Kein Schutz, kein Datengeschäft

Wie das EuGH-Urteil erneut den transatlantischen Datenmarkt umwirft

Nadine Hofmann

August 2020
Blogpost

Key Facts

- Datenschutz durchlebt starke Entwicklung in den letzten Jahren
- Transatlantische Datenverarbeitung wurde durch Privacy Shield als Datenschutzabkommen gesichert
- Am 16. Juli 2020 jubeln Datenschützer: Der Europäische Gerichtshof erklärt das EU-US Privacy Shield für ungültig
- Europäische Unternehmen, die ihre Daten bei Partnern in den USA verarbeiten lassen, vor allem aber auch amerikanische Unternehmen, die Daten von europäischen Betroffenen verarbeiten, werden von dem Urteil schwer getroffen
- Der lukrative transatlantische Datenmarkt wird über Nacht illegal
- Datenschutzaufsichtsbehörden und Unternehmen müssen schnell agieren und zeitnah handeln

Safe Harbor – das erste Datenschutzabkommen zwischen EU und USA sinkt auf hoher See

Der Datenschutz durchlebte in den letzten 20 Jahren viele Entwicklungen zum Schutz personenbezogener Daten im Sinne der Bürger der EU. In dieser Zeit gab es immer wieder Bedenken beim Transfer dieser Daten in Nicht-EU-Länder, insbesondere den USA, dem Sitz vieler großer Firmen, die einen Großteil der daraus gewonnenen personenbezogenen Daten verarbeiten. Als fundamentale Bedingung galt, dass ein Drittland ein ausreichendes Schutzniveau gewährleisten müsse.

Im Jahr 2000 beschloss die Europäische Kommission das Safe Harbor-Abkommen, welches die Übermittlung in Übereinstimmung mit der europäischen Datenschutzrichtlinie von der EU in die USA sichern sollte. Betroffene Unternehmen konnten sich dieser Vereinbarung unterwerfen und öffentlich verpflichten die dort aufgestellten Prinzipien einzuhalten. Zur Untermauerung der Transparenz wurden diese Unternehmen in einer Liste des US-Handelsministerium *Federal Trace Comission* (FTC) geführt. Verstöße wurden mit Sanktionen und Verboten bestraft. Allerdings kamen diese Maßnahmen selten zum Tragen. Die Rechte der amerikanischen Geheimdienste zur Überwachung bemächtigen die USA zu Datensammlungen im großen Umfang, die dem europäischen Schutz vor Eingriffen in die Grundrechte[1] widersprechen, sodass das Abkommen vom Europäischen Gerichtshof (EuGH) für ungültig erklärt wurde. Auslöser war eine Klage gegen Facebook, das – wie viele andere Unternehmen auch – Daten aus Europa in die USA weiterleitete. Die irische Behörde, die zuständig ist für den europäischen Ableger des sozialen Netzwerkbetreibers, reagierte nicht die Datenübertragung zu überprüfen und gegebenenfalls auszusetzen. Die Untersuchungen ergaben, dass, trotz der Anforderungen des Safe Harbor-Abkommens die unterworfenen Unternehmen jederzeit und ohne Einschränkung vom Gesetzgeber verpflichtet seien die vereinbarten Schutzregeln nicht anzuwenden und die personenbezogenen Daten an die US-Sicherheitsbehörden auszuhändigen. Auch gibt es in den USA keine gesetzliche Regelung diese Eingriffe zu beschränken oder überhaupt gerichtlichen Rechtsschutz dagegen, wodurch es zur Verletzung von mindestens fünf der sieben Grundsätze kam: Der Betroffene wurde nicht informiert, ihm wurden die Wahlmöglichkeit vorenthalten sowie

[1] Charta der Grundrechte der Europäischen Union

die Möglichkeit von seinem Recht auf Korrektur oder Löschung Gebrauch zu machen sowie die fehlende Durchsetzung, hätte es zu eine Beschwerde kommen können. Der EuGH ist nicht ermächtigt Befugnisse nationaler Kontrollbehörden in Drittländern zu beschränken. Wenn aber, wie der Generalanwalt bemerkte, systematische Mängel festgestellt werden, dann ist die EU angehalten, Maßnahmen zum Schutz der Grundrechte ihrer Bürger, auf Achtung des Privat- und Familienlebens und auf den Schutz personenbezogener Daten zu ergreifen, um diese Rechte zu wahren.

Die Außerkraftsetzung des Beschlusses durch das EuGH erfolgte 2015 basierend auf bzw. begleitet von dem Positionspapier der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz)[2], das konstantierte, dass die Angemessenheit des Datenschutzniveaus nach Art. 45 DSGVO und das Vorliegen geeigneter Garantien gewährleistet sein müssen.Somit war die Datenübertragung auf Basis des Safe Harbor ausgeschlossen.

Das zweite transatlantische Abkommen scheitert erneut aufgrund der US-Überwachungsgesetze

Um dennoch Unternehmen Geschäftsbeziehungen zu ermöglichen, folgte im Folgejahr das EU-US Privacy Shield (es konnte seit dem 1. August 2016 angewendet werden). Die Verordnung klärte, so meinte man, wie Daten von EU-Bürgern beim Transfer in die USA geschützt werden sollen.

Das EU-US Privacy Shield wurde eine der wichtigsten Rechtsgrundlagen für den Transfer personenbezogener Daten europäischer Bürger in die USA, da es den Umgang mit den Informationen aus der EU in den USA festlegt. Um etwaige Zweifel zu beseitigen, begannen Konzerne parallel personenbezogene Daten in der EU zu speichern. Doch nicht alle beließen es dabei.

Wieder im Fokus stand der US-Konzern Facebook und die unterbesetzte irische Datenschutzaufsichtsbehörde. Während die irische Behörde um zusätzliche Mittel kämpft, um die weltweiten Anfragen zu bearbeiten und zu prüfen[3], übertrage Facebook trotz des Sitzes in Irland Daten in die USA. Der Fall spitzte sich zu mit der Enthüllung Edward Snowdens, dass die National Security Agency (NSA; Auslandsgeheimdienst für die weltweite Überwachung, Entzifferung und Auswertung elektronischer Kommunikation) Zugriff auf Daten von Facebook-Nutzern habe. Facebook argumentierte, dass das EU-Recht nicht für die Verarbeitung personenbezogener Daten für Zwecke der nationalen Sicherheit gelte. Weiter ist bekannt, dass der USA Patriot Act NSA und Crime Scene Investigation (CSI; Tatortermittlung / Spurensicherung) zur Verarbeitung personenbezogener Daten ohne richterliche Anforderung ermächtigt. Es folgte eine Überprüfung des EU-US Privacy Shields durch den EuGH. Auch wenn die Gesetzgebung in den USA hinsichtlich Datenschutz bisher unberührt blieb, verwundert es, dass das EU-US Privacy Shield laut des EuGH den Erfordernissen der „nationalen Sicherheit, des öffentlichen Interesses und der Einhaltung des amerikanischen Rechts Vorrang“ einräume, was wiederum die Eingriffe in die Grundrechte der Personen (Betroffenen) erlaube, deren Daten und deren Person die Verordnung

[2] DSK Kurzpapier Nr.4: Datenübermittlung in Drittländer
[3] https://www.thejournal.ie/data-protection-budget-4848807-Oct2019/

zu schützen gedachte. Dies wird rechtlich durch den National Security Letter (NSL)[4] unterstützt, durch den die Freigabe von Bestands- und Metadaten von Kommunikationsdienstleistern verlangt werden kann, die US-Unternehmen zur Übertragen der Daten beanspruchen. Allein im Fall von Facebook, dessen Nutzeranzahl seit 2015 fast auf das Doppelte gestiegen ist, handelt es sich in diesem Jahr immerhin um 2.6 Mrd. Nutzer[5]. Facebook, Apple, Google, Yahoo und weitere US-Konzerne in den USA sind also gesetzlich verpflichtet der NSA und dem Federal Bureau of Investigation (FBI; amerikanische Bundespolizei, vergleichbar mit deutschem Bundeskriminalamt) die Daten zur Verfügung zu stellen, welche die Daten wiederum auch für andere US-Behörden verfügbar machen. Die Betroffenen (Personen, deren personenbezogenen Daten verarbeitet werden) können sich dagegen nicht wehren – nicht nur, weil es gesetzlich geregelt ist[6], sondern weil sie gar nicht davon in Kenntnis gesetzt werden, ob ihre Daten offengelegt wurden. Die Zusage der USA, dass Daten aus der EU angemessen geschützt werden, konnte nicht belegt werden, trotz verbesserter Kontrollen der US-Behörden.. Eine Umfrage im Mai 2018[7] ergab, dass auch die Hälfte der Nutzer der Ansicht waren, dass Facebook die Schuld an der unerlaubten Datenweitergabe trägt. Trotz des Reputationsschadens bemerkte man in Summe keinen Einbruch der Nutzerzahlen. Die Ansprechperson für EU-Bürger, die sogenannte Ombudsperson, auf Seiten der USA als Teil des EU-US Privacy Shields konnte das richterliche Urteil nicht abwenden, da diese nicht unabhängig genug agieren kann und damit ist der gewährte Schutz der Betroffenen zweifelhaft bei den weitreichenden Überwachungsgesetzen der USA.

Final konstatiert der EuGH: Das Europäische Recht und insbesondere die DSGVO gelten generell für zu gewerblichen Zwecken erfolgenden Transfers persönlicher Daten.

Aufmerksamen Betroffenen könnte hier auffallen, dass der Grund für den Fall des Safe Harbor auch der Grund für den Fall des EU-US Privacy Shield ist. Warum dieser Missstand nicht früher erkannt wurde, wird oft mangelnden Ressourcen, fehlendem einheitlichen Vorgehen sowie der individuellen Auslegung des Datenschutzes in der Praxis und der exponentiell wachsenden Herausforderungen im Hinblick auf Datenschutz zugeschrieben. Das „unsichtbare Geschäft Datenschutz“ ist für viele nicht greifbar. Die Ignoranz demgegenüber hat auch Einfluss auf die heute präsenten Fragestellungen in Unternehmen. Im Jahr 2016[8] betrug der Gewinn aus eben diesem Geschäft in Deutschland im Bereich Marktforschung und Studien bereits 2,7 Mrd. Euro, in Europa 13,5 Mrd. Euro und weltweit 37,7 Mrd. Euro. Bis 2018 wuchsen diese Werte um weitere vier (14,0 Mrd. Euro) bis sechs Prozent (40,2 Mrd. Euro)[9]. Von den zehn größten Marktforschungsunternehmen sitzen sechs in den USA.

[4] Das Federal Bureau of Investigation stellt jährlich über 10.000 NSL, die das vier- bis fünffache an Daten betrifft (Quelle: Office of the Director of National Intelligence: Annual Statistics for Calendar Year 2015 regarding Use of Certain National Security Legal Authorities, 30. April 2016).
[5] Quelle: Facebook Q1 2020 Results, Seite 3 , April 2020
[6] Paragraf 702 des Foreign Intelligence Surveillance Act (FISA)
[7] Quelle: Umfrage PWC Vertrauen in Medien 2018, Seite 22 , Mai 2018
[8] Quelle: Deutsche Fachpresse Der B2B-Medien- und Informationsmarkt in Deutschland 2016, Seite 6 , Mai 2016
[9] Quelle: ESOMAR Global Market Research Report, September 2019

Unruhige Zeiten im Datenschutz bedingen Beratungsbedarf

Für die Unternehmen, die sich dem EU-US Privacy Shield unterworfen haben, bedeutet dies Unsicherheit, weil der Datentransfer in vielen Fällen illegal wird. Das betrifft nicht nur die amerikanischen Unternehmen wie Facebook, Google, Microsoft, Apple und Yahoo, die jeweils unzählige Nutzer in der EU haben. Die International Association of Privacy Professionals (IAAP) gibt zu bedenken, dass zehntausenden Unternehmen die legale Möglichkeit genommen wird, transatlantische Geschäfte im Wert von Billionen Dollar zu machen. Aus Europa sind bekannte Großunternehmen betroffen wie SAP, Aldi, Telefonica und Siemens.

Datenschutz per se verlangt nicht nur die Ergreifung technischer, sondern auch organisatorischer Maßnahmen. Der Schutz von personenbezogenen Daten richtet sich nicht nur an die Kunden/Klienten sondern auch an die Beschäftigten (z.B. zwischen Gesellschaften oder Niederlassungen eines Konzers). Diese sollen nicht nur im Unternehmen greifen, sondern die Überlegungen sollen sich auch auf internationale Datentransfers beziehen, weshalb ein Unternehmen prüfen muss, ob eine Datenübermittlung außerhalb der EU/des Europäischen Wirtschaftraums (EWR) wirklich notwendig ist. Denn mit der entstandenen Illegitimität des Datentransfers können auch Betroffene wie Klienten, Kunden und Beschäftigte zusätzlich Klage wegen unzulässigen Datenexports erheben und Schmerzensgeld verlangen. Mit den steigenden Bußgeldern und schärferen Kontrollen liegt es nahe, dass Unternehmen die verfügbaren Optionen untersuchen und ergreifen müssen. Neben der eigenen datenschutzkonformen Aufstellung im Unternehmen auf der Mikroebene, heißt das für den transatlantischen Datenhandel auf der Makroebene andere Möglichkeiten bis zu einem neuen Abkommen wahrzunehmen:

Gesetzliche Ausnahmen (Art. 49 Abs. 1 S. 1, 2 DSGVO)

Unter die gesetzlichen Ausnahmen fallen Verträge bei denen eine Übermittlung absolut erforderlich ist um diese zu erfüllen sowie bei der die Verarbeitung in diesem Drittland sogar zwingend erforderlich ist[10] oder im Interesse des Betroffenen liegt.

Einwilligungen (Art. 6 Abs.1 lit.a DSGVO)

Individuell ausgehandelte Vertragsklauseln bzw. Verwaltungsvereinbarungen, die die DSGVO auch erfüllen müssen. Dabei darf es sich aber, um die Grundsätze Transparenz, Freiwilligkeit und Widerruflichkeit zu erfüllen, nicht um lediglich Bestandteile der AGB handeln. Heute klassische Beispiele im Internet sind Opt-out Verfahren und Checkboxen unter Angabe von Kontaktmöglichkeiten für den Widerruf.

Standardvertragsklauseln (SVK; Art. 46 Abs. 2 lit. c DSGVO)

Diese Standardvertragsklauseln wurden von der EU Kommission aufgesetzt und sollen laut dem EuGH von bestimmten Voraussetzungen abhängig gemacht werden. Als Bedingungen gilt ein

[10] Z.B. bei einem Online-Einkauf im Ausland oder der Buchung eines Hotelzimmers

gleichwertiges Datenschutzniveau im Drittland. Das betrifft nicht nur den Schutzmaßnahmen des Unternehmens, sondern ebenso den Gesetzen des Landes. Ergänzungen zu den SVK dürfen darauf keinen Einfluss haben. Unverändert und unter Zustimmung der Datenschutzaufsichtsbehörden[11] können diese den Datentransfer in die USA erlauben. Veränderte Versionen müssen vorab von ihnen geprüft und zugestimmt werden. Im Fall der USA bedeutet dies jedoch, dass der Datenübermittler sich dem Recht und der Datenschutzaufsicht des Partnerlandes unterwerfen muss. Aktuell unterliegen diese Standardvertragsklauseln einer Überprüfung und deren Verwendung muss gut begründet werden.

Eine Auslegung des rheinland-pfälzischen Landesbeauftragen veranschaulicht, dass das datenübertragende Unternehmen Daten weiterhin übertragen könne, wenn sie nicht dem Foreign Intelligence Surveillance Act (FISA) 702 unterliege. Dies wird jedoch wiederum obsolet, sollte das Unternehmen Dienstleistungen von Telekommunikationsanbietern in Anspruch nehmen, an die sich das Gesetz vorrangig bezieht, da die US-Sicherheitsbehörden dadurch den Zugriff auf die personenbezogenen Daten erhalten.

Laut der US-amerikanischen Executive Order 12.333 kommt eine mögliche Überwachung der nicht ausreichend verschlüsselten Daten hinzu, wenn diese die transatlantischen Kabel durchqueren.

Binding Corporate Rules (BCR; Art. 47 DSGVO)

Wenn internationale Konzerne verbindliche Datenschutzregeln auf Basis von EU-Vorgaben aufstellen, spricht man von BCR. Der Vorteil liegt in der Schaffung eines einheitlichen und angemessenen Datenschutzniveaus innerhalb der Unternehmensgruppe. Die Datenschutzbehörden, in denen diese Konzerne einen Sitz haben, müssen dem zustimmen, wodurch sie auch weiterhin dem europäischen Datenschutz unterstehen und nicht vom EuGH-Urteil betroffen sind. Demgegenüber steht jedoch weiterhin die lokale Gesetzgebung sowie die Handlungsfähigkeit der zuständigen Datenschutzaufsichtsbehörden vor Ort, die die BCR zu genehmigen hat.

Nach heutigem Wissenstand gibt es noch zwei weitere Möglichkeiten:

Zertifizierungen (Art. 46 Abs. 2 lit. f, 42 DSGVO)

Unter bestimmten Kriterien können Unternehmen freiwillig datenschutzspezifische Zertifizierungsverfahren, Siegel oder Prüfzeichen erlangen, die dem Standard des Europäischen Datenschutzsiegels genügen und nachweisen, dass geeignete verbindliche und durchsetzbare Maßnahmen zum Schutz von personenbezogenen Daten ergriffen wurden. Außerdem müssen den betroffenen Personen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen. In der Praxis sind diese Zertifizierungen noch nicht in dem gewünschten Maße einsetzbar, da die paneuropäische Standardisierung dafür fehlt.

[11] In Deutschland gilt diese Regelung nicht

Code of Conduct (Art. 40 DSGVO)

Genehmigte Verhaltensregeln sind spezifische Vorgaben eines Verbandes[12], dem ihre Mitglieder eines Branchenverbandes Folge leisten müssen. Dabei dürfen sie das Sicherheitsniveau der DSGVO nicht unterschreiten, im Gegensatz dazu aber auch strengere Regelungen auferlegen.

Trotz Alternativen stellt das Urteil für viele Unternehmen eine schwer überwindbare Schranke dar

Britische und irische Datenschutzaufsichtsbehörden wiesen bereits nach der Außerkraftsetzung des Safe Harbor Abkommens darauf hin, dass Datenexporte auf Basis von vertraglichen Vereinbarungen[13], EU-Standardvertragsklauseln oder aktiven Einwilligungen[14] weiterhin möglich sind (simultan wie oben aufgeführt). Diese gebräuchlicheren Klauseln sollen garantieren, dass ein angemessener Schutz während der Übermittlung ins Ausland (im Gegensatz zum EU-US Privacy Shield, dass den Umgang im Ausland thematisiert) gegeben ist und wurden auch vom EuGH für zulässig erklärt. Die Klauseln wurden abgenickt mit dem Konsens, dass Datenschutzaufsichtsbehörden die Übertragung verbieten können und müssen, wenn der Datenschutz in einem anderen Land nicht erbracht werden kann. Im Umkehrschluss unterstreicht es den Grundsatz, dass das Drittland ein gleichwertiges Datenschutzniveau vorweisen muss. Dieses Schutzniveau darf durch die Europäische Kommission mit Hilfe eines einschlägigen Beschlusses auf Basis der DSGVO des Europäischen Parlaments und des Rates festgestellt werden[15].

Wenn das Schutzniveau nicht bestätigt werden kann, dann obliegt es dem in der EU ansässigen Unternehmen geeignete Garantien zur Datenübermittlung vorzusehen – also mit den Standardvertragsklauseln, die ebenfalls garantieren, dass Betroffene durchsetzbare Rechte und rechtswirksame Behelfe erhalten. Das bedeutet, dass das datentransferierende Unternehmen und der Empfänger der Daten dies vorab für das jeweilige Drittland prüfen. Für die in den USA ansässigen Muttergesellschaften heißt das, dass sie ihre Tochtergesellschaften selbst darüber informieren müssen, wenn bzw. dass die Standardvertragsklauseln nicht eingehalten werden können. Dies bestätigte einige Tage nach dem EuGH-Urteil auch der Europäische Datenschutzausschuss (EDPB). Weiterhin sollen die datentransferierenden Unternehmen weitere geeignete Maßnahmen zum Schutz der Daten vornehmen. Wie diese konkret aussehen sollen, ist noch nicht konkretisiert. Neben den Maßnahmen verweisen sie auf die Leitlinien zur Ausnahmevorschrift Art. 49 DSGVO, welche die Übertragung von Einzelfällen unter bestimmten Voraussetzungen erlaubt. Dies schließt regelmäßige und wiederkehrende Datentransfers aus.

Die Klärung der Rechtmäßigkeit des Datentransfers von Facebook aus Irland in die USA, welches den ganzen Prozess bis zur Nichtigerklärung des EU-US Privacy Shields anstieß, führte den Sachverhalt von der irischen Kontrollbehörde über den irischen High Court direkt zum EuGH.

[12] Wie Versicherungen, Industrie-, Handels- oder Handwerkskammern sowie Gewerkschaften oder Arbeitgeberverbände; in Deutschland z.B. Gesamtverband der Deutschen Versicherungswirtschaft e.V.
[13] Nach dem BDSG: zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen
[14] Unter der Prämisse nach Paragraf 4 a BDSG: Transparenz, Freiwilligkeit und Widerruflichkeit
[15] Solche Angemessenheitsbeschlüsse bestehen u.a. für die Schweiz, Neuseeland, Argentinien, Japan sowie für Kanada und Israel

Weil die USA das gleichwertige Niveau nicht vorweisen kann und die Grundrechte gefährdet sind, droht Facebook und möglicherweise auch anderen US-Konzernen in Hinblick auf das gefällte Urteil ebenso ein mögliches Verbot für die Nutzung der Standardklauseln, die weiterhin Bestand haben.

Fazit

Kritiker sehen einem Datenchaos entgegen, weil die Übertragung von Daten in die USA über Nacht verboten wurde und auch andere Importländer in naher Zukunft unter Kritik stehen. Sie fordern die Aushandlung eines neuen Abkommens für den Datentransfer zwischen der EU und den USA unter Berücksichtigung dort neu erlassener Datenschutzgesetze wie das California Consumer Privacy Act (CCPA), welches die Betroffenenrechte ähnlich der DSGVO regelt. Es ist ebenso möglich einen Vertrag oder zusätzliche Vertragsklauseln zu formulieren, in denen das gesetzliche Zugriffsrecht durch die NSA (und weiteren US-Behörden) für Daten aus der EU außer Kraft gesetzt wird.

Deutsche Datenschutzaufsichtsbehörden kündigten bereits an, verstärkt ihrer Prüfpflicht, demnach ihrem Recht zur Überprüfung des vorausgesetzten Datenschutzniveaus in Drittländern, nachzukommen. Damit gelangen auch Länder wie China, Russland oder Indien in den Fokus, aber auch England, wenn die Übergangsphase nach dem Brexit überstanden ist.

"Das Urteil und seine Folgen wird möglicherweise Einfluss auf die amerikanischen Überwachungsgesetze haben und Änderungen nach sich ziehen, um die Geschäfte in Europa wieder zu stabilisieren, denn für den aktuellen Präzedenzfall Facebook („Schrems II“) und andere Unternehmen ist die Verwendung von Standardvertragsklauseln nicht möglich, solange die USA auf dem Homeland Security Act bestehen. Auch wenn die Standardvertragsklauseln für die EU KOM ausreichend sind, genügen Sie nicht mehr dem EuGH. Übertragen solche Unternehmen in der Zwischenzeit trotzdem weiterhin Daten, können Bußgelder nach der DSGVO folgen – und dazu äußerte Facebook sich bisher gar nicht.

Auch Standardvertragsklauseln stellen erst dann eine Alternative dar, wenn dabei das gleiche Datenschutzniveau erreicht wird, wie es die DSGVO fordert. Diesen Beweis müsste der Verantwortliche führen, weil die DSGVO eine Verantwortung der Softwarehersteller bisher nicht kennt. Weitere Instrumente sind ausdrückliche Einwilligungserklärungen oder Binding Corporate Rules. Das bedeutet: Ohne den „Sonderzugang“ zu den EU-Daten, einer Änderung der amerikanischen Gesetzeslage und/oder der Ausklammerung (und deren Gewährleistung) dieser Daten aus der FISA bleibt den Unternehmen ggf. nur die Möglichkeit einer Auslagerung des Unternehmens nach Europa mit eigener Infrastruktur, juristischer Unabhängigkeit und auch dem bisher aus dem Weg gegangenen Zahlen von Steuern in der EU.

Fakt ist, dass Datenschützer nun auf eine Welle aufspringen müssen, die eine einheitliche Interpretation der DSGVO und klare Definitionen vonauszuführenden Maßnahmen verlangt. Konkurrierende Bestreben einen europäischen Cloud-Player auf den Markt zu bringen, wie aktuell GaiaX, dürften folglich des EuGH-Urteils auch verstärkt Aufmerksamkeit und Förderungen erhalten.

Quellen

1. Heise.de
2. Tagesschau.de
3. Sueddeutsche.de
4. Privacyshield.gov
5. Rnd.de (Redaktionsnetzwerk Deutschland)
6. Statista.com
7. Dr. Datenschutz
8. DSGVO
9. Datenschutz.org
10. https://www.datenschutzkonferenz-online.de

Autoren

Nadine Hofmann ist Expert Associate bei CORE. Ihr technischer Hintergrund liegt als Luft- und Raumfahrtingenieurin in der Konstruktion von Entwicklungsprozessen, sowie in der Produktion und Automatisierung. Bei CORE nutzt Nadine diese Erfahrung insbesondere für die Entwicklung zukunftsweisender Konzepte und Lösungen in der Informationssicherheit und unterstützt Kunden bei ihrer strategischen Geschäftsausrichtung durch den Einsatz innovativer Technologien.

Mail: nadine.hofmann@core.se

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://core.se/
Phone: +49 30 263 440 20
office@core.se

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://core.se/
Phone: +41 44 261 0143
office@core.se

COREtransform Ltd.
Canary Wharf, One Canada Square
London E14 5DY | Great Britain
https://core.se/
Phone: +44 20 328 563 61
office@core.se

COREtransform Consulting MEA Ltd.
DIFC – 105, Currency
House, Tower 1
P.O. Box 506656
Dubai I UAE Emirates
https://core.se/
Phone: +97 14 323 0633
office@core.se