 1993 das Thema erkannt und sich in Abhandlungen wie z.B. „Europas Weg in die Informationsgesellschaft" oder sich im „Weißbuch über Wachstum, Wettbewerbsfähigkeit und Beschäftigung" näher damit beschäftigt haben.

Maria Christina Rost
ist Leiterin des Justiziariat beim HBDI und die persönliche Referentin des Hessischen Datenschutzbeauftragten. Vor ihrer Tätigkeit beim HBDI war sie in der Kanzlei des Hessischen Landtags, im Ministerium für Schule und Weiterbildung des Landes NRW und als Rechtsanwältin tätig.

Dr. Stefan Brink
ist seit 2017 der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg.

Tobias Birk
ist Dipl. Wirtschaftsinformatiker (BA) und bereits lange Jahre als Dozent, Prüfer und Mentor an der Dualen Hochschule Baden-Württemberg (DHBW) aktiv. Hauptberuflich ist er heute als Geschäftsfeldleiter für Security Solutions bei der PROFI Engineering Systems AG tätig. Er verfügt über 20 Jahre Erfahrung im Bereich der IT- und Informationssicherheit.

Dr. Sebastian Bretthauer

Die datenschutzbehördliche Informierung als neuartiges Instrument der Aufsichtsbehörden nach Art. 58 Abs. 2 DS-GVO

Art. 58 DS-GVO normiert die aufsichtsbehördlichen Befugnisse umfassend. Gleichwohl können die Mitgliedstaaten weitere zusätzliche Rechtsvorschriften erlassen, die über das datenschutzrechtliche Instrumentarium der DS-GVO hinausgehen. Mit der datenschutzbehördlichen Informierung wenden Teile der Aufsichtsbehörden schon länger eine Maßnahme an, die so nicht ausdrücklich von Art. 58 DS-GVO erfasst und bisher auch nicht im deutschen Recht verankert ist. Der Beitrag untersucht daher das Phänomen der datenschutzbehördlichen Informierung näher.

I. Einleitung

Mit Einführung der Europäischen Datenschutzgrundverordnung (DS-GVO) wurden die Befugnisse der nationalen Datenschutzbehörden erheblich erweitert. Zentrale Regelung ist nunmehr Art. 58 DS-GVO, der gegenüber seiner Vorgängerregel in Art. 28 Abs. 3 DSRL die Untersuchungs-, Abhilfe- und Genehmigungsbefugnisse umfangreicher und wesentlich detaillierter ausgestaltet.[1] Dabei sieht die Regelung ein zweistufiges sowie abgestuftes „Eskalationsverfahren" vor.[2]

Auf der ersten Stufe – diese betrifft die Ermittlungsphase – werden den Aufsichtsbehörden verschiedene Untersuchungsbefugnisse eingeräumt (Art. 58 Abs. 1 DS-GVO). Hier wird zunächst umfangreich geprüft, ob überhaupt ein Verstoß gegen die DS-GVO vorliegt. Dabei können die Datenverarbeiter etwa angewiesen werden, bestimmte Informationen bereitzustellen (Art. 58 Abs. 1 lit. a DS-GVO) oder aber auch Zugang zu ihnen zu gewähren (Art. 58 Abs. 1 lit. e DS-GVO).[3]

Wurde sodann ein datenschutzrechtlicher Verstoß tatsächlich festgestellt, so stehen auf der zweiten Stufe – diese

1 Polenz, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 58 Rn. 1.

2 Ebenso Dieterich, ZD 2016, 260 (263); Nguyen, in: Gola (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 58 Rn. 17.

3 Siehe dazu Polenz, in: Simitis/Hornung/Spiecker gen. Döhmann (Hrsg.), Datenschutzrecht, 2019, Art. 58 Rn. 9 ff.; Wenzel/Wybitul, ZD 2019, 290 (292).