LINK11

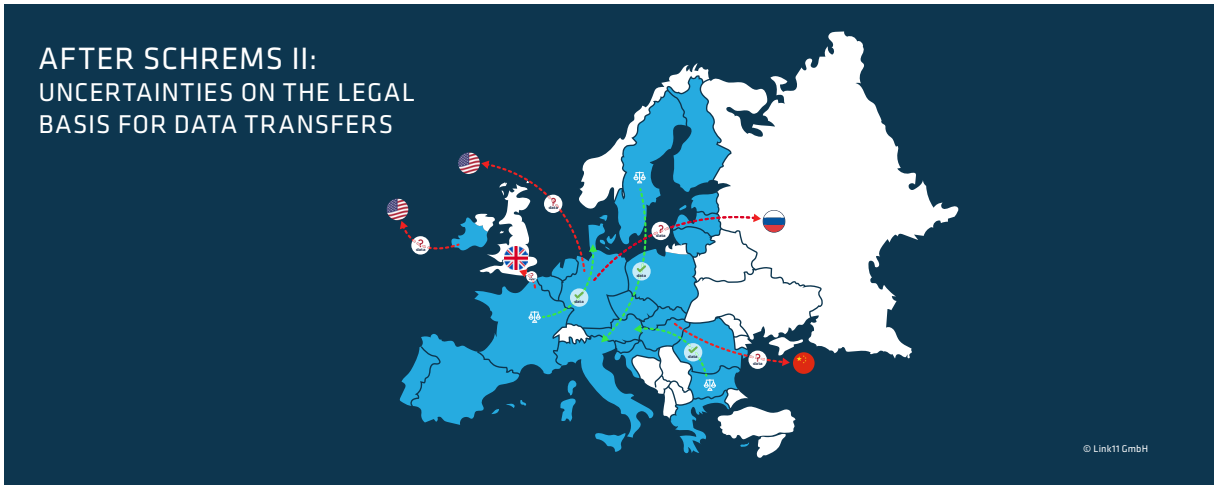
Das bedeutet das Aus zum Privacy Shield für CDN-Anwender

www.link11.com

Das Urteil des EuGHs hinsichtlich des Privacy Shield und der Übertragung personenbezogener Daten in Drittländer kann auch Folgen für Sicherheitslösungen oder CDNs haben.

Der Europäische Gerichtshof („EuGH“) hat mit seiner sogenannten „Schrems II“ Entscheidung am 16. Juli 2020 das EU-US Privacy Shield für unwirksam erklärt. Das wirft ein neues Licht auf die Vertrauenswürdigkeit von CDN-basierten IT-Sicherheitslösungen US-amerikanischer Hersteller und rückt gleichzeitig europäische Anbieter mit hohen Datenschutzstandards in den Vordergrund.

Das ,,Schrems II‘‘-Urteil ist die Fortsetzung des Verfahrens, das der Österreicher Maximilian Schrems vor dem Irish High Court gegen Facebook hinsichtlich der Datenübermittlung in die USA angestoßen hat. Im Jahr 2015 erklärte der EuGH das ,,Safe Harbor‘‘-Abkommen der EU für die Datenübermittlung in die USA für unwirksam. Die EU-Kommission ersetzte daraufhin „Safe Harbor“ durch das EU-US Privacy Shield. Der EuGH kam in „Schrems II“ zu dem Ergebnis, dass der Beschluss der EU-Kommission zum EU-US Privacy Shield unwirksam sei. Es biete kein der EU gleichwertiges Schutzniveau, insbesondere wegen weitreichender staatlicher Zugriffe und wegen mangelnden Rechtsschutzes für Betroffene. Der EuGH fand die Verwendung von Standardvertragsklauseln (SCC) grundsätzlich als Rechtsgrundlage für den Datentransfer außerhalb der EU/EWR ausreichend. Er stellte jedoch klar, dass im Einzelfall zu prüfen sei, ob die SCC im Staat des Datenempfängers tatsächlich eingehalten werden. Bei Datenübermittlungen in die USA reichen SCC ohne zusätzliche Maßnahmen grundsätzlich nicht aus.



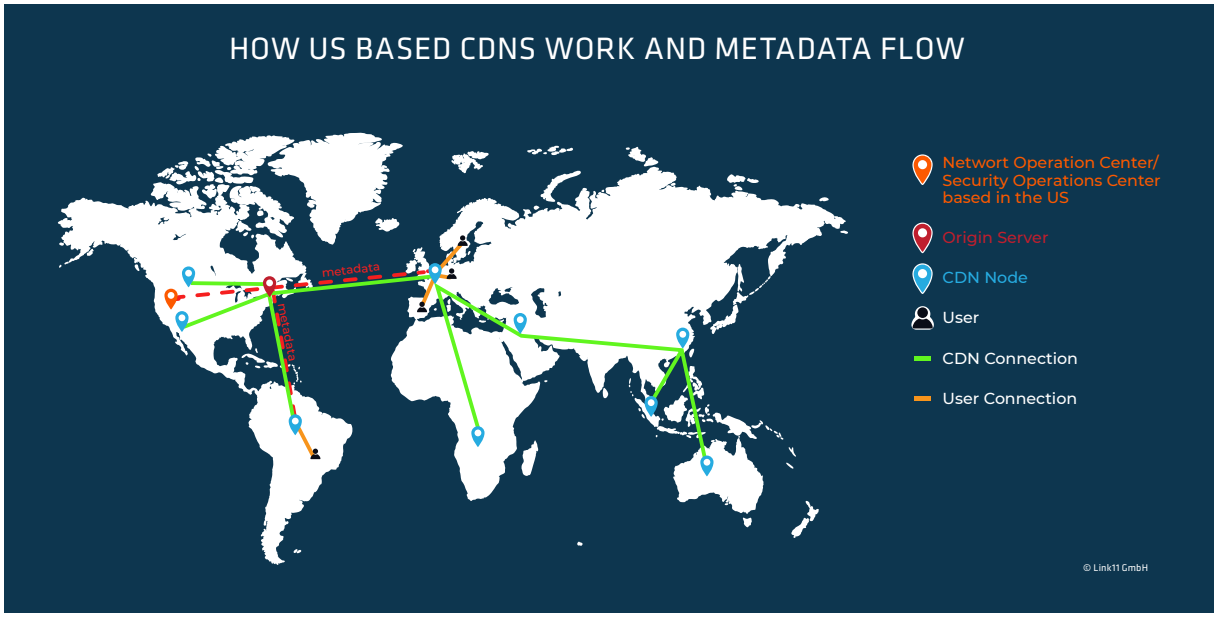
Mit der Entscheidung des Europäischen Gerichtshofs ist in vielen Unternehmen die Rechtsgrundlage für die transatlantische Übermittlung personenbezogener Daten entfallen.

Infolgedessen findet die Datenübertragung in den USA nun in einer rechtlichen Grauzone statt. Denn in der Praxis werden SCCs von den meisten Unternehmen für den Datentransfer ins außereuropäische Ausland genutzt. Vor diesem Hintergrund bedeutet die Schrems II-Entscheidung für Unternehmen eine große Rechtsunsicherheit beim Einsatz diverser Dienste wie etwa Server-Hosting, Anwendungen für Videokonferenzen sowie Online-Marketing- und Webanalyse-Services, z. B. wenn es um die Nutzung von Cloud-basierten Diensten geht.

Schutzlösungen auf CDN-Basis können ebenfalls Daten in die USA übertragen

US-amerikanischen Anbieter von Cyber-Sicherheitsdiensten wie DDoS-Schutz oder Web Application Firewall (WAF) könnten ebenfalls von dem Urteil betroffen sein. Viele dieser Dienste nutzen zur Leistungserbringung ein Content Delivery Networks (CDN) als eine Art Datenautobahn. Diese CDNs wurden vor allem konzipiert, um Daten (insbesondere Medieninhalte) weltweit im Internet via Caching zu verteilen. Ziel ist es, die Ladenzeiten von Webseiteninhalten über Zwischenspeicher zu verkürzen oder Web-Applikationen sicher und schnell in optimaler Qualität auszuliefern. Somit müssen Anfragen nicht vom Original-Server beantwortet werden. Das hilft Lastenspitzen, wie sie durch großvolumige DDoS-Attacken entstehen können, bis zu einem gewissen Level auszugleichen.

CDNs sind komplex und lassen sich nur schwer taktisch an solche weitreichenden regulatorischen Anforderungen wie „Schrems II“ anpassen. Im CDN haben Algorithmen die Kontrolle über die Routenführung und Verbindungsoptimierung, der Anwender selbst kann keinen Einfluss darauf nehmen. Faktoren wie Latenzzeiten, Paketverlustraten und Datendurchsatz sind dabei wichtige Kriterien dafür, wie die Daten ihren Weg zum Nutzer finden. Datenschutzverordnungen spielen dafür keine Rolle. Mit einem Wimpernschlag befindet sich der Datenverkehr schnell auf Überseekabeln bzw. außerhalb der EU-Datenschutzzone. Zudem speichern die Dienste-Anbieter oft Logfiles auf US-amerikanischem Territorium und nutzen sie innerhalb ihres Network Operation Centers (NOC) für weitreichende Optimierungen der eingesetzten Systeme oder zur besseren Einstufung der Bedrohungslage. Darüber hinaus können die wertvollen Metadaten auch in die Arbeit zentral geführter Security Operations Centers (SOC) einfließen. Diese werten sie zur Gefahrenerkennung und Schärfung der relevanten Filter und Schutzmechanismen aus. Allzu oft jedoch befinden sich das NOC und SOC außerhalb der EU, z.B. in den USA. Die daraus resultierende Problematik wurde durch von Eduard Snowden enthüllte Programme wie PRISM und Xkeyscore deutlich.



Im Gegensatz zu dem CDN-basierten Ansatz beim Schutz vor DDoS-Attacken stehen Sicherheitslösungen, die auf eine eigene Schutz-Infrastruktur setzen. Europäische Anbieter, die dieses Konzept verfolgen, unterliegen mit den selbstbetriebenen Filter-Clustern und Netzwerken an allen Standorten den Datenschutzverordnungen ihres Heimatlandes und halten damit die strengen Vorgaben der DSGVO sowie anderer nationaler Regularien ein.

Rechtliche Handlungsempfehlungen

Unternehmen sollten unmittelbar tätig werden, um internationale Datentransfers, also in die USA und in Staaten außerhalb der EU/ EWR mit dem Urteil des EuGHs in Einklang zu bringen. Das Schrems-II Urteil wirkt sich nicht nur auf die Datenübermittlungen in die USA aus, sondern dessen Grundsätze sind auch für sämtliche Übermittlungen außerhalb der EU/ EWR zu berücksichtigen.
Zunächst sollen verantwortliche Unternehmen eine Bestandsaufnahme durchführen und jede Datenübermittlung in ein Drittland, wie z.B. USA, identifizieren. Mit Blick auf den Ablauf der Brexit-Übergangsperiode am 31. Dezember 2020 sind auch Übermittlungen in die UK zu untersuchen.

Dann ist die Rechtsgrundlage für die internationale Datenübermittlung zu prüfen. Welche Daten werden zu welchem Zweck übermittelt? Wie sind diese Daten im Transit und am Zielort geschützt? Datentransfers auf Grundlage des Privacy Shields sollten eingestellt, mit zusätzlichen Maßnahmen versehen oder auf eine andere Rechtsgrundlage gestützt werden.

Nach der Bestandsaufnahme ist das Risiko für die Datenübermittlung zu analysieren. Wie ist die Rechtslage im Drittland? Können Behörden oder Regierung im Zielland auf die Personendaten zugreifen? Werden die Rechte der Betroffenen wirksam gewährleistet? Welche technischen Maßnahmen werden ergriffen, um die übermittelten Daten zu schützen? Anschließend ist die Risikoanalyse zu dokumentieren.

Werden SCC als Rechtsgrundlage für die Datenübermittlung verwendet, ist im Einzelfall zu prüfen, ob das Drittland ein der EU gleichwertiges Schutzniveau bietet, z.B. durch Transparenz, technische Maßnahmen, Rechtsschutz. Wenn das Schutzniveau nicht ausreichend ist, müssen zusätzliche Maßnahmen getroffen werden, z.B. (stärkere) Verschlüsselung oder Anonymisierung, vertragliche Beobachtungs- und Mitteilungspflichten.

Neben den SCC können auch Binding Corporate Rules oder Ausnahmen nach Art. 49 DSGVO, z.B. Einwilligungen der betroffenen Personen, zur Anwendung kommen.

Zudem ist zu erwägen, ob eine Datenverarbeitung nur innerhalb der EU/EWR in Betracht kommt oder nur im sicheren Drittland erfolgt. Ein sicheres Drittland ist ein Land außerhalb der EU/ EWR, für die ein Angemessenheitsbeschluss der EU vorliegt, z.B. Andorra, Argentinien, Kanada (nur Handelsorganisation), Israel, Isle of Man, Japan, Jersey, Schweiz.

Auch bei CDNs beispielsweise ist sicherzustellen, dass eine Übermittlung von personenbezogenen Daten außerhalb der EU/ EWR rechtmäßig ist. Die internationalen Datenübermittlungen sind samt Rechtsgrundlage zu identifizieren. Der Verantwortliche muss im Einzelfall eine Risikoanalyse für die Datenübermittlung durchführen und die Analyse dokumentieren. Dann ist zu erwägen, welche wirksame Rechtsgrundlage für die Datenübermittlungen besteht bzw. wo Anpassungen erforderlich sind.

Personenbezogene Daten in sicheren Händen

Unternehmen, die auf Nummer sicher gehen möchte, sollten ihre Daten und IT-Sicherheit einem Anbieter aus Deutschland bzw. Europa anvertrauen und damit eine Datenübertragung in die USA von vornherein ausschließen. Die strengen Vorgaben des europäischen und des deutschen Gesetzgebers zum Datenschutz und der Datensicherheit bieten die erforderliche Sicherheit für eine Datenübermittlung. Meist wird dadurch auch die Einhaltung von Compliance-Anforderungen erleichtert. Sicherheitshalber sollte man einen Dienstleister ohne Niederlassung in den USA wählen, um einen etwaigen Zugriff der US-Niederlassung auszuschließen. Bei einem EU-Anbieter ohne US-Niederlassungen sind neben rechtlichen Aspekten auch technologische Vorteile verbunden. Zudem verfügen sie über eine umfassende und profunde Kenntnis des europäischen Marktes sowie der Bedürfnisse ihrer europäischen Kunden.

Autoren:

Anne Baranowski, LL.M. Rechtsanwältin, Schalast Rechtsanwälte Notare
Michael Hempe, Regional Sales Director, Link11 GmbH

Über Link11

Link11 ist der im Bereich Cyber-Resilienz führende europäische IT-Sicherheitsanbieter. Die globalen Schutzlösungen der Cloud Security Plattform sind vollständig automatisiert, reagieren in Echtzeit und wehren alle Angriffe, so auch unbekannte und neue Muster, in unter 10 Sekunden ab. Link11 bietet laut einhelliger Analysten-Meinung (Gartner, Frost & Sullivan) die schnellste Mitigation (TTM), die auf dem Markt verfügbar ist. Um Cyber-Resilienz zu gewährleisten, sorgen u.a. Web- und Infrastruktur-DDoS-Schutz, BOT-Management, API-Schutz, Secure-DNS, Zero-Touch-WAF, Secure-CDN bis hin zu Threat-Intelligence-Services für eine ganzheitliche und Plattform-übergreifende Härtung der Netzwerke und kritischer Anwendungen von Unternehmen. Die internationalen Kunden können sich so auf ihr Geschäft und digitales Wachstum konzentrieren. Seit der Gründung des Unternehmens im Jahr 2005 wurde Link11 mehrfach für seine innovativen Lösungen ausgezeichnet.

Link11 GmbH

Lindleystraße 12
Germany
+49 (0)69 – 264929777
info@link11.com