WHITEPAPER

Der CLOUD Act und die DSGVO

Was Sie jetzt wissen müssen.

Es könnte bald unmöglich sein, die Risiken im Zusammenhang mit der Nutzung von US-Cloud-Anbietern für die Verarbeitung persönlicher Daten zu akzeptieren.

Dieses Whitepaper beschäftigt sich mit der Datensouveränität in Zeiten, in denen das US-Recht mit FISA, ECPA und CLOUD Act in einen immer größeren Konflikt zum EU-Recht, insbesondere zur DSGVO, gerät. Weitere Herausforderungen dürften sich durch den Brexit, sowie neue Entscheidungen des Gerichtshofs der Europäischen Union (EuGH) ergeben.

Inhalt

Glossar

AWS	Amazon Web Services: US-Anbieter für Cloud-Computing-Dienstleistungen
BREXIT	British Exit: der Austritt Großbritanniens aus der Europäischen Union (EU)
CLOUD Act	Clarifying Lawful Overseas Use of Data Act: das US-Gesetz zur Klärung der rechtmäßigen Nutzung von Daten im Ausland
DSGVO	Die Datenschutzgrundverordnung
ECPA	Electronic Communications Privacy Act: US-Gesetz zur Regelung von Privatsphäre und Zugriffsbefugnissen durch US-Behörden in elektronische Kommunikation
EU	Europäische Union
EUGH	Gerichtshof der Europäischen Union bestehend aus Gerichtshof und Gericht der Europäischen Union
EWR	Europäischer Wirtschaftsraum
FISA	Foreign Intelligence Surveillance Act: US-Gesetz zur Überwachung in der Auslandsaufklärung und zur Tätigkeit der US-Nachrichtendienste außerhalb des Territoriums der USA
PATRIOT Act	Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act: US-Anti-Terrorismus-Gesetz
US	United States of America: Vereinigte Staaten von Amerika

Einführung

Sind Ihnen Datenschutz und Datensicherheit wichtig? Ganz egal, wie Sie jetzt antworten: Wenn Sie ein europäisches Unternehmen sind, müssen Sie sich spätestens seit dem 25. Mai 2018, ernsthafte Gedanken zu Datenschutz und Datensicherheit machen. Denn an diesem Tag trat die Datenschutzgrundverordnung (DSGVO) in Kraft. Zudem können US-Behörden von US-Firmen spätestens seit dem 23. März 2018 im Rahmen des CLOUD (Clarifying Lawful Use of Overseas Data) Acts den Zugriff auf Daten verlangen und das unabhängig davon, in welchen Ländern sich die Server und Daten befinden.

Damit kam es 2018 auf beiden Seiten des Atlantiks zu massiven Veränderungen. Die Regularien verfolgen jedoch ganz unterschiedliche Ziele im Hinblick auf den Datenschutz. Für Unternehmen bedeutet das nicht nur ein Labyrinth von Vorgaben und Paragraphen. Darüber hinaus widersprechen sich die Gesetze in wesentlichen Punkten. Unternehmen sind unter Umständen gezwungen, zwei unvereinbaren Regelwerken zu entsprechen, um Bußgeldern und anderen Strafmaßnahmen zu entgehen.

Dieses Whitepaper gibt Ihnen eine kurze Einführung, Illustration und Orientierung bezüglich dieser unterschiedlichen Regularien. Wir wollen Ihnen alternative Ansätze aufzeigen und Ihre Entscheidungsfindung im Konfliktfeld zwischen CLOUD Act und der europäischen DSGVO erleichtern.

Verlust von 20 Millionen Euro oder 4 % Ihres weltweiten Umsatzes!

Die Risiken bei Nichteinhaltung der DSGVO sind ganz real: Ein EWR-Unternehmen verstößt im Regelfall gegen die DSGVO, wenn es Gesuche nach US-amerikanischen ECPA- oder FISA Acts befolgt. Denn der Schutz von Datenübermittlungen in Drittländer gemäß Kapitel V DSGVO ist von besonderer Bedeutung. Allein für Verstöße gegen Kapitel V DSGVO kann es zu den Höchstbußgeldern von 20 Millionen Euro beziehungsweise vier Prozent des weltweiten Konzernumsatzes kommen. [i] Aufsichtsbehörden und Gerichte der EU-Mitgliedstaaten könnten bei Missachtung der DSGVO-Vorgaben sogar Unterlassungsanordnungen oder Gefängnisstrafen verhängen. [ii]

CLOUD Act und ECPA

Motiv

Der CLOUD Act wurde von den Vereinigten Staaten in Kraft gesetzt, um die US-Zugriffsberechtigung auf weltweite elektronische Informationen klarzustellen, zu erweitern und Zugriffe zu beschleunigen. Zuvor hatte der PATRIOT Act bereits 2001 einen deutlich erweiterten US-Zugang zu Informationen in den USA und weltweit festgelegt. Die Einhaltung bestehender Rechtshilfeabkommen wurde als zu umständlich angesehen, um den wachsenden US-Bedarf an elektronischem Beweismaterial zeitnah zu decken. Internationale Abkommen gemäß CLOUD Act, die den direkten US-Zugriff auf weltweit gespeicherte Daten für Unternehmen ohne Bezug zu den USA erweitern, dürften der nächste Schritt sein.

Zweck

Das CLOUD Act autorisiert internationale Abkommen zwischen den Vereinigten Staaten und ausländischen Partnern. Diese Abkommen zielen darauf ab, den Bürgern beider Nationen mehr Sicherheit zu bieten und gleichzeitig einen – mit geltendem US-Recht vergleichbaren – Datenschutz zu gewährleisten. Diese gegenseitigen internationalen Abkommen sollen es ausländischen Partnern ermöglichen, schneller Zugang zu elektronischen Beweismitteln zu erhalten und dadurch effektiver Kriminalität und Terrorismus zu bekämpfen. Diese Abkommen werden wahrscheinlich keinen ausreichenden Schutz im Sinne der DSGVO bieten.

Definition

Der Clarifying Lawful Overseas Use of Data Act ist ein Bundesgesetz der Vereinigten Staaten, das im Jahr 2018 mit der Verabschiedung des Consolidated Appropriations Act in Kraft getreten ist. Es sieht den Zugang zu elektronischen Informationen aus aller Welt vor und erlaubt Durchführungsvereinbarungen mit ausländischen Regierungen über den wechselseitigen Zugang zu Daten.

Auswirkungen

US-Behörden waren überzeugt, vor dem CLOUD Act bereits über weltweite Zugriffsrechte zu verfügen, was laut jüngster Gerichtsentscheidung jedoch nicht zutraf. Das neue Gesetz stellt nun klar, dass der physische Standort der Daten für das Zugriffsrecht nach ECPA unerheblich ist. [iii]

Daher sollten Sie den CLOUD Act, vor allem aber dessen mögliche Folgen für Ihr Geschäft kennen. Sie sollten für betroffene Geschäftsprozesse am besten eine gründliche Risikoanalyse durchführen: Geschäftsprozesse, die den Einsatz von öffentlichen Cloud-Diensten (wie E-Mail, soziale Medien, Datenaustausch, Datenspeicherung und Plattformen) umfassen, sind besonders betroffen. Die Analyse sollte unbedingt auch eine Überprüfung der Dienstleister Ihres Cloud-Anbieters einschließen. Überdenken Sie die Cloud-Strategie Ihres Unternehmens und ziehen Sie einen hybriden Ansatz in Betracht. Definieren Sie, welche Daten Sie ohne Risiko in Clouds von US-Unternehmen speichern können und welche Daten Sie nur DSGVO-konformen europäischen Dienstanbietern anvertrauen. Lassen Sie sich vom Namen des US-amerikanischen CLOUD Act nicht irreführen: Tatsächlich bezieht sich das Gesetz nicht nur auf die Cloud: Der CLOUD Act wirkt weit über die Cloud hinaus. Betroffen ist vielmehr grundsätzlich jede Art von Information, die ein Anbieter für Sie vorhält.

Datenschutzgrundverordnung (DSGVO)

Motiv

Einerseits zielt die Datenschutzgrundverordnung darauf ab, den Schutz von Betroffenen bezüglich ihrer personenbezogenen Daten besser zu gewährleisten. Dazu wurden unter anderem höhere Bußgelder, präzisere Regelungen, eine Kooperation zwischen nationalen Behörden und eine klare internationale Geltung eingeführt. Gleichzeitig soll sie im EWR das regulatorische Umfeld vereinfachen. Dazu ersetzt die DSGVO die zuvor gültige EU-Datenschutzrichtlinie mit konkreteren verbindlichen und im EWR weitgehend einheitlichen Regelungen.

Zweck

Bei der Verarbeitung personenbezogener Daten sind die Grundrechte und -freiheiten sowie das Recht auf den Schutz personenbezogener Daten zu respektieren. Die Verordnung zielt auf die EU-weite Angleichung beim Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Datenverarbeitung sowie die Gewährleistung des Austauschs personenbezogener Daten zwischen den EU-Mitgliedstaaten ab.

Definition

In der EU ist das Recht natürlicher Personen auf Privatsphäre und Datenschutz ein Grundrecht. Die DSGVO regelt die Verarbeitung und Vertraulichkeit personenbezogener Daten und gewährleistet das Recht des Einzelnen auf Datenschutz und den Schutz seiner Privatsphäre. Die Datenschutzgrundverordnung gilt in der EU und im Europäischen Wirtschaftsraum (EWR). Die DSGVO schützt aber nicht nur personenbezogenen Daten von Bürgern der Europäischen Union (EU) und des Europäischen Wirtschaftsraums, sondern auch von Personen, deren Daten von Unternehmen innerhalb der EU oder des EWR verarbeitet werden. Die DSGVO enthält spezielle Anforderungen für die Übermittlung personenbezogener Daten außerhalb der EU und des EWR.

Auswirkungen

Die DSGVO regelt die Verarbeitung personenbezogener Daten und das weitreichend: Die DSGVO gilt nicht nur für die Verarbeitung von Informationen zu natürlichen Personen durch Unternehmen mit Sitz in der EU [iv] oder innerhalb des EWR. Auch Unternehmen außerhalb der EU oder des EWR sind unmittelbar der DSGVO unterworfen, wenn sie das Verhalten von Personen in der EU beobachten, oder wenn sie Personen innerhalb der EU Waren und Dienstleistungen anbieten [v]. Wer gegen die Vorgaben der DSGVO verstößt oder diese ignoriert, sollte mit schweren Sanktionen rechnen. Dazu gehören Schadensersatzklagen sowie Bußgelder, deren Höhe 20 Millionen Euro oder vier Prozent des weltweiten Konzernumsatzes betragen kann.

EU-Grundrechte und US-Zugriffsrechte im Konflikt

Der Schutz der Privatsphäre fußt in der EU und in den USA auf völlig unterschiedlichen Rechtsgrundlagen. In beiden Regionen drohen Unternehmen bei Verstößen gegen gesetzliche Vorgaben hohe Bußgelder und möglicherweise sogar Haftstrafen: Die Weitergabe von Daten an US-Behörden verstößt in der Regel gegen EU-Recht. Die Nicht-Weitergabe verstößt meist gegen US-Recht. US-Recht könnte sogar EU-Unternehmen mit Niederlassungen in den USA betreffen.

Privatsphäre ist (k)ein universelles Grundrecht

In der EU gehört das Recht auf Privatsphäre zu den Grundrechten. [vi] Die DSGVO sorgt für weitreichenden Schutz personenbezogener Daten. Seit Inkrafttreten der DSGVO kann die Missachtung der Privatsphäre recht teuer werden, auch für Unternehmen, die ihren Firmensitz außerhalb der EU haben. In den USA hingegen gibt es kein verfassungsmäßig geschütztes universelles Grundrecht auf Privatsphäre oder Datenschutz. [vii] Im Falle von Cloud-Daten, „die der Kontrolle eines dritten Computerbetreibers unterliegen, könnten die Informationen keinerlei verfassungsmäßigem Datenschutz unterliegen". [viii].

Damit haben US-Regierungsbehörden sehr weitreichende Befugnisse zur Datenbeschaffung. Die Nichteinhaltung der US-Gesetze zum Datenzugriff bewirkt für US-Firmen ein hohes Risiko. Die Einhaltung der US-Gesetze birgt dagegen (abgesehen von der Öffentlichkeitswirkung) meist nur geringe Risiken. Die Privatsphäre ist in den USA unter bestimmten Umständen geschützt, aber nicht universell. Der Schutz ist wohl auch gering, weil das US-amerikanische Verfassungsrecht dem Gesetzgeber bei der Einschränkung des Rechts auf Privatsphäre kaum Grenzen setzt.

US-Zugriff vs. DSGVO-Bestimmungen

Selbst bei Zivilprozessen in den USA gilt die Regel, dass die Streitparteien im Grundsatz vollständigen Zugang zu allen relevanten nicht besonders geschützten („privileged") Beweisen haben. Ähnlich ist es auch in anderen Bereichen. Jenseits des vierten Zusatzes der US-Verfassung zum Schutze von US-Bürgern vor staatlichen Übergriffen können sich US-Regierungsbehörden Informationen häufig ohne gerichtliche Genehmigung beschaffen. Da es kein universelles Grundrecht auf Privatsphäre gibt, ist der Schutz der Privatsphäre häufig optional. Das Maß an Privatsphäre gegenüber US-Behörden sinkt zudem im Hinblick auf Personen außerhalb der USA: Der ohnehin schon sehr eingeschränkte Schutz der Privatsphäre schrumpft oft weiter oder wird gar vollständig aufgehoben. Den Zugang zu weltweiten Informationen hatten die USA demnach schon lange vor Inkrafttreten des CLOUD Act für sich in Anspruch genommen:

„Ein Gericht oder eine Behörde in den Vereinigten Staaten kann, durch ein Gesetz oder eine Gerichtsentscheidung dazu ermächtigt, eine seiner Zuständigkeit unterstehende Person verpflichten, (...) Informationen (...) außerhalb der Vereinigten Staaten vorzulegen." [ix]

US-Vorladungsbefugnisse für weltweite Dokumente

Eine US-Zwangsvorladung („Subpoena“) kann DSGVO-widrigen US-Zugang zu Informationen ermöglichen. Für eine solche Vorladung genügt, dass ein Unternehmen „Besitz, Gewahrsam oder Kontrolle“ („possession, custody, or control“) über Daten ausübt. Zum Beispiel, wenn sich die Informationen im Zugriff eines Tochterunternehmens, eines verbundenen Unternehmens oder einer Muttergesellschaft befinden:

„Der Standort der Dokumente – ob in der territorialen Zuständigkeit des Gerichts oder nicht – ist unerheblich.“ [x]

Zwangsvorladungen können nicht nur von staatlicher Seite, sondern auch von nichtstaatlicher Seite ergehen, beispielsweise im Rahmen von straf- oder zivilrechtlichen Gerichtsverfahren. Bereits vor Erlass des CLOUD Acts waren Zwangsvorladungen zur Herausgabe von Daten in den USA oder anderen Ländern (einschließlich persönlicher Information über EU-Bürger) möglich. [xi] Eine zentrale Begrenzung ist die Kontrolle (z. B. faktische Zugriffsmöglichkeit) einer Person über Daten und die Zuständigkeit des US-Gerichts für diese Person. [xii] Selbst ein ausländischer Vertreter einer Drittpartei kann möglicherweise zwangsvorgeladen und zur Datenherausgabe verpflichtet werden. [xiii]

Auch in Zivilprozessen sind weitreichende Zwangsvorladungen möglich, wenn eine der Prozessparteien bezüglich der Daten Besitz, Gewahrsam oder Kontrolle hat. [xiv]

Dies kann je nach Interpretation auch bei Tochterunternehmen, verbundenen Unternehmen oder einer Muttergesellschaft der Fall sein, denn der Begriff „Kontrolle“ wird sehr weit ausgelegt. So definieren einige Gerichte „Kontrolle“ als „Rechtsanspruch, Dokumente zu beschaffen“. Dieser besteht nach US-Recht etwa, wenn eine Niederlassung einer Partei die Daten besitzt und diese Niederlassung der Partei gehört oder vollständig von dieser kontrolliert wird. [xv] Eine Tochtergesellschaft könnte sogar die „Kontrolle“ über die Informationen im Besitz ihrer Muttergesellschaft haben, soweit die Tochtergesellschaft Informationen der Muttergesellschaft regelmäßig für ihre eigenen Geschäftsbedürfnisse erhalten kann. [xvi]

Demnach sind die meisten EU-Töchter von US-Konzernen zumindest verpflichtet, die bei ihnen gespeicherten Informationen der US-Mutter zur Verfügung zu stellen. Darüber hinaus könnten sie sogar dazu verpflichtet werden, Daten von verbundenen Unternehmen oder Mutterunternehmen herauszugeben. US-Verwaltungsbehörden brauchen häufig weder einen Gerichtsbeschluss noch einen hinreichenden Verdacht für eine Zwangsvorladung. [xvii]

Über 500.000 Zwangsvorladungen wurden erlassen, seit der PATRIOT Act 2001 die Anforderungen für die Vorladungen herabsetzte. [xviii]

Der ECPA in der durch das CLOUD-Gesetz geänderten Fassung

Nicht nur Vorladungen im Allgemeinen, sondern auch Maßnahmen nach dem Electronic Communications Privacy Act (ECPA, in der durch den CLOUD Act geänderten Fassung) können den DSGVO-widrigen US-Zugang zu Informationen ermöglichen. [xix] Ein solcher Zugang setzt voraus, dass ein Unternehmen „Besitz, Gewahrsam oder Kontrolle" bezüglich der Daten hat, zum Beispiel, wenn sich die Informationen im Zugriff eines Tochterunternehmens, eines verbundenen Unternehmens oder einer Muttergesellschaft befinden:

> „Ein Anbieter (...) muss (...) Informationen offenlegen (...), die sich in seinem (...) Besitz, Gewahrsam oder unter seiner Kontrolle befinden (...), unabhängig davon, ob sich diese (...) Informationen innerhalb oder außerhalb der Vereinigten Staaten befinden." 18 U.S. Code § 2713. [xx]

Bisher ist die Definition des Begriffs „Kontrolle" mangels Rechtsprechung in diesem Zusammenhang noch unklar. Es ist jedoch wahrscheinlich, dass diese Vorschrift ähnlich ausgelegt wird wie die soeben dargestellte Vorschrift zu zivilrechtlichen Zwangsvorladungen [xxi].

Die meisten US-Anbieter könnten betroffen sein, und eine Tochtergesellschaft könnte sogar die „Kontrolle" über Informationen im Besitz ihrer Muttergesellschaft haben. [xxii] Anbieter können Daten nach US-Recht ohne Wissen der Betroffenen weitergeben. [xxiii]

Der ECPA regelt Vorladungen, Gerichtsbeschlüsse und Durchsuchungsbeschlüsse. Wie viele Anordnungen für einen Datenzugriff aufgrund der Modifikation des CLOUD Acts ergangen sind, ist schwer zu sagen. Google berichtet jedoch, dass Vorladungen und Durchsuchungsbeschlüsse gemäß ECPA die „bei Weitem häufigste" Art der Anfrage seien [xxiv]. Google kritisiert den ECPA dafür, die Privatsphäre unter ein bestimmtes Niveau zu senken, das Nutzer vernünftigerweise erwarten können. [xxv]

Der CLOUD Act führt ferner ein System von Exekutivabkommen ein: Der US-Präsident ist befugt, internationale Datenaustauschverträge zu unterzeichnen. Es ist sehr zweifelhaft, ob solche Abkommen im Einklang mit der DSGVO abgeschlossen werden dürfen. [xxvi] In Großbritannien ist bereits ein solches Abkommen in Kraft. [xxvii]

FISA Act: Geheime unkontrollierte Massenüberwachung

Der FISA Act ermöglicht den geheimen US-Zugriff auf (Personen-) Daten im Widerspruch zur DSGVO. FISA steht für Foreign Intelligence Surveillance Act. Der FISA Act ist ein Paradebeispiel dafür, dass US-Datenschutz Personen, die sich außerhalb der USA aufhalten, benachteiligt. Denn der erleichterte Zugang zu Informationen setzt die begründete Annahme voraus, dass sich eine Zielperson „außerhalb der Vereinigten Staaten befindet“. [xxviii]

Zudem müssen die US-Behörden nach Informationen suchen, welche die Sicherheit oder die Außenpolitik der Vereinigten Staaten betreffen. [xxix] Der FISA Act erfordert keine Gerichtsentscheidung für geheime Überwachung, Unterstützung oder Zugang zu Informationen. [xxx]

In den sechs Monaten zwischen Januar und Juni 2018 allein erhielt Google auf der Grundlage des FISA Acts Anfragen bezüglich der Daten von fast 100.000 Nutzern oder Konten. [xxxi]

Die FISA-Gerichtsverhandlungen sind geheim. Das Gericht unterliegt keiner öffentlichen Aufsicht. Im Januar 2018 wurde der FISA Act bis zum Jahr 2023 verlängert. [xxxii]

Missachtung von CLOUD oder FISA: US-Bußgelder und Haft

US-Recht erfordert im Allgemeinen, dass personenbezogene Daten von EU-Bürgern auch dann an die USA weitergegeben werden müssen, wenn dies gegen ausländisches Recht oder ein internationales Abkommen, wie z.B. einen Rechtshilfevertrag, verstößt. [xxxiii] Wenn ein Unternehmen Informationen nicht zur Verfügung stellt, verstößt es daher im Allgemeinen gegen US-Recht. [xxxiv] Die Verletzung einer US-Gerichtsentscheidung („Missachtung des Gerichts") kann schwerwiegende Folgen haben:

„Ungehorsam oder Widerstand gegen den rechtmäßigen Erlass, den Prozess, die Verfügung, die Entscheidung, das Dekret oder die Anordnung" eines US-Gerichts erlaubt es dem US-Gericht, „nach eigenem Ermessen mit einer Geldstrafe oder einer Gefängnisstrafe oder beidem zu bestrafen." [xxxv]

Yahoo wurde mit einer Geldstrafe von 250.000 Dollar pro Tag für die Nichteinhaltung einer FISA-Anfrage gedroht. [xxxvi] Eine Inhaftierung wegen Missachtung des Gerichts könnte auch das Management eines Konzerns treffen. Für den CLOUD Act könnten DSGVO-Strafen teilweise hoch genug sein, um einen Anbieter „unzumutbar zu belasten" [xxxvii], was die gerichtliche Anordnung nach CLOUD-Act anfechtbar machen könnte.

Bei ECPA- und FISA-Compliance: Kaum Risiken in den USA

In US-Gerichten müssen Anbieter im Allgemeinen keine Zivilklage auf Schadenersatz wegen Verletzung von Persönlichkeitsrechten befürchten, wenn sie dem ECPA oder dem FISA-Gesetz nachkommen. Aber Cloud-Anbieter könnten die Ausnahme sein.

Laut Edward Snowden gab es früher wenig Schutz vor Missbrauch. [xxxviii] Daher könnte eine Zusammenarbeit mit US-Behörden auf den ersten Blick riskant erscheinen. Aber der FISA Act entbindet „jeden Anbieter elektronischer Kommunikationsdienste für die Bereitstellung von Informationen, Einrichtungen oder Hilfe" weitgehend von zivilrechtlichen Haftungsansprüchen. [xxxix] „Kommunikationsdienstanbieter" und Personen die solchen helfen, sind auch durch den ECPA weitgehend von Haftungsansprüchen bezüglich ihrer Unterstützung befreit:

„Gegen einen Anbieter von drahtgebundenen oder elektronischen Kommunikationsdiensten, seine leitenden Angestellten, Mitarbeiter, Agenten oder andere angegebene Personen darf kein Klageanspruch vor einem [Anm.: US-] Gericht bestehen wegen der Bereitstellung von Informationen, Einrichtungen oder Unterstützung in Übereinstimmung mit den Bestimmungen einer gerichtlichen Verfügung, einer richterlichen Anordnung, einer Zwangsvorladung, einer gesetzlichen Ermächtigung oder einer Bestätigung gemäß diesem Kapitel." [xl]

Daher besteht in den USA im Allgemeinen ein geringes Haftungsrisiko für Unternehmen und Personen, die US-Anforderungen nachkommen oder dabei helfen. Typische Cloud-Anbieter wie Amazon AWS könnten jedoch teilweise vor einem US-Zivilgericht haftbar sein: Sie bieten keine „elektronischen Kommunikationsdienste", sondern „Ferndatenverarbeitung" an. Nach dem Wortlaut des ECPA sind sie damit nicht vom Haftungsschutz erfasst. [xli]

Nebenbei ist die Haftung außerhalb der USA immer eine Option: Der Haftungsschutz, der nur ein Teil des US-Rechts ist, wird von Gerichten oder Aufsichtsbehörden in der EU, z.B. im Falle von DSGVO-Verletzungen, nicht angewendet. Doch die Durchsetzung von Haftungsentscheidungen kann je nach dem Standort der pfändbaren Vermögenswerte später ein Problem darstellen. Denn es scheint unwahrscheinlich, dass eine EU-Gerichtsentscheidung in den USA gegen ein Unternehmen, das auf ein US-Ersuchen gemäß FISA oder ECPA reagiert hat, erfolgreich durchgesetzt werden kann. [xlii]

DSGVO-Anforderung: Garantiertes Schutzniveau

Die Weitergabe personenbezogener Daten an Drittstaaten außerhalb eines internationalen Vertrages verstößt vermutlich meist gegen Art. 5.1 (a) i.V.m. Art. 6.1 und Kapitel V DSGVO. Ein solcher Verstoß könnte der Regelfall sein, sollten EU-Unternehmen oder ihre Auftragsverarbeiter gemäß ECPA Informationen bereitstellen. [xliii]

Die DSGVO verlangt im Allgemeinen eine gesetzliche Grundlage für die Verarbeitung nach Art. 6 DSGVO. Die „rechtliche Verpflichtung" gem. Art. 6.1 DSGVO als Grundlage für die rechtmäßige Verarbeitung berücksichtigt nur Gesetze und Behörden der EU und der Mitgliedstaaten. Abgesehen von internationalen Rechtshilfeabkommen („MLATs") – können Gesetze von Drittstaaten mangels Anerkennung durch die DSGVO grundsätzlich nicht zu einer Rechtfertigung der Datenverarbeitung führen. [xliv]

Wenn personenbezogene Daten während der Verarbeitung in ein Drittland gelangen, gilt Kapitel V DSGVO: Verantwortliche und Auftragsverarbeiter müssen Kapitel V befolgen, „um sicherzustellen, dass das durch diese Verordnung garantierte Schutzniveau für natürliche Personen nicht untergraben wird". [xlv] Soweit kein Angemessenheitsbeschluss vorliegt, müssen „Verantwortliche oder Auftragsverarbeiter geeignete Garantien" vorsehen und „durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung" stellen. [xlvi]:

Es müssen dann geeignete Schutzmaßnahmen getroffen werden. Geeignete Schutzmaßnahmen sind Standarddatenschutzklauseln, verbindliche interne Datenschutzvorschriften, genehmigte Verhaltensregeln zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen und ein genehmigter Zertifizierungsmechanismus. Wenn ein Unternehmen nicht „sicherstellt, dass das durch diese Verordnung garantierte Schutzniveau für natürliche Personen nicht untergraben wird" [xlviii] und „durchsetzbare Rechte der betroffenen Personen und wirksame Rechtsbehelfe für die betroffenen Personen zur Verfügung stehen" [xlix], und keine Ausnahme gilt [l], verstößt es regelmäßig gegen die DSGVO. [li]

Bietet das Privacy Shield ein „der Sache nach gleichwertiges" Schutzniveau?

Noch steht das Ergebnis aus, doch könnte der Europäische Gerichtshof (EuGH) den Angemessenheitsbeschluss der EU-Kommission für das „Privacy Shield" [das aktuelle EU-Datenschutzabkommen mit den USA] für ungültig erklären. Der EuGH könnte noch im Sommer 2020 zur Entscheidung gelangen, dass auch Standarddatenschutzklauseln keinen ausreichenden Grund für die Verarbeitung personenbezogener Daten in den USA darstellen. Damit wäre die Verarbeitung personenbezogener Daten durch US-Cloud-Anbieter im Regelfall rechtswidrig. [lii] Aufgrund der weitreichenden FISA- und ECPA-Regelungen (s. o.) könnte sich diese Entscheidung auch auf EU-Niederlassungen US-amerikanischer (Cloud-)Anbieter erstrecken.

Die Rechtmäßigkeit von Datenübertragungen im Rahmen des EU-US Privacy Shield [liii] beruht auf einem Angemessenheitsbeschluss der Europäischen Kommission. In Anwendung der Vorgaben der Schrems-I-Entscheidung des EuGHs [liv] stellt sich die Frage, ob das Privacy Shield ein „Schutzniveau der Grundrechte gewährleistet, das dem in der Rechtsordnung der Union garantierten Niveau (...) der Sache nach gleichwertig ist." [ECJ Judgment of 6.10.2015, C-362/14 - Schrems at 73 and 96]

Aufgrund der Bedeutung des Rechts auf Privatsphäre und der Anzahl der Betroffenen verfügt die Europäische Kommission über wenig Ermessensspielraum und steht nun vor einer strengen Überprüfung ihres Angemessenheitsbeschlusses. [lv]

Problematisch für die Angemessenheit ist:

- wenn sich „Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen nicht auf das absolut Notwendige beschränken“ [lvi];
- wenn „eine Regelung, die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen (...) gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, (...) [um] spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken“, die einen solchen Eingriff rechtfertigen können [lvii];
- wenn das Recht „es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen“ [lviii];
- wenn Betroffenenrechte unzureichend gewährleistet sind [lix]; und
- wenn wirksame Rechtsmittel fehlen [lx].

Wichtige Überlegungen in diesem Zusammenhang könnten auch sein,

- ob innerstaatliche Gesetze den Schutz der Privatsphäre in internationalen Verträgen missachten;
- ob eine betroffene Person nichts von einer möglichen Verletzung ihrer Rechte erfährt, beispielsweise wenn Daten im Geheimen weitergegeben und verarbeitet werden;
- ob ein für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter von der Haftung für Datenschutzverletzungen befreit ist; und
- ob eine unkontrollierte Massenüberwachung zulässig ist.

UPDATE: Privacy Shield ab sofort unwirksam – US-Anbieter überhaupt noch DSGVO-konform?

Der EuGH hat am 16. Juli 2020 (Rechtssache C-311/18) wie erwartet entschieden, dass auch Privacy Shield unwirksam ist. US-Anbieter die nur Privacy Shield anbieten, dürfen ab sofort unter anderem von EWR-Unternehmen wie dargestellt nicht mehr für personenbezogene Daten genutzt werden. Aber auch wenn Anbieter Standardvertragsklauseln oder andere Absicherugen nach Kapitel V DSGVO anbieten, sind Verantwortliche und Datenschutzbehörden bei US-Anbietern oft verpflichtet, eine Datenübertragung zu untersagen:

Wenn der Datenschutz in einem Land tatsächlich nicht gewährleistet ist - so liegt es wohl regelmäßig zumindest bei US-Cloud-Anbietern – verstößt deren Nutzung gegen die DSGVO und die dargestellten Sanktionen drohen. Denn die dargestellte Möglichkeit der US-Behörden zu weitgehend unkontrollierter Massenüberwachung verstößt gegen die DSGVO. Die dargestellte Haftungsfreistellung dürfte bei Standardvertragsklauseln zu zusätzlichen Problemen führen.

Schlussfolgerungen

EU-Unternehmen sollten im Lichte des Rechtmäßigkeitsprinzips und Kapitel V der DSGVO sowie um vor EU-Sanktionen sicher zu sein, US-Behörden grundsätzlich wie jede andere unbefugte Person behandeln, die rechtswidrig Informationen erlangen möchte. Die Androhung u. a. von Haftstrafen wegen Nichteinhaltung des US-Rechts könnte DSGVO-Bußgelder reduzieren, dürfte sie aber nicht abwenden.

Wegen der Unwirksamkeit des Privacy Shields und des dargestellten hohen Risikos der Unwirksamkeit von alternativen Maßnahmen nach Kapitel V DSGVO noch in 2020 sollten Unternehmen jetzt mit der Umstellung von US- auf EU-Anbieter anfangen oder zumindest die entsprechenden Pläne und Strategien für entwickeln.

Verweise

[i] Art. 83.5 (c) GDPR.

[ii] The details largely depend on EU Member State law beyond the scope of this paper. The requirement for such law would likely be that "provisions of domestic law contain a legal basis for ordering such detention which is sufficiently accessible, precise and foreseeable in its application" and "that the limitation on the right to liberty, guaranteed by Article 6 of the Charter of Fundamental Rights, that would result from so ordering complies with the other conditions laid down in that regard in Article 52(1) of the Charter", ECJ Judgment of 19.12.2019, C-752/18 – Deutsche Umwelthilfe.

[iii] 18 U.S. Code Chapter 121.

[iv] Art. 3.1 GDPR.

[v] Art. 3.2 GDPR.

[vi] e. g. Art. 7 and 8 European Charter of Fundamental Rights, the general principles of Community law, and Article 8 of the European Convention on Human Rights, centrally regulated in the EU via the General Data Protection Regulation.

[vii] Constitutional amendment 4 provides a protection against searches and with wording could have been the basis for extensive privacy protections. Constitutional amendments 1, 3, 5, and 9 are at least sometimes interpreted to provide some form of privacy in some areas to some persons. But in common law tradition, the amendments are mostly interpreted narrowly along their wording and not extended to cover modern needs. Statutory privacy protections are not universal either in territorial or substantive scope, e. g.: The California Consumer Privacy Act centrally applies in California and rules are significantly reduced unless there is a sale of information. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) applies across the US, but only to Health Information.

[viii] Microsoft Corp. v. United States (In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197 (2d Cir. 2016) at 38, available at https://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf citing H.R. Rep. No. 99-647, at 23.

[ix] Restatement (Third) of Foreign Relations Law § 442(1)(a).

[x] Gerling Intern. Ins. Co. v. C.I.R, 839 F.2d 131, 140 (3d Cir. 1988) citing Marc Rich Co., A.G. v. United States, 707 F.2d 663, 667 (2d Cir. 1983), cert. denied 463 U.S. 1215, 103 S.Ct. 3555, 77 L.Ed.2d 1400 (1983); In re Uranium Antitrust Litigation, 480 F. Supp. 1138, 1144 (N.D.Ill. 1979). See also In re Search Content That Is Stored at Premises Controlled by Google, Case No. 16-mc-80263-LB (N.D. Cal. Apr. 19, 2017); In re Search Content That Is Stored at Premises Controlled by Google, Case No. 16-mc-80263-LB (N.D. Cal. Apr. 25, 2017);

[xi] Microsoft Corp. v. United States (In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197 (2d Cir. 2016) at 11 footnote 5.

[xii] "It is no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has in personam jurisdiction of the person in possession or control of the material. See, e.g., First National City Bank of New York v. Internal Revenue Service etc., 271 F.2d 616 (2d Cir. 1959), cert. denied, 361 U.S. 948, 80 S.Ct. 402, 4 L.Ed.2d 381 (1960).", United States v. First National City Bank, 396 F.2d 897, 900-1 (2d Cir. 1968).

[xiii] H. Christopher Boehning & Daniel J. Toal, "Third-Party Subpoena Extended to Overseas Affiliates" N.Y.L.J., June 2, 2015, copy available at https://www.paulweiss.com/media/3006545/3june15nylj.pdf.

[xiv] Rule 45 of the US Federal Rules of Civil Procedure; further conditions apply for a subpoena.

[xv] A "corporation must produce documents possessed by a subsidiary that the parent corporation owns or wholly controls", United States v. Int'l Union of Petroleum & Indus. Workers, AFL-CIO, 870 F.2d 1450, 1452 (9th Cir. 1989); King.com Ltd. v. 6 Waves LLC, No. C-13-3977 MMC (N.D. Cal. Mar. 31, 2014). Control could here be that "the parent had the power to elect a majority of the board of directors of the subsidiary." Gerling Intern. Ins. Co. v. C.I.R, 839 F.2d 131, 140 (3d Cir. 1988) citing In re Uranium Antitrust Litigation, 480 F. Supp. 1138, 1144 (N.D.Ill. 1979).

[xvi] "Where the relationship is thus such that the agent-subsidiary can secure documents of the principalparent to meet its own business needs and documents helpful for use in the litigation, the courts will not permit the agent-subsidiary to deny control for purposes of discovery by an opposing party." Gerling Intern. Ins. Co. v. C.I.R, 839 F.2d 131, 141 (3d Cir. 1988)

[xvii] Microsoft Corp. v. United States (In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197 (2d Cir. 2016) at 16 footnote 16, available at https://cases.justia.com/federal/appellate-courts/ca2/14-2985/14-2985-2016-07-14.pdf.

[xviii] Jennifer Valentino-DeVries, N.Y.Times, Sept. 20, 2019, "Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies", https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html.

[xix] For a more detailed analysis see Jansen, CR-Blog 28 Mar 2018, Krieg der Daten: Episode I – Die Drittländer-Cloud-Bedrohung, https://www.cr-online.de/blog/2019/07/12/krieg-der-daten-episode-i-die-drittlaender-cloud-bedrohung/ and EPDB-EDPS, 12 July 2019, Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex), available at https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en. Further criticism at https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data and https://blog.dropbox.com/topics/company/the-cloud-act-passed--what-s-next, and https://blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/. Opposing view: https://aws.amazon.com/de/compliance/cloud-act/.

[xx] 18 U.S. Code § 2713.

[xxi] Both 18 U.S. Code § 2713 and FRCP Rule 45 use the words "possession, custody, or control". US v. Microsoft already discussed whether the standard of subpoenas applies. The legislation using the exact same wording as a subpoena could be regarded as a clarification that the subpoena standard does indeed apply. But due to the different context, courts could (and should) apply a different definition. Ideally, such a definition would respect the privacy laws of foreign countries.

[xxii] In case courts interpret the statute as they interpret Rule 45 of the US Federal Rules of Civil Procedure, which uses the same wording of "possession, custody, or control".

[xxiii] 18 U.S. Code § 2703 (b) (1) (A)

[xxiv] "By far the most common is the subpoena, followed by search warrants. A federal statute called the Electronic Communications Privacy Act, known as ECPA, regulates how a government agency can use these types of legal process to compel companies like Google to disclose information about users. (...)" The ECPA (18 U.S. Code CHAPTER 121) was modified by the CLOUD Act to clarify that information must be provided "regardless of whether such communication, record, or other information is located within or outside of the United States" (18 U.S. Code § 2713). It's possible, however, that this is only the most common type of request, not the type of request affecting the most users.

[xxv] "It has failed to keep pace with how people use the Internet today. That's why we've been working (...) to seek updates to this important law so it guarantees the level of privacy that you should reasonably expect when using our services.", see Google, Legal process for user data requests FAQs, "What types of legal requests does Google receive from U.S. government agencies?" available at https://support.google.com/transparencyreport/answer/7381738.

[xxvi] Jansen, CR-Blog 28 Mar 2018, Krieg der Daten – Kollision von EU DSGVO und US CLOUD Act, https://www.cr-online.de/blog/2018/03/28/krieg-der-daten-kollision-von-eu-dsgvo-und-us-cloud-act/.

[xxvii] Kitty Donaldson, Mark Burton, 28. September 2019, Facebook, WhatsApp Will Have to Share Messages With U.K., available at https://www.bloomberg.com/news/articles/2019-09-28/facebook-whatsapp-will-have-to-share-messages-with-u-k-police.

[xxviii] Section 702 FISA Act = 50 U.S. Code § 1881a.

[xxix] Foreign intelligence information includes "information with respect to a foreign power or foreign territory that relates to (...) (A) the (...) security of the United States; or (B) the conduct of the foreign affairs of the United States" (50 USC § 1801(e) (2)).

[xxx] A court decision is not required for targeting a person: "[T]he Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information" (50 U.S. Code § 1881a (a)). "[T]he Attorney General and the Director of National Intelligence may direct, in writing, an electronic communication service provider to immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services" (50 U.S. Code § 1881a (i) (1)). An interesting question is whether the requirement to provide "assistance" according to the FISA Act could force a business to establish subpoena and/or CLOUD Act "control".

[xxxi] https://transparencyreport.google.com/user-data/us-national-security.

[xxxii] https://www.congress.gov/bill/115th-congress/senate-bill/139/text.

[xxxiii] e.g. Agreement with the United States on mutual legal assistance, Art. 13 allows refusal due to "sovereignty, security, or public or other essential interests." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:22003A0719(02).

[xxxiv] A US court order can be granted in 50 U.S. Code § 1881a (j)(3) or a warrant in 18 U.S. Code § 2703 (b)(1) (A), (d).

[xxxv] 18 U.S. Code § 401.

[xxxvi] https://www.wired.com/2014/09/feds-yahoo-fine-prism/

[xxxvii] 18 U.S. Code § 2703 (d).

[xxxviii] '[T]here was a guy who was supposed to be teaching me. And sometimes he would spin around in his chair, showing me nudes of whatever target's wife he's looking at. And he's like: "Bonus!"', https://www.spiegel.de/international/world/interview-with-edward-snowden-about-his-story-a1286605.html.

[xxxix] 50 U.S. Code § 1881a (i)(3).

[xl] 18 U.S. Code § 2703 (e).

[xli] Remote computing services provide remote "computer storage or processing services" (18 USC § 2711(2)) and "remote computing service providers" are not "electronic communication service providers" (see 18 USC § 2711(2), 18 USC § 2258E(2), and 18 USC § 2510(15)).

[xlii] While the wording e.g. "cause of action" (18 U.S. Code § 2703 (e)) does not point towards a judgement enforcement restriction, foreign court decisions ignoring it or other restrictions could be regarded as contrary to the public policy of the US.

[xliii] "Currently, unless a US CLOUD Act warrant is recognised or made enforceable on the basis of an international agreement, and therefore can be recognised as a legal obligation, as per Article 6(1)(c) GDPR, the lawfulness of such processing cannot be ascertained, without prejudice to exceptional circumstances where processing is necessary in order to protect the vital interests of the data subject on the basis of Article 6(1)(d) read in conjunction with Article 49(1)(f).", EPDB-EDPS, 12 July 2019, Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex), available at https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

[xliv] "The extraterritorial application of [third country] laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation." (Recital 115 GDPR); EPDB-EDPS, 12 July 2019, Joint Response to the LIBE Committee on the impact of the US Cloud Act on the European legal framework for personal data protection (annex), available at https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-edps-joint-response-libe-committee-impact-us-cloud-act_en.

[xlv] Art. 44 GDPR.

[xlvi] Art. 46.1 GDPR.

[xlvii] Regulated in Art. 45 GDPR and Art. 46 GDPR.

[xlviii] Art. 44 GDPR.

[xlix] Art. 46.1 GDPR.

[l] e.g. Art. 49 GDPR.

[li] Assuming the GDPR is applicable to the case otherwise.

[lii] An exception would be where a company legally uses other methods under chapter V, such as Binding Corporate Rules, if the ECJ does not invalidate them for US processing of personal data.

[liii] Commission Implementing Decision (EU) 2016/1250, last reviewed by the European Commission in December 2018. The review does not seem to have considered the CLOUD Act in this review.

[liv] ECJ Judgment of 6.10.2015, C-362/14 - Schrems at 73 adjusted to apply to the GDPR.

[lv] ECJ Judgment of 6.10.2015, C-362/14 - Schrems at 78.

[lvi] ECJ Judgment of 6.10.2015, C-362/14 - Schrems at 92.

[lvii] ECJ Judgment of 6.10.2015, C-362/14 - Schrems at 93.

[lviii] ECJ Judgment of 6.10.2015, C-362/14 - Schrems at 94.

[lix] ECJ Judgment of 6.10.2015, C-362/14 - Schrems at 95.

[lx] ECJ Judgment of 6.10.2015, C-362/14 - Schrems at 95.

Der Autor

Dennis G. Jansen, LL.M. (Berkeley):

Nach seiner juristischen Ausbildung an Universitäten in Freiburg, Berlin, Sydney, London und Berkeley arbeitete Herr Jansen als Justiziar, Rechtsanwalt und Dozent mit Schwerpunkt auf IT-Recht und internationalem Datenschutz und gründete das Digitalforensik-Unternehmen Devidence.

A1 Digital

Kontakt Deutschland
A1 Digital Deutschland GmbH
St.-Martin-Straße 59
81669 München
Deutschland
E-Mail: sales@a1.digital

https://a1.digital

Kontakt Österreich
A1 Digital International GmbH
Lassallestraße 9
1020 Wien
Österreich
E-Mail: info@a1.digital

https://a1.digital

Jetzt Partner werden!
A1 Digital Deutschland GmbH
St.-Martin-Straße 59
81669 München
Deutschland
E-Mail: partner@a1.digital

https://a1.digital/partner-werden

Impressum A1 Digital Deutschland GmbH
Registriert im Handelsregister des Amtsgerichts München, HRB 232709,
Umsatzsteuer-ID: DE31182648, Wirtschafts-Identifikationsnummer: TAX ID 143/111/41741,
Vertretungsberechtigte Personen: Elisabetta Castiglioni (CEO), Roland Haidner (CFO)

Impressum A1 Digital International GmbH
Firmenbuchnummer: 366000k, Registriert bei: Handelsgericht Wien,
Umsatzsteuer-ID: ATU 66624566, Vertretungsberechtigte Personen:
Elisabetta Castiglioni (CEO), Roland Haidner (CFO),
Kammerzugehörigkeit: Wirtschaftskammer Wien,
Gewerbliche Vorschriften: Gewerbeordnung – GewO in der geltenden Fassung

202005_v1