DATENSCHUTZKONFORMER EINSATZ VON US-SERVICES

Natascha Windholz

VIG Group Data Protection Coordinator, Vienna Insurance Group AG Wiener Versicherung Gruppe, Group Compliance
Schottenring 30, 1010 Wien, AT
natascha.windholz@vig.com, www.vig.com

Schlagworte: ***Datenschutz, DSGVO, CLOUD-Act, Privacy Shield, Standarddatenschutzklauseln, e-Evidence-Verordnung***

Abstract: *Privacy Shield und Standarddatenschutzklauseln scheinen legitime Mittel zur Datenübertragung in die USA zu sein. Doch ist dem tatsächlich so? Die Aufdeckungen durch Whistleblower Snowden haben die Praktiken der USA zu Massenabfragen deutlich gemacht. Der CLOUD-Act erlaubt Zugriffe auf Daten, die US-Unternehmen verarbeiten – unabhängig vom Speicherort. Der neueste geplante Streich der EU, die e-Evidence-Verordnung ist ein Versuch, Datenübermittlungen an US-Behörden und US-Gerichte zu legalisieren. Der Preis dafür wäre jedoch hoch. Diese Analyse befasst sich mit Wegen und Irrwegen der Datenübermittlung in die USA.*

1. Ausgangslage für Unternehmen

Ein europäisches Unternehmen möchte einen US-Dienstleister einsetzen. Die DSGVO[1] ist gem. Art. 3 DSGVO voll anwendbar. Das Unternehmen wird wohl in der Regel Verantwortlicher gem. Art. 4 Z. 7 DSGVO sein. Allenfalls treffen auf das Unternehmen auch noch nationale Gesetze zu, die einzuhalten sind. Das Bankwesengesetz[2] sieht etwa in § 25 BWG vor, dass bei der Heranziehung eines Dienstleisters aus einem Drittland besondere Sorgfalt zu gelten hat. § 109 VAG[3] legt Vorgaben hinsichtlich der Auslagerung bestimmter Dienste fest.

Oft besteht der Eindruck, dass es keine (brauchbaren) Alternativen gibt, dass ein Unternehmen keine andere Wahl hat, als einen US-Dienstleister einzusetzen. Der Wille, das Geld oder das Wissen fehlen, um selbst zu programmieren oder einen anderen Dienstleister zu suchen. Gern wird auch behauptet, dass die Kunden, die Mitarbeiter, etc. diese Dienste wünschen oder gar brauchen – «sie wollen das so». Gerade kleinere Unternehmen argumentieren, dass ein DSGVO-Verstoß weniger teuer kommt als die volle Compliance mit derselben.

Der Wunsch zur Nutzung von Diensten aus Silicone Valley ist groß. Die Reichweite von Facebook und Co ist enorm.

Auf der anderen Seite stehen diverse Skandale und Skandälchen rund um US-Dienste: Zufällig gibt Twitter die Telefonnummern zur Zwei-Faktor-Authentifizierung zur Werbung für Drittanbieter frei[4]. Sprachaufzeichnungen von Alexa werden im Home Office von Mitarbeitern ausgewertet[5]. Office 365 birgt das Risiko

---

1 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), 1. Abl., L 2016/119.

2 Bundesgesetz über das Bankwesen (Bankwesengesetz – BWG) BGBl. I Nr. 532/1993 i.d.F. BGBl. I Nr. 46/2019.

3 Bundesgesetz über den Betrieb und die Beaufsichtigung der Vertragsversicherung (Versicherungsaufsichtsgesetz 2016 – VAG 2016) BGBl I Nr. 34/2015 i.d.F. BGBl. I Nr. 62/2019.

4 https://www.derstandard.at/story/2000109667139/twitter-nutzte-fuer-sicherheitszwecke-vorgesehene-nutzer-telefonnummern-fuer-werbung (zuletzt abgerufen am 26.10.2019).

5 https://www.heise.de/newsticker/meldung/Bericht-Amazon-laesst-Alexa-Mitschnitte-im-Homeoffice-auswerten-4487911.html (zuletzt abgerufen am 26.10.2019).

unrechtmäßiger Datenübermittlungen, u. a. wegen der Intransparenz der Übermittlung von Diagnosedaten[6]. Gesundheitsdaten, die Google im Zuge eines Cloud-Dienstes bekommt, werden vom Suchdienst-Betreiber auch gleich mittels Künstlicher Intelligenz analysiert bzw. diese mit den Gesundheitsdaten trainiert, ohne dass Patienten darüber informiert werden[7]. Die Liste ließe sich wohl endlos fortsetzen.

Doch selbst wenn es diese Skandale und Probleme nicht gäbe – oder diese auf ein erträgliches Maß reduziert würden – wäre dann der Einsatz von US-Services datenschutzrechtlich unbedenklich?

2. Rechtsgrundlagen für die Datenverarbeitung

Zunächst muss sich das Unternehmen überlegen, wozu es einen Service einsetzen möchte (Zweck der Datenverarbeitung) und warum es das darf (Rechtmäßigkeit). Arbeitnehmerdaten können für die Erfüllung des Arbeitsvertrages oder aufgrund von Gesetzen verarbeitet werden, eine Buchhaltung muss ebenfalls nach den gesetzlichen Vorgaben geführt werden, für einen Newsletter wird in der Regel eine Einwilligung notwendig sein, Verarbeitungen aus Datensicherheitsgründen werden wahrscheinlich mit berechtigtem Interesse argumentierbar sein, usw. Art. 6, Art. 9 und Art. 10 DSGVO zählen die Rechtsgrundlagen auf. Bevor die Frage nach dem «Wo» oder «Wodurch» gestellt werden kann, müssen erst die Fragen nach dem «Was» und «Warum» geklärt werden.

3. Rechtsgrundlagen für die Datenübermittlung

In einem Zwischenschritt ist zu prüfen, ob es sich bei dem US-Service um einen Auftragsverarbeiter handelt, also jemanden der für das verantwortliche Unternehmen eine Datenverarbeitung durchführt, oder um gemeinsame Verantwortliche, die gemeinsam Mittel und Zweck festlegen. Der Begriff des Verantwortlichen wird vom EuGH[8] weit interpretiert. Je nach dem Ergebnis dieser Prüfung, ist ein Auftragsverarbeitervertrag gem. Art. 28 DSGVO oder ein Vertrag über die gemeinsame Verantwortlichkeit gem. Art. 26 DSGVO abzuschließen. Nach der Beantwortung dieser Vorfrage ist zu prüfen, gem. welcher Rechtsgrundlage nach Art. 46 ff DSGVO die Daten in die USA übermittelt werden dürfen. Verlassen Daten nämlich EU bzw. EWR, sind entsprechende Garantien zu erbringen, wonach – kurz gesagt – sichergestellt werden muss, dass die Daten genauso sicher sind wie in der EU.

Für Datenübermittlungen in die USA sind die zwei wichtigsten Möglichkeiten: Privacy Shield und Standardvertragsklauseln. In weiteren Schritten wird geprüft, inwiefern der CLOUD-Act und die geplante e-Evidence-Verordnung eine Rolle spielen.

3.1. Privacy Shield

Das Privacy Shield ist ein Unterfall des Angemessenheitsbeschlusses. Ein Angemessenheitsbeschluss besagt, dass das Datenschutzniveau im betreffenden Nicht-EU-Staat genauso hoch ist wie innerhalb von EU/EWR. Für die gesamte USA gibt es einen solchen Beschluss nicht, aber Unternehmen können sich selbst gemäß Privacy Shield zertifizieren und so von sich selbst behaupten, dass die Daten bei ihnen genauso sicher sind wie innerhalb der EU. Im Wesentlichen handelt es sich beim Privacy Shield um ein Abkommen zwischen EU-Kommission und US-Handelsministerium. Für Beschwerden von EU-Bürgern ist die Federal Trade Commission zuständig.

---

6 https://www.datenschutzbeauftragter-info.de/datenschutz-office-365-dsgvo-konformer-einsatz-im-unternehmen/ (zuletzt abgerufen am 26.10.2019).

7 https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790?shareToken=st51c1d21de7a944baba1d9e70f15e908f (zuletzt abgerufen am 15.12.2019).

8 EuGH 05.06.2018, C-210/16.

Die EU-Kommission[9] bestätigte erst im Oktober 2019 den ungehinderten Datentransfer in die USA und die Aufrechterhaltung des Privacy Shield. Der Europäische Datenschutzausschuss[10] sieht das Privacy Shield jedoch nach wie vor kritisch. Die amtswegigen Kontrollmaßnahmen durch das amerikanische Department of Commerce und die Federal Trade Commission sind zwar erhöht worden, der Fokus bei diesen Kontrollen liegt jedoch bei formalen oder prozeduralen Aspekten und nicht bei substantiellen Themen. Offen ist außerdem noch die Frage des Zugriffs der USA auf Daten für Sicherheitszwecke. Der Europäische Datenschutzausschuss spricht auch die Überwachungsmaßnahmen durch US-Behörden kritisch an und bemängelt fehlende Reports dazu, mithilfe derer er feststellen könnte, ob willkürlich Daten gesammelt werden. Auch die Frage des Verhältnisses vom Privacy Shield zum CLOUD-Act wird angesprochen, doch selbst das Department of Commerce hat sich mit dieser Frage noch nicht befasst.

3.2. Standarddatenschutzklauseln

Dabei handelt es sich um eine Garantie gem. Art 46 DSGVO. Noch wurden keine «neuen» Standarddatenschutzklauseln erlassen. Es gibt nur die Standardvertragsklausen gem. Datenschutz-Richtlinie, welche von der EU-Kommission erlassen wurden. Diese «Vertragsvorlage» ist zwischen dem EU- und dem US-Unternehmen abzuschließen. Der Vertrag enthält eine Reihe von Schutzrechten zugunsten Dritter, namentlich der Betroffenen. Viele Rechte können direkt vom Betroffenen gegenüber dem US-Anbieter geltend gemacht werden. Neue Standarddatenschutzklauseln gem. DSGVO wurden von der EU-Kommission bis dato nicht erlassen. Die dänische Aufsichtsbehörde hat jedoch eigene Standarddatenschutzklauseln erlassen, dabei handelt es sich jedoch um keine Standarddatenschutzklauseln, mithilfe derer Daten außerhalb von EU/EWR verarbeitet werden dürften[11].

3.3. Wegfall der Rechtsgrundlagen?

Beides – Privacy Shield und Standarddatenschutzklauseln – liegen beim EuGH und könnten zeitnah gekippt werden. Seit Whistleblower Edward Snowden ist bekannt, dass die USA Massenüberwachung betreiben, EU-Bürger eingeschlossen. Da weder Privacy Shield[12] noch die Standardvertragsklauseln[13] das verhindern und EU-Bürger damit keinerlei Recht auf Datenschutz bzw. Geheimhaltung in den USA genießen, finden sich beide Instrumente vor dem EuGH.

Es besteht daher einerseits das Risiko, dass die beiden wichtigsten Rechtsgrundlagen für die Datenübermittlung in die USA mehr oder weniger gleichzeitig unrechtmäßig werden könnten und damit die Rechtsgrundlage für die Datenübermittlung weg fallen könnte. Andererseits besteht immer das Risiko, dass Daten unrechtmäßig vom US-Unternehmen an US-Behörden oder US-Gerichte übertragen werden könnten.

Gem. Art. 48 DSGVO dürfen Daten – kurz gesagt – nur dann aufgrund eines Urteils eines Drittlands bzw. einer Entscheidung einer Verwaltungsbehörde offengelegt werden, wenn es auch eine entsprechende internationale Übereinkunft gibt. Damit soll verhindert werden, dass es zu Datenübermittlungen aufgrund von ausländischem Recht kommt. Sollte es sogar so weit kommen, dass es einen US-Beschluss zur Herausgabe von Daten gäbe, so wäre dieser in der EU in der Regel nicht durchsetzbar. Erst müsste geprüft werden, ob es ein Rechtshilfeabkommen mit dem betreffenden Staat gibt. Mit Österreich gibt es kein solches Abkommen.

9 https://netzpolitik.org/2019/eu-kommission-erneutert-persilschein-fuer-datenaustausch-mit-den-usa/ (zuletzt abgerufen am 27.10.2019).
10 Europäischer Datenschutzausschuss, EU – US-Privacy Shield – Third Annual Joint Review 2019, adopted on 12 November 2019.
11 https://edpb.europa.eu/news/news/2019/first-standard-contractual-clauses-contracts-between-controllers-and-processors-art_de (zuletzt abgerufen am 15.12.2019).
12 EuGH, T-738/16 (noch keine Entscheidung).
13 EuGH, C-311/18 (noch keine Entscheidung).

3.4. Keine Rechtsgrundlage: CLOUD-Act

Zur Vorgeschichte: Microsoft weigerte sich, Daten, die nicht in den USA gespeichert waren, heraus zu geben. Die Rechtssache ging sogar bis zum Supreme Court. Zu einer Entscheidung kam es allerdings nicht, da zwischenzeitlich der CLOUD-Act erlassen worden war.

CLOUD-Act steht für «Clarifying Lawful Overseas Use of Data Act». Der CLOUD-Act zwingt US-Unternehmen Daten ans US-Behörden oder US-Gerichte auszuhändigen, egal wo diese Daten gespeichert wird. Anwendbar ist der CLOUD-Act bei schweren Verbrechen inkl. Terrorismus. Eine Definition, um welche Verbrechen es sich genau handelt, fehlt im CLOUD-Act. Grundsätzlich gibt es keine Einschränkung, dass nur Daten von US-Bürgern oder in den USA wohnhaften Personen abgefragt werden dürfen.

Den US-Unternehmen steht ein Widerspruchsrecht[14] zu, wenn es sich um Daten von Nicht-US-Bürgern handelt bzw. Personen die nicht in den USA leben. Für diejenigen Unternehmen, die in einem Staat ansässig sind, der dem CLOUD-Act beigetreten ist, besteht ein weiteres Widerspruchsrecht, nämlich wenn die Herausgabe gegen das Recht des partizipierenden Staates verstoßen würde. Es besteht daher die Möglichkeit, dass ein Staat dem CLOUD-Act quasi beitreten kann[15].

Betont sei an dieser Stelle nochmals, dass es sich lediglich um ein Widerspruchsrecht des Unternehmens handelt. Es handelt sich um kein Verbot der USA, Daten von Nicht-US-Bürgern zu verarbeiten. Das Unternehmen muss die ansuchende US-Behörde darauf hinweisen, dass es sich nicht um einen US-Bürger handelt, dessen Daten verlangt werden. Daten von EU-Bürgern könnten trotzdem übermittelt werden.

Deutlich wird das fehlende Verständnis von Datenschutz für EU-Bürger auch dadurch, dass ein beigetretener Staat keine US-Bürger «trageten» darf, weder direkt noch indirekt[16]. Ein solches Verbot gibt es für die USA nicht, wenn es um EU-Bürger oder andere Nicht-US-Bürger geht.

3.4.1. Exkurs: «Beitritt» UK zum CLOUD-Act

Großbritannien hat als erster Staat ein Abkommen mit dem USA zum CLOUD-Act abgeschlossen[17], wobei die Vereinbarung erst mit 31. März 2020 rechtskräftig wird. Damit ist eine gegenseitige weitgehend unbeschränkte Abfrage bei Unternehmen möglich. Im Abkommen[18] sind jedoch die Straftaten definiert, aufgrund derer bei Unternehmen angefragt werden können. Konkret handelt es sich um Verbrechen mit einer Höchststrafe von mindestens 3-jähriger Freiheitsstrafe. Es ist nicht vorgesehen, dass es ein ähnliches Verbrechen im jeweils anderen Staat geben muss. Es dürfen nur User bzw. Konten abgefragt werden, Gesamtabfragen sind nicht möglich. Die Ermittlungsbehörden müssen also schon zumindest einen indirekten Personenbezug haben, z.B. eine IP-Adresse oder IMEI. Unternehmen wird nicht verboten, Daten zu sammeln, die sie nach der Gesetzgebung des eigenen Staates nicht bräuchten. Einige Einschränkungen gibt es außerdem. UK darf keine US-Bürger oder US-Einwohner als Ziel von Ermittlungen haben, die USA dürfen jedoch gegen UK-Bürger ermitteln, wenn diese nicht in UK wohnhaft sind. Beide Staaten müssen jeweils ein Verfahren vorsehen, welche Konten abgefragt werden dürfen. Der CLOUD-Act ist nicht die einzige Möglichkeit für Datenabfragen, internationale Rechtshilfeersuchen bleiben aufrecht. Gemäß der Vereinbarung muss ein Ersuchen zunächst der zuständigen Behörde des jeweils anderen Staates übermittelt werden. Dieser bestätigt die Rechtmäßigkeit des Ersuchens und übermittelt es dem Unternehmen. Sollte ein Staat begründet annehmen, dass die abzufragende Person in einem Drittstaat ist, müssen die zuständigen Behörden des Drittstaats informiert werden. Von

14 Vgl. CLOUD-Act Section 3 § 2713 (h) (2) Motions to Quash and Modify.
15 Vlg. CLOUD-Act Section 5 § 2523 (b) (2) und (3).
16 Vgl. CLOUD-Act Section 5 § 2523.
17 https://www.golem.de/news/cloud-act-usa-und-grossbritannien-vereinbaren-austausch-von-serverdaten-1910-144286.html (zuletzt abgefragt am 26.10.2019).
18 USA No. 6 (2019) Agreement between the Government of the United Kondom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, 3 October 2019.

dieser Vorgabe ausgenommen sind jedoch Umstände, wonach die nationale Sicherheit, Menschenrechte oder die Information den Ermittlungen zuwider laufen würde. Sollte ein Unternehmen der begründeten Meinung sein, dass die Vereinbarung im Hinblick auf das konkrete Ersuchen nicht ordentlich umgesetzt wurde, kann es einen Widerspruch bei der zuständigen Behörde erheben. UK ist dazu verpflichtet Minimierungsmaßnahmen hinsichtlich der empfangenen Daten zu treffen und darauf achten, dass Daten, die in die USA übermittelt werden, ebenfalls minimiert werden. Für letztere Pflicht sind jedoch wieder Ausnahmen vorgesehen, etwa wenn es um die nationale Sicherheit der USA geht. In Drittländer dürfen Daten generell nicht übermittelt werden, außer es liegt eine Einwilligung der Partei vor, von der die Daten empfangen wurden. Die USA holt sich die Genehmigung von UK ein, wenn Daten in Fällen verwendet werden, wo die Todesstrafe vorgesehen wäre. UK muss sich dagegen die Genehmigung der USA holen, wenn um Fälle der Redefreiheit geht. Jedes Jahr wird die Vereinbarung und deren Einhaltung überprüft. In einem jährlichen Bericht werden aggregierte Daten über die Verwendung der Vereinbarung ausgetauscht.[19]

Interessant am Übereinkommen mit UK ist, dass sich die USA selbst begrenzt. Der CLOUD-Act in seiner einseitigen Form sieht etwa keine klaren Beschränkungen auf bestimmte Verbrechen vor, während die bilaterale Variante diese gegenüber UK sehr wohl vorsieht. Die Frage ist, wann die USA je die bilaterale Variante zur Anwendung bringt, da diese mit mehr Aufwand und Beschränkungen verbunden wäre, haben sie doch die einseitige Variante. Zu denken wäre nur an UK-Unternehmen, die keinerlei Bezug zu den USA haben. Aber selbst hier ist aufgrund der großen Verbreitung von US-Diensten die Frage, ob die USA nicht auf anderem Weg zu den gewünschten Daten kommen kann.

3.5. Mögliche Rechtsgrundlage: E-Evidence-Verordnung

Der CLOUD-Act zeigt deutlich die (sicherheits-)politischen Begehrlichkeiten von Staaten an Daten, die bei Unternehmen liegen. Die EU plant daher im Wesentlichen genau dasselbe. Die geplante e-Evidence-Verordnung[20] könnte ein Abkommen gem. Art. 48 DSGVO sein. Auf Ansuchen eines Staates können Verkehrs- und Inhaltsdaten von einem anderen Staat zu Zwecken der Strafverfolgung verlangt werden – und zwar ohne Umwege über die nationalen Behörden des Staates, in dem angefragt wird, wie es derzeit notwendig wäre. Die direkte Anfrage beim ausländischen Unternehmen soll das Verfahren abkürzen und Daten schneller den Strafverfolgungsbehörden bzw. Gerichten zur Verfügung stehen.

Das Recht des Herkunftslandes soll anwendbar sein. Für Betroffene gibt es kaum Schutz. Dazu kommt, was in einem Land strafbar ist, muss es in einem anderen Land nicht sein (Stichwort Abtreibung). Das Strafrecht ist in der EU nämlich nicht vollständig harmonisiert. Auch die Grundrechte können sich mitunter innerhalb der EU unterscheiden, was eine Beschneidung dieser bedeuten könnte. Die Datenabfrage soll außerdem geheim bleiben. Unternehmen, die sich weigern, Daten herauszugeben, drohen hohe Geldbußen bis zu 2% des weltweiten Jahresumsatzes. Verhandlungen mit den USA über ein ähnliches Abkommen über digitale Beweise haben bereits begonnen.

Gemäß dem Entwurf bestehen zwei Möglichkeiten: Einerseits ist eine Europäische Herausgabeanordnung vorgesehen. Damit können mittels richterlichem Beschluss europaweit insb. digitale Daten bei Unternehmen angefordert werden. Andererseits soll es die Europäische Sicherheitsanordnung geben, mithilfe der die Datensicherung erfolgen soll. Das angefragte Unternehmen müsste innerhalb von 10 Tagen reagieren oder in dringenden Fällen auch schon in sechs Stunden. Für die Herausgabe von Teilnehmer- und Zugangsdaten gäbe es derzeit keine Beschränkungen – diese dürften also bei jeglichen Straftaten angefragt werden. Unter

[19] https://www.insideprivacy.com/surveillance-law-enforcement-access/10167/ (zuletzt abgerufen am 17.12.2019).

[20] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über eine Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:52018PC0225&from=EN (zuletzt abgerufen am 26.10.2019).

Teilnehmerdaten fallen jedoch auch die Standorte von Telefonmasten. Schon mithilfe dieser Daten könnte ein Bewegungsprofil des Betroffenen erstellt werden. Beschränkungen gibt es für Transaktions- und Inhaltsdaten. Eine Herausgabe dieser soll nur bei Straftaten mit mindestens 3-jähriger Haftstrafe im ansuchenden Staat möglich sein. Eine Anordnung darf nur erlassen werden, wenn eine ähnliche Maßnahme im Vollstreckungsstaat auch vorgesehen bzw. möglich wäre. Hier stellt sich die Frage, ob das Unternehmen, das der Anordnung Folge leisten soll, das prüfen soll? In Anbetracht der Geldstrafen, die bei Nichtbefolgung drohen und dem allfälligen Zeitdruck, wird das unwahrscheinlich sein. Der Betroffene wird erst im Nachhinein informiert, wenn keine Gefahr für die Ermittlung mehr besteht, bei einer Sicherungsanordnung erfolgt nicht einmal diese, da ja keine Daten weitergegeben wurden. Die Einbindung des Vollstreckungsstaates passiert erst bei einem Vollstreckungsantrag, dann sind auch Rechtsmittel möglich. Der Betroffene hat Rechtsmittel nur im Anordnungsstaat – dies erachtet der Entwurf als nicht unverhältnismäßig. Betroffenenrechte müssten in einem ersten Schritt vom Unternehmen wahrgenommen werden. Dieses wird jedoch in aller Regel kein Interesse daran haben, die Grundrechte des Betroffenen zu wahren, sondern wahrscheinlich im Zweifel die Angelegenheit möglichst schnell vom Tisch haben wollen. Was bis dato vollkommen im Entwurf fehlt, sind Vorgaben, wie mit Daten unbeteiligter Dritter vorzugehen ist.

Datenschutzrechtliche und grundrechtliche Aspekte sind noch nicht geklärt. Offen ist auch noch das Verhältnis zum CLOUD-Act, da Letzterer umfangreicher ist.

3.5.1. Kritische Stimmen

Für die Autorin stellt sich die Frage der staatlichen Souveränität. Ausländische Gerichtsbeschlüsse wären plötzlich durchsetzbar in Österreich. Dabei handelt es sich jedoch um eine völkerrechtliche Frage, die den Rahmen dieses Artikels sprengen würde.

Die deutsche Bundesregierung hat sich bereits Gedanken dazu gemacht. Die e-Evidence-Verordnung enthalte keine ausreichende Grundrechtsprüfung. Es gibt keine ausreichende Möglichkeit im Einzelfall ein Ersuchen zur Datenherausgabe zurückzuweisen. Es gibt zwar gewisse Schutzmaßnahmen für Geheimnisträger (z.B. Journalisten, Parlamentarier), diese sind aber nicht zufrieden stellend. Es gibt kein Vetorecht des Herausgabestaates.[21]

Auch der Europäische Datenschutzbeauftragte Wojciech Wiewiórowski kritisiert die e-Evidence-Verordnung[22]. Dieser fordert etwa ein Vetorecht des Staates, in dem angefragt wird. Grundsätzlich unterstützt der Europäische Datenschutzbeauftragte das Ziel effektiver Mittel für Strafverfolgungsbehörden zur Ermittlung und Verfolgung von Straftaten und die geplante Vereinfachung bei grenzüberschreitenden Fällen innerhalb der EU. Er verlangt jedoch, dass die Grundrechte und die datenschutzrechtlichen Vorgaben eingehalten werden.

3.6. Zwischenresümee

Als US-Unternehmen hat man derzeit die Wahl zwischen Pest oder Cholera. Man kann sich «aussuchen», ob man gegen den CLOUD-Act verstößt, sich mit dem Widerspruchsrecht herumschlägt oder gegen die DSGVO verstößt.

Als EU-Unternehmen hängt über einem – sobald man US-Services einsetzt – das Damoklesschwert einer Datenschutzverletzung. Ständig kann es zu einer unrechtmäßigen Datenübermittlung an US-Behörden oder US-Gerichte kommen. Unrechtmäßige Datenübermittlungen sind gem. DSGVO sanktioniert. Eine hohe Strafe, berechnet vom weltweiten Konzernumsatz, kann drohen.

---

[21] https://www.heise.de/ct/artikel/Geplante-EU-Verordnung-gefaehrdet-die-Grundrechte-der-Buerger-4471900.html (zuletzt abgerufen am 26.10.2019).

[22] Europäischer Datenschutzbeauftragter, Opinion 7/2019, EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronical Evidence in criminal Matters, 6 November 2019.

Privacy Shield und Standarddatenschutzklauseln mögen zwar formell eine Datenübermittlung in die USA rechtfertigen, aber aufgrund der anhängigen Verfahren bald nicht mehr bereit stehen.

4. Datensicherheitsmaßnahmen und Vertragsrecht als Ausweg?

Als EU-Unternehmen kann man versuchen, entsprechende vertragliche Vereinbarungen oder Datensicherheitsmaßnahmen zu treffen.

Über Datensicherheitsmaßnahmen könnte sichergestellt werden, dass das US-Unternehmen keinen Zugriff auf die EU-Daten hat oder diese zumindest nicht lesen kann. Letzteres könnte über Verschlüsselung oder Pseudonymisierung erreicht werden. Der Systemzugang könnte getrennt werden, sodass das US-Unternehmen zwar den Service bereitstellt, aber auf die Daten, die dadurch verarbeitet werden, nicht zugreifen kann. Bei der Pseudonymisierung wird der direkte Personenbezug durch einen indirekten ersetzt. Das US-Unternehmen sieht zwar die Daten, kann sie aber nicht direkt zuordnen. Diese Variante ist jedoch nur sinnvoll, wenn das US-Unternehmen den Schlüssel nicht hat. Als Datenspeicherort sollte die EU vereinbart werden.

Vertraglich könnte vereinbart werden, dass das US-Unternehmen eine Informationspflicht gegenüber dem EU-Unternehmen hat. Kommt es also zu einer Offenlegung an US-Behörden oder US-Gerichte muss das EU-Unternehmen informiert werden. Dennoch kann es sich um eine Gag-Order handeln – diese würde genau das verbieten. Es könnte eine Pflicht vereinbart werden, Rechtsmittel auszuschöpfen oder dafür zu sorgen, dass das EU-Unternehmen im Verfahren angehört wird. Genauer gesagt, das US-Unternehmen sollte dazu verpflichtet werden, das angesprochene Widerspruchsrecht des CLOUD-Act zwingend wahrzunehmen, wenn es sich um einen EU-Bürger handelt. Last but not least, es könnte vertraglich vereinbart werden, dass im Fall einer unrechtmäßigen Offenlegung der Vertrag schnell beendet werden kann. Das Problem dabei ist allerdings, dass eine Umstellung der Unternehmensinfrastruktur nicht über Nacht erfolgen kann und Alternativen zum verwendeten Dienst erst gefunden werden müssen.

5. Resümee

Vertragsrecht und Datensicherheitsmaßnahmen können zwar das Risiko für unrechtmäßige Datenübertragungen senken, lösen aber das Grundproblem der Massenabfragen durch die USA nicht. Die Datenübermittlung in die USA an sich wäre kein Problem, wenn nicht die Gefahr der rechtsgrundlosen Weiterübermittlung an US-Behörden bestünde. Der Entwurf zur e-Evidence-Verordnung und den Gesprächen mit den USA dazu zeigen deutlich die Bemühungen, dass zumindest «offizielle» Anfragen von US-Behörden legalisiert werden sollen.

Bis auf einer politischen Ebene eine Lösung gefunden wird, müssen sich EU-Unternehmen bewusst sein, dass jede Datenschutzbehörde in der EU eine Datenschutzübermittlung in die USA beanstanden (Art. 58 Abs. 1 lit. d DSGVO, Art. 58 Abs. 2 lit. b DSGVO) oder sogar verbieten (Art. 58 Abs. 2 lit. f DSGVO) könnte, weil entweder die Rechtsgrundlage weggefallen ist und/oder sie das Risiko für die Betroffenen als zu hoch erachtet. Der Europäische Datenschutzausschuss äußert in seinem dritten Review zum Privacy Shield seine Bedenken zur Datenverarbeitung von US-Behörden für Zwecke der Rechtsdurchsetzung und nationalen Sicherheit[23]. Dass nationale Datenschutzbehörden Aussagen des Europäischen Datenschutzausschusses ignorieren ist unwahrscheinlich.

[23] Europäischer Datenschutzausschuss, EU – US-Privacy Shield – Third Annual Joint Review 2019, adopted on 12 November 2019.

6. Literatur

Anderson Trisha/Berengaut, Alexander/Garland, Jim/Hansen, Marty/Peets, Lisa, U.S. and U.K. Sign CLOUD Act Agreement, https://www.insideprivacy.com/surveillance-law-enforcement-access/10167/ (zuletzt abgerufen am 17.12.2019), 2019.

APA/red, Twitter nutzte für Sicherheit vorgesehene Telefonnummern für Werbung, https://www.derstandard.at/story/2000109667139/twitter-nutzte-fuer-sicherheitszwecke-vorgesehene-nutzer-telefonnummern-fuer-werbung (zuletzt abgerufen am 26.10.2019), 2019.

Bleich, Holger, Geplante EU-Verordnung gefährdet die Grundrechte der Bürger, https://www.heise.de/ct/artikel/Geplante-EU-Verordnung-gefaehrdet-die-Grundrechte-der-Buerger-4471900.html (zuletzt abgerufen am 26.10.2019), 2019.

Europäischer Datenschutzausschuss, First standard contractual clauses for contracts between controllers and processors (art. 28 GDPR) at the initiative of DK SA published in EDPB register, https://edpb.europa.eu/news/news/2019/first-standard-contractual-clauses-contracts-between-controllers-and-processors-art_de (zuletzt abgerufen am 15.12.2019), 2019.

Europäischer Datenschutzausschuss, EU – US-Privacy Shield – Third Annual Joint Review 2019, adopted on 12 November 2019, https://edpb.europa.eu/our-work-tools/our-documents/eu-us-privacy-shield-third-annual-joint-review-report-12112019_en (zuletzt abgerufen am 15.12.2019), 2019.

Europäischer Datenschutzbeauftragter, Opinion 7/2019, EDPS Opinion on Proposals regarding European Production and Preservation Orders for electronical Evidence in criminal Matters, 6 November 2019, https://edps.europa.eu/sites/edp/files/publication/opinion_on_e_evidence_proposals_en.pdf (zuletzt abgerufen am 15.12.2019), 2019.

Fanta, Alexander, EU-Kommission erneuert Persilschein für Datenaustausch mit den USA, https://netzpolitik.org/2019/eu-kommission-erneutert-persilschein-fuer-datenaustausch-mit-den-usa/ (zuletzt abgerufen am 27.10.2019), 2019.

Greis, Friedhelm, USA und Großbritannien vereinbaren Austausch von Serverdaten, https://www.golem.de/news/cloud-act-usa-und-grossbritannien-vereinbaren-austausch-von-serverdaten-1910-144286.html (zuletzt abgefragt am 26.10.2019), 2019.

Wittenhorst, Tilman, Bericht: Amazon lässt Alexa-Mitschnitte im Homeoffice auswerten, https://www.heise.de/newsticker/meldung/Bericht-Amazon-laesst-Alexa-Mitschnitte-im-Homeoffice-auswerten-4487911.html (zuletzt abgerufen am 26.10.2019), 2019.