Datenschutz Europa und USA

Prekärer Datenfluss

Was sich die USA beim Datenschutz von Europa abschauen

In den USA hatten Datenkraken lange Zeit leichtes Spiel. Doch nun droht der Datenfluss zu versiegen. Joe Biden hat den Datenverkehr mit Europa zur Chefsache erklärt, gleichzeitig arbeiten Demokraten und Republikaner fieberhaft an einem bundesweiten Datenschutzgesetz. Das hat aber seine Tücken, wie unser Überblick zeigt.

Von Falk Steiner

kompakt

- Bislang gelten in den US-Bundesstaaten unterschiedliche Datenschutzgesetze.
- Ein einheitliches Datenschutzgesetz ist in greifbare Nähe gerückt, lässt den Zugriff der Behörden aber außen vor.
- Präsident Biden will darüber hinaus den Datenaustausch zwischen der EU und den USA mit einem neuen Datenschutzrahmen absichern, der EU-Bürgern ein Klagerecht einräumt.

Mit der Datenschutz-Grundverordnung (DSGVO) hat die EU 2016 einen Standard gesetzt, an dem sich Anbieter und Gesetzgeber aus aller Welt orientieren müssen, wenn sie mit dem Recht des 27-Staaten-Bundes in Europa kompatibel sein wollen. Dabei

prallen immer wieder Welten aufeinander – insbesondere transatlantische. Die USA gelten mit ihren staatlichen und privatwirtschaftlichen Akteuren immer noch als Land der Datensammler. Dort existiert bis heute kein bundesweites Datenschutzrecht. Stattdessen kocht jeder US-Bundesstaat sein eigenes Süppchen. Weil die transatlantischen Datenflüsse aus Europa zu versiegen drohen, muss die US-Regierung dringend eine Lösung finden.

Das fehlende Datenschutzrecht auf Bundesebene ist eine von mehreren Hürden: Die DSGVO erlaubt den Export von personenbezogenen EU-Daten nur, wenn im Zielland der Schutz dieser Daten auf einem vergleichbaren Niveau wie in Europa gewährleistet ist. Die EU-Kommission als zuständige Behörde muss dies prüfen und dann eine sogenannte Angemessenheitsentscheidung treffen.

Derartige „Adequacy Decisions“ wurden bislang für 14 Staaten getroffen, darunter Südkorea, Japan, Israel, Uruguay, Kanada und die Färöer-Inseln. Der US-Rechtsrahmen ist hingegen nicht ausreichend. Daher suchten die USA in den vergangenen 20 Jahren immer wieder nach Alternativen, um die Datentransfers rechtlich abzusichern.

Doch sowohl die sogenannte Safe-Harbor-Vereinbarung zwischen EU und US-Regierung aus dem Jahr 2000 als auch die Nachfolgeregelung Privacy Shield von 2016 wurden vom Europäischen Gerichtshof (EuGH) kassiert: Die Absprachen, die keine Verträge im Sinne des Völkerrechts sind, konnten in der EU erhobene Daten nicht ausreichend sichern, befanden die Richter in Luxemburg nach zwei Klagen des österreichischen Aktivisten Max Schrems.

Nach Privacy Shield

Lange ist danach wenig passiert. Doch nun läuft den Unternehmen die Zeit davon: Nach und nach fallen die verbliebenen rechtlichen Möglichkeiten weg, doch noch

irgendwie legal personenbezogene Daten in die USA zu transferieren. Die irische Datenschutzaufsichtsbehörde DPC Ireland bearbeitet dabei den wichtigsten Fall: Sie könnte Facebook untersagen, personenbezogene Daten von seinem EU-Hauptsitz auf der Insel in die USA zu transferieren. Das steht in einem Entscheidungsentwurf, den die Iren Anfang Juli an ihre Kollegen der übrigen europäischen Datenschutzaufsichtsbehörden verschickt haben. Obwohl die DPC unter Datenschützern als sehr zurückhaltend gilt, könnte ihr Vorhaben das Aus für datengetriebene US-Unternehmen in Europa bedeuten. Die Facebook-Mutter Meta hat ihre Aktionäre schon mehrfach gewarnt, dass sie aufgrund der dann drohenden empfindlichen DSGVO-Bußgelder womöglich Teile ihres Europageschäfts aufgeben müsste – und damit Milliarden an Umsatz verlöre.

Mark Zuckerberg hat Aktionäre von Meta bereits gewarnt, dass sein Konzern womöglich bald keine personenenbezogenen Daten aus Europa mehr in die USA übertragen darf. *Bild: Eric Risberg/AP/dpa*

Sammelklagen statt Aufsichtsbehörden

Parallel dazu bewegt sich der Datenschutz in den USA: Viele US-Bundesstaaten bereiten Gesetze vor oder haben bereits welche erlassen, die die Privatsphäre besser schützen sollen. Zwei Staaten stehen im Zentrum der Aufmerksamkeit: Kalifornien schärft im Januar 2023 seinen fünf Jahre alten California Consumer Privacy Act (CCPA) mit dem Californian Privacy Rights Act (CPRA) nach. In Illinois gilt seit 2008 der Biometric Information Privacy Act (BIPA). Das Schutzgesetz für biometrische Daten hatte nach Sammelklagen mehrere Vergleiche mit bemerkenswerten Summen zur Folge: McDonalds zahlte 50 Millionen Dollar, Google 100 Millionen Dollar und Facebook sogar 650 Millionen Dollar an Kläger aus Illinois, weil sie deren biometrische Daten unerlaubt verarbeitet und gegen den BIPA verstoßen hatten. Fast im Monatstakt kommen neue Millionenvergleiche hinzu, der Druck auf die Unternehmen steigt.

Während in Europa Aufsichtsbehörden die Strafen für Verstöße verhängen, schließen sich in den USA Betroffene vor allem in Sammelklagen zusammen. Organisationen sammeln die Rechtsansprüche vieler Bürger und reichen vor Gericht Klage gegen ein Unternehmen ein. In den seltensten Fällen enden diese Verfahren mit einem Urteil. Stattdessen schließen Kläger und Beklagte einen Vergleich. Das kann für die Firmen mitunter teurer sein als ein Gerichtsurteil.

Aufsichtsbehörden haben in den USA deutlich weniger Möglichkeiten, Bußgelder zu verhängen als in Europa. Nur in wenigen Fällen nutzt etwa die Handelsaufsicht, die Federal Trade Commission (FTC), ihre rechtlich begrenzten Möglichkeiten: Zuletzt etwa, weil sich ein Unternehmen nicht an seine Selbstverpflichtung hielt, die es im Zuge der Privacy-Shield-Vereinbarung abgegeben hatte. Auch wenn der EuGH die Privacy-Shield-Angemessenheitsentscheidung inzwischen annulliert hat, behalten die damit verbundenen

Selbstverpflichtungen von Firmen in den USA weiterhin ihre Gültigkeit.

Flickenteppich

Für in- und ausländische Unternehmen sind die in einzelnen Bundesstaaten der USA aufploppenden neuen Datenschutzgesetze ein Problem: Statt an einem einzelnen Rechtsrahmen müssten sie sich eigentlich an den Vorgaben jedes Staates einzeln ausrichten und somit Nutzer in Maine anders als in Illinois oder Kalifornien behandeln. Kein Wunder, dass sich viele der großen Technologiekonzerne ein einheitliches US-Datenschutzrecht wünschen.

Einige der Datenschutzgesetze der Bundesstaaten definieren den Begriff „personenbezogene Daten“ äußerst weitreichend, erläutert Jan Sebisch von der Gesellschaft für Außenwirtschaft und Standortmarketing (GTAI): „Sie räumen den Verbrauchern in Bezug auf ihre Daten durchaus mit EU-Niveau vergleichbare Betroffenenrechte ein, zum Beispiel das Recht auf Löschung, und in bestimmten Konstellationen sogar ein privates Klagerecht.“ Mangels US-Bundesdatenschutzgesetz gebe es für Unternehmen jedoch keine allgemeinen Leitlinien oder Faustformeln, wann sie „auf der sicheren Seite sind“. Es komme stets auf die konkrete Fallkonstellation und das entsprechende einzelstaatliche Recht an, sagt Sebisch.

Neues Bundesdatenschutzrecht

Ein Vorschlag, das zu ändern, liegt derzeit in den beiden Kammern des US-Kongresses: der American Data Privacy and Protection Act (ADPPA). Er wurde von Vertretern der Republikaner und Demokraten initiiert und schließlich von einflussreichen Mitgliedern des Repräsentantenhauses und des Senats eingebracht. Aus Sicht von Sebisch ist ein solch parteiübergreifender Vorschlag sehr beachtlich, weil Demokraten und Republikaner in puncto Datenschutzrecht zuvor nicht auf einen Nenner gekommen seien.

Der ADPPA könnte ein Bundesdatenschutzrecht schaffen, das in einigen Teilen dem EU-Recht ähnelt. Er betrachtet nicht nur unmittelbar personenbezogene Daten als regulierbar, sondern auch solche Daten, die einen Personenbezug herstellen können, wenn man sie mit weiteren Angaben koppelt. Dazu zählen auch sogenannte Identifier, denen sich Personen eindeutig zuordnen lassen.

Zudem schreibt er vor, das Erheben, Verarbeiten und Weitergeben von Daten auf das Nötige zu beschränken und fordert damit eine ähnliche Datensparsamkeit wie die DSGVO. Laut ADPPA dürfen Daten nur noch erhoben werden, wenn dies „vernünftigerweise notwendig und verhältnismäßig“ ist. Darunter fallen Daten für Produktion und Dienstleistungen, Kundenkommunikation, Rechnungswesen und IT-Sicherheit.

An einigen Stellen geht der ADPPA-Vorschlag sogar über den Text der DSGVO hinaus: etwa beim Verbot irreführender Oberflächengestaltungen, die Betroffene zu ungewollten Einwilligungen verleiten. Hier folgt der ADPPA dem neuen Digital Services Act (DSA) der EU und formuliert darüber hinaus restriktive Regelungen zur algorithmischen Verarbeitung biometrischer Daten. „Er hat mehr Momentum als jede Vorgängerinitiative“, erläutert Tyson Barker, der für die Deutsche Gesellschaft für Auswärtige Politik (DGAP) in Berlin die transatlantische Technologiepolitik beobachtet. „Der Vorschlag beschränkt Sammelklagen, verdrängt stärkere Einzelstaatengesetze, macht bei den Betroffenenrechten viele Anleihen bei der DSGVO und integriert Elemente des DSA, etwa zu datenbasierter Werbung“, zählt Barker auf.

Derzeit hält er es jedoch für unwahrscheinlich, dass der ADPPA in dieser Form verabschiedet werde, weil ihn die wichtigste Person nicht unterstützt: Maria Cantwell, die demokratische Vorsitzende im Wirtschaftsausschuss des Senats. An Cantwell führt laut Barker kein Weg vorbei. Sie fordert wesentlich weiter gehende Regelungen zum Schutz der Privatsphäre, als sie der ADPPA derzeit vorsieht. Auf jeden Fall will sie eines

verhindern: dass ein schwaches Bundesgesetz stärkere Regelungen in einzelnen Bundesstaaten aushebelt.

US-Senatorin Maria Cantwell möchte verhindern, dass ein zu laxes bundesweites Datenschutzgesetz künftig rigidere Vorgaben in einzelnen Bundesstaaten blockiert. *Bild: Maria Cantwell / U. S. Senate*

Bundesrecht und Landesrecht

Der Streit um den ADPPA und Cantwells Auffassung ähnelt der Subsidiaritätsdebatte in Europa: Was soll auf der obersten Ebene rechtlich geregelt werden, was sollen untere Ebenen beschließen? Die vollständige Vereinheitlichung auf Bundesebene zu Lasten der Gesetzgebung der Mitgliedstaaten wird in den USA als „preemption“ bezeichnet. Dies ist im ADPPA zumindest für bestehende Gesetze nicht vorgesehen. Er führt eine lange Liste von strengeren Gesetzen auf Bundes- und Einzelstaatsebene auf, die ausdrücklich nicht ausgehebelt werden sollen – etwa der Biometric Privacy Act aus Illinois. Cantwell befürchtet jedoch, dass der ADPPA künftige strengere Datenschutzregelungen in einzelnen Bundesstaaten ausschließt und somit landesweit einen zu laxen Datenschutz zementiert.

Der ADPPA regelt laut Sebisch auch den Zusammenhang zwischen behördlichen und privatrechtlichen Klagen. So sollen

geschädigte Personen vier Jahre nach Inkrafttreten des Gesetzes private Klagen vor dem Bundesgericht einreichen dürfen. Bei Datenschutzverletzungen von Unternehmen könnten sie Schadenersatz, Unterlassung, Prozesskosten und Anwaltsgebühren geltend machen, erläutert Sebisch.

Bevor sie eine Klage einreichen, müssten Betroffene dem ADPPA-Entwurf zufolge aber die Federal Trade Commission (FTC) und den Generalstaatsanwalt ihres Bundesstaates informieren. Eröffnet eine der beiden Institutionen ein Verfahren, wären Sammelklagen für dessen Dauer erst einmal ausgeschlossen. Die FTC könnte die Regelungen ähnlich wie die Datenschutzaufsichtsbehörden in Europa von sich aus durchsetzen. In diesen Tagen diskutiert der Ausschuss für Energie und Wirtschaft des US-Repräsentantenhauses sehr intensiv über den ADPPA-Entwurf. Damit er schließlich Gesetz wird, müssen seine Befürworter aber noch Maria Cantwell überzeugen. Jan Sebisch von der GTAI erwartet deshalb noch einige Änderungen, bevor der ADPPA das erste in den gesamten USA gültige Datenschutzgesetz überhaupt werden kann.

Mit dem ADPPA würden sich die USA der europäischen Vorstellung von Datenschutz deutlich annähern. Das wäre für transatlantische Datenübertragungen eine Verbesserung – dürfte aber noch lange nicht den Ansprüchen europäischer Datenschützer genügen. Dennoch begrüßt der Landesdatenschutzbeauftragte von Baden-Württemberg, Stefan Brink, die Initiative für das Gesetz: „Die Strahlkraft der Datenschutzgrundverordnung reicht ganz offensichtlich bis in die USA“, freut sich Brink angesichts vieler konzeptioneller Übernahmen im US-Vorschlag. „Inwiefern ein US-Datenschutzrecht die Beratung und Prüfung von Datenverarbeitungen mit Übermittlung in die USA verändert, hängt jedoch von der genauen Ausgestaltung des Gesetzes ab.“

Geheimdienste bleiben unberührt

Bei aller Euphorie enthält der ADPPA noch einige Lücken. Denn er soll grundsätzlich nur die Rechte von Personen mit einer US-Aufenthaltserlaubnis schützen. Darunter fallen auch viele in den USA lebende Ausländer. Doch selbst US-Bürger, die im Ausland leben, könnten sich dem Entwurf nach nicht auf ihn berufen, betont Calli Schroeder von der US-Bürgerrechtsorganisation EPIC. Zugleich wären Ansprüche aus den Vorschriften nicht von Personen außerhalb der USA einklagbar – also auch nicht von Europäern.

Einen Aspekt klammert der ADPPA zudem vollständig aus, da er als Verbraucherschutznorm konzipiert ist: den Datenzugriff von US-Behörden, darunter Strafverfolgern und Geheimdiensten wie der NSA. Genau hier liegt seit dem Urteil des EuGH zum Privacy Shield 2020 aber ein großer Stolperstein. Infolge der Snowden-Affäre prüfte der EuGH, unter welchen Umständen US-Behörden auf personenbezogene Daten zugreifen dürfen, die in den USA oder aber von US-Unternehmen außerhalb der USA gespeichert sind. In seinem Urteil bemängelte der EuGH sowohl die umfangreichen Zugriffsmöglichkeiten der US-Geheimdienste als auch das Fehlen von Rechtsmitteln, die EU-Bürger dagegen einlegen können. Dieses Urteil fordert das politische Washington gleich auf mehreren Ebenen heraus.

Auf der einen Seite ist es aus Sicht vieler US-amerikanischer Politiker ein Unding, dass ein europäisches Gericht amerikanischen Behörden und Gesetzgebern Vorschriften machen möchte. Auf der anderen Seite steht die enorme wirtschaftliche Bedeutung, die der EU-Markt für die meisten US-Tech-Konzerne hat. Und ein Szenario, in dem US-Firmen vom Datenstrom aus Europa abgeschnitten werden, ist mit der kommenden Entscheidung der irischen Datenschutzaufsichtsbehörde DPC nur noch Monate statt Jahre entfernt.

US-Präsident Joe Biden hat den Datenaustausch mit Europa zur Chefsache erklärt. Er möchte die EU mit Präsidialverfügungen zufriedenstellen. *Bild: Evan Vucci/AP/dpa*

TADPF soll Datenverkehr sichern

Damit EU-US-Datentransfers in Zukunft rechtssicher sind, soll daher eine neue Vereinbarung zwischen den USA und der EU her. Damit sie nicht ebenfalls vor dem Europäischen Gerichtshof scheitert, soll sie Daten von EU-Bürgern besser schützen als Safe Harbor und Privacy Shield.

US-Präsident Joe Biden erklärte dies zur Chefsache und kündigte bei seinem Besuch in Brüssel im Frühjahr einen neuen transatlantischen Datenschutzrahmen an: Die US-Regierung bietet der EU-Kommission ein Transatlantic Data Privacy Framework (TADPF) an. Die Vorarbeiten dafür laufen seit Anfang vorigen Jahres. Doch bis Redaktionsschluss fehlte das wohl wichtigste Element: der Rechtstext, mit dem die US-Regierung den Einwänden des EuGH künftig begegnen will.

Bislang gibt es nur mündliche Ankündigungen von Präsident Biden. So wollen die USA künftig weniger Daten über EU-Bürger

sammeln und ihre Behörden strenger prüfen. EU-Bürger sollen sich zudem rechtlich gegen eine Erfassung durch US-Geheimdienste wehren können – vor einer dafür zuständigen Gerichtsinstanz.

Solange die Präsidialverfügungen aber nicht vorhanden sind, kann die EU-Kommission mit dem in der DSGVO vorgesehenen Prozess für eine Angemessenheitsentscheidung nicht beginnen. Offen ist zudem, ob die EU-Kommission eine solche Entscheidung auf Basis von US-Präsidialverfügungen überhaupt treffen kann. Denn ein künftiger Präsident könnte eine Executive Order jederzeit mit einem Federstrich ändern.

Landesdatenschützer Stefan Brink wünscht sich deshalb einen anderen Weg: „Ein – parlamentarischer – Rechtsakt würde mehr Beständigkeit und damit auch Rechtssicherheit versprechen." Seine Behörde hätte bei der Angemessenheitsentscheidung der EU-Kommission zwar ein Recht zur Mitsprache, allerdings nicht zum Veto.

Klagen mit Ansage

„Europas Sorgen im Fall einer Wiederkehr Trumps könnten Überlegungen nötig machen, wie der Kongress die Präsidialverfügungen in Gesetzen kodifizieren könnte", sagt Tyson Barker von der DGAP. 2024 muss der US-Kongress den Abschnitt 702 des für die Überwachungsbefugnisse der Behörden wichtigsten Gesetzes, dem Foreign Intelligence Surveillance Act (FISA), erneut beschließen. „Das könnte eine Gelegenheit sein, das Gesetz so anzupassen, dass es die Inhalte der Präsidialverfügungen widerspiegelt", erklärt Barker.

Es bewegt sich also etwas beim Datenschutz in den USA, wenn auch aus europäischer Sicht zu wenig. Bei der Ankündigung des TADPF meinte Datenschutzvorkämpfer Max Schrems, er wolle die Vereinbarung prüfen. Er geht davon aus, dass nach einer eventuellen Angemessenheitsentscheidung der EU-Kommission zum TADPF Klagen beim EuGH eingereicht werden. Falls nicht von ihm

selbst, dann von anderen Datenschutzaktivisten. (*hag@ct.de*)

Datenschutzaktivist Max Schrems hat mit seinen Klagen bereits Safe Harbor und Privacy Shield gekippt. Die Geschichte könnte sich mit dem TADPF wiederholen. *Bild: Hans Punz/APA/dpa*

1. Literatur
2. Holger Bleich, FAQ: Das Ende des Privacy Shields, c’t 21/2020, S. 178