Der zerbrochene Schild

Was Unternehmen nach dem Privacy-Shield-Urteil beachten müssen

Ein Whitepaper der Open Source Business Alliance

von Henriette Baumann

Am 16. Juli 2020 gab der Europäische Gerichtshof dem österreichischen Juristen Max Schrems Recht und kippte das Privacy-Shield-Datenschutzabkommen zwischen der EU und den USA. Der EU-US Privacy Shield bildete eine Rechtsgrundlage für Datenübermittlungen aus der EU[1] in die USA und wurde mit diesem Urteil mit sofortiger Wirkung für ungültig erklärt. Begründet hat der Europäische Gerichtshof das Urteil mit den weitreichenden Überwachungsmöglichkeiten von US-amerikanischen Behörden bei gleichzeitig ungenügenden Rechtsbehelfen für betroffene Personen in der EU. Gemessen an der EU-Grundrechte-Charta wurden die staatlichen Überwachungsmaßnahmen der USA als unverhältnismäßig eingestuft. Für den Schutz der persönlichen Daten und der digitalen Souveränität jedes einzelnen Bürgers wurde damit ein Erfolg erzielt. Aber welche Konsequenzen hat das Urteil für Unternehmen, speziell in Hinblick auf den Umgang mit personenbezogenen Daten?

1 Die Ausführungen gelten gleichermaßen für die EWR-Staaten Norwegen, Island und Liechtenstein.

Inhalt

Hintergrund

Ob in einem Drittland ein angemessener Datenschutz gewährleistet ist, stellt die EU-Kommission anhand eines sogenannten "Angemessenheitsbeschlusses" fest. Solche Drittländer sind etwa Andorra, Argentinien, Kanada, die Färöer-Inseln, Guernsey, Israel, die Isle of Man, Japan, Jersey, Neuseeland, die Schweiz und Uruguay. Die vollständige Liste der Länder mit Angemessenheitsbeschluss findet sich auf der Website der Europäischen Kommission (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en). Mit diesen Ländern darf ein Datenaustausch erfolgen, als wären sie Teile der EU.

Die USA fehlen jedoch auf dieser Liste. Für die Vereinigten Staaten erstellte die EU-Kommission deshalb im Jahr 2016 das "EU-US Privacy Shield"-Abkommen als Folge des vom Europäischen Gerichtshof 2015 für unwirksam erklärten Safe-Harbor-Abkommen, das ebenfalls auf dem Klageweg durch Max Schrems gestürzt wurde. Der Nachfolger Privacy Shield definierte einen angemessenen Datenschutz in den USA nur dann als gegeben, wenn sich die amerikanischen Verarbeiter von Personendaten per Selbstdeklaration dem Abkommen unterwerfen.

Privacy Shield beinhaltet Datenschutzgrundsätze, zu denen sich US-amerikanische Unternehmen verpflichten konnten, indem sie sich auf der Website des US-Handelsministeriums in eine Liste eintragen ließen (https://www.privacyshield.gov/list). Bis zum Urteil des Europäischen Gerichtshofs (EuGH) von 16. Juli 2020 war mit diesen Regeln ein Datentransfer in die USA wie innerhalb der EU möglich. Das EU-US Privacy Shield

bildete die Rechtsgrundlage für Datenübermittlungen aus der EU in die USA, doch das Urteil hat den EU-US Privacy Shield für unwirksam erklärt.

Begründet hat der EuGH das Urteil mit den weitreichenden Überwachungsmöglichkeiten von US-amerikanischen Behörden bei gleichzeitig ungenügenden Rechtsbehelfen für betroffene Personen in der EU. Gemessen an der EU-Grundrechte Charta wurden die staatlichen Überwachungsmaßnahmen der USA als unverhältnismäßig eingestuft.

Damit fallen US-amerikanische Cloud-Anbieter und Anbieter elektronischer Kommunikationsdienste wie zum Beispiel Apple, AT&T, Amazon AWS, Dropbox, Microsoft, Facebook, Google, Yahoo und Verizon unter FISA 702. Ob ein US-Anbieter unter FISA 702 fällt, kann man direkt beim Anbieter erfragen.

Mit dem Urteil des Europäischen Gerichtshofes fällt die USA zurück in den Status eines Drittlandes ohne Angemessenheitsbeschluss wie beispielsweise Indien, China, Russland oder möglicherweise auch das Vereinigte Königreich nach einem ungeregelten Brexit. Betrachtet man die engen Verflechtungen zwischen der EU und den USA und die stetig ansteigenden Datenübermittlungen nicht nur aber auch in US-Cloud-Dienste, Google oder Facebook, handelt es sich also um eine sehr weitreichende Entscheidung des EuGH.

Glossar: Foreign Intelligence Surveillance Act FISA

Section 702 des US-Geheimdienstgesetzes FISA erlaubt Geheimdiensten wie der NSA, ohne konkreten Verdacht und ohne entsprechenden Gerichtsbeschluss weitreichende Zugriffe auf Daten von Ausländern ("non-US persons"), die von US-amerikanischen Unternehmen wie beispielsweise Google und Telekommunikationsanbietern erhoben wurden, auszuwerten. Danach dürfte die gesamte elektronische Kommunikation von und zur Zielperson sowie über die Zielperson abgefangen werden. Voraussetzung ist die die Relevanz für Ermittlungen zur Terrorismusabwehr. Es erfolgt keine Einschränkung der Art der Daten, daher können beispielsweise auch Finanzdaten erfasst werden.

Unter dieses Massenüberwachungsgesetz fallen US-amerikanische (Zitat in Originalsprache):

"electronic communication service provider:

A) telecommunications carrier

B) provider of electronic communication service

C) provider of a remote computing service

D) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored

E) an officer, employee, or agent of an entity described in A), B), C) or D)“

Der Privacy Shield bildet jedoch nicht die einzige Rechtsgrundlage für Datenübertragung in die USA, die DSGVO bietet weitere Möglichkeiten für einen rechtskonformen Datentransfer in Drittländer ohne Angemessenheitsbeschluss. Für die Datenübermittlung in die USA bedeutet das, dass seit dem 16. Juli 2020 jede Übertragung daraufhin geprüft werden muss, ob eine andere gültige Rechtsgrundlage als der Privacy Shield vorliegt, so wie dies für alle anderen Drittländer ohne Angemessenheitsbeschluss auch vor dem Urteil erforderlich war und ist.

Welche Daten sind in welcher Form betroffen?

Täglich werden heute riesige Mengen personenbezogener Daten aus der EU an die USA übermittelt, nicht nur in multinationalen Konzernen. Auch kleinere Unternehmen speichern immer häufiger Daten in der Cloud, setzen Software US-amerikanischer Anbieter ein und bei der Kommunikation auf die großen Anbieter von sozialen Netzwerken. Webkonferenzsysteme wie Zoom oder Microsoft Teams, Sprachdienste von Amazon und Apple oder auch die Cookies und Tracker der Dienste zur Webseitenanalyse wie Google Analytics finden sich allerortens. Mit den Konsequenzen des Urteils beschäftigen muss sich deshalb jedes in der EU ansässige Unternehmen, das personenbezogene Daten von Kunden, Partnern, Mitarbeitern, Lieferanten, Websitebesuchern oder sonstigen Personen in Drittländer übermittelt.

Die Verarbeitung personenbezogener Daten umfasst alle Vorgänge wie das Erheben, Erfassen, Ordnen, Speichern, Anpassen, Verändern, Auslesen, Abfragen, Offenlegen durch Übermittlung, Verbreitung, Abgleich, Verknüpfung, Einschränkung, Löschung oder Vernichtung. Es spielt also nicht nur eine Rolle, wo die Daten

gespeichert sind, sondern auch, wo weitere Verarbeitung stattfindet. Datenübermittlung umfasst nicht nur den physischen „Export“ der Daten. Auch jede Zugriffsmöglichkeit aus Drittländern beispielsweise über Schnittstellen, Abrufmöglichkeiten oder Fernwartungszugänge sind ebenfalls als Datenübermittlung in ein Drittland zu sehen. Unternehmen, die aufgrund des Privacy-Shield-Urteils eine Bestandsaufnahme ihrer Datenübermittlungen in Drittländer durchführen, müssen also nicht nur ihre Datenbestände analysieren, sondern auch alle stattfindenden Verarbeitungen.

Es gibt Cloud-Anwendungen, die Daten in der EU speichern, spezifische Verarbeitungen hingegen nach wie vor in den USA durchführen. Auch die Auslagerung von Datenverarbeitungen an ein US-Unternehmen, der konzerninterne Datentransfer an eine US-Muttergesellschaft, der Zugriff von US-Mutterkonzernen auf Daten von Konzerngesellschaften innerhalb der EU und die Nutzung von US-Cloud-Diensten wie Google Cloud oder Amazon AWS sind betroffen.

Nicht zu unterschätzen sind Verarbeitungen sensibler Daten und Betriebsgeheimnisse wie Techniken, Rezepturen, Patentanmeldungen, Marktstrategien, Finanzdaten, Entwicklungs- und Forschungsdaten. Diese Inhalte fallen zwar – sofern nicht personenbezogen – nicht unter das Datenschutzgesetz und sind vom EuGH-Urteil nicht betroffen.

Allerdings sollte ein Unternehmen diese Datenbestände in die Analysen mit einbeziehen und – je nach Wirtschaftszweig und Unternehmenstätigkeit – das Risiko bewerten, inwieweit ein nicht ausreichendes Datenschutzniveau und weitreichende Überwachungs- und Zugriffsmöglichkeiten im Drittland dem Unternehmen schädlich werden können. Insbesondere Betreiber kritischer Infrastrukturen sehen sich hier größeren Herausforderungen ausgesetzt.

Was ist zu tun?

Weil der Europäische Gerichtshof keine Übergangs- oder Schonfrist eingeräumt hat, müssen Unternehmen möglichst zeitnah mit ersten Maßnahmen beginnen und diese Aktivitäten nachweisen können.

Analyse der Datenübermittlungen

Im ersten Schritt sollten alle Datenflüsse in die USA und weitere Drittländer geprüft werden. Das umfasst auch Zugriffsmöglichkeiten durch Dritte, die Verarbeitungen bei Auftragnehmern (Subunternehmen) und die Weitergabe von Daten durch einen Auftragnehmer. Transparenz ist hier das oberste Gebot. Als verantwortliches Unternehmen ist man dabei in der Pflicht, die Situation beim Dienstleister bzw. Subunternehmen aufzunehmen. Die Non-Profit-Organisation NOYB (Europäisches Zentrum für digitale Rechte, www.noyb.eu) hat dafür Musterfragebögen zur Verfügung gestellt. Dabei ist man darauf angewiesen, dass Dienstleister, Hersteller und Subunternehmen ihrer Informationspflicht vollumfänglich nachkommen und sämtliche Verarbeitungen offenlegen. Nach dieser Bestandsaufnahme sollte für jede Datenübermittlung die Rechtsgrundlage bestimmt werden. Im folgenden zeigen wir die für Unternehmen wesentlichen Rechtsgrundlagen, Garantien und Maßnahmen auf.

Gelegentliche notwendige Datenübermittlung

Der EuGH hat ausdrücklich betont, dass durch die Aufhebung des EU-US Privacy Shield kein Rechtsvakuum entsteht, da unbedingt notwendige, gelegentliche Datenübermittlungen zur Erfüllung vertraglicher Leistungspflichten weiterhin stattfinden können. Diese Ausnahmen sind unter Art. 49 Abs. 1 DSGVO aufgeführt und umfassen beispielsweise Datenübermittlungen zur Vertragserfüllung wie Reisebuchungen, Kauf von Waren bei einem US-amerikanischen Unternehmen oder die Ausführung eines Zahlungsauftrags. Dies kann für Unternehmen zutreffen, die keine regelmäßigen Datenübermittlungen in die USA durchführen, sondern nur punktuell zur Erfüllung eines Vertrags Personendaten in die USA transferieren.

Für Datenübermittlungen in die USA, die nicht unter die Ausnahmen aus Art. 49 DSGVO fallen, stehen mehrere rechtliche und technische Instrumente zur Verfügung, um die Datenübermittlungen rechtskonform zu gestalten.

Einholen einer Einwilligung

Grundsätzlich besteht die Möglichkeit, eine Einwilligung derjenigen Personen einzuholen, deren Daten in die USA übermittelt werden. Diese Option wird von den meisten Unternehmen erst dann eingesetzt, wenn sich keine anderen Rechtsgrundlagen eignen. Dafür gibt es zwei Gründe: Nicht jedes Unternehmen möchte seine Kunden, Mitarbeiter oder Partner klar und deutlich darüber informieren, dass deren Daten in einem Drittland verarbeitet werden, in dem kein adäquater Datenschutz gewährleistet werden kann. Zudem kann eine solche Einwilligung jederzeit widerrufen werden, was dann letztlich bedeuten würde, dass das Unternehmen den Datentransfer derjenigen Personen, die ihre Einwilligung widerrufen, sofort stoppen müsste.

Anonymisierung

Die Anonymisierung vor der Datenübermittlung in die USA ist eine weitere Möglichkeit der rechtskonformen Übermittlung. Durch die Anonymisierung ist eine Identifikation von Personen durch den Empfänger nicht mehr möglich, die Persönlichkeitsrechte werden gewahrt und die Datenübermittlung unterliegt nicht mehr dem Datenschutzgesetz. Das Fehlen des Personenbezugs kann Funktionalitäten einschränken und ist daher nicht in jedem Fall möglich. Das Anonymisierungsverfahren muss eine Re-Identifizierung ausschließen.

Anwendung von Standarddatenschutzklauseln

Nach Feststellung des Europäischen Gerichtshofes sind die EU-Standarddatenschutzklauseln für die USA nur noch bedingt verwendbar. Mit Standarddatenschutzklauseln lassen sich Vertragspartner in Drittländern vertraglich verpflichten, das Datenschutzniveau der EU sicherzustellen. Allerdings nur, wenn es im Drittland kein kollidierendes Recht gibt. Folgerichtig ist in einer Einzelprüfung vom verantwortlichen Unternehmen in der EU (EU-Datenexporteur) zu überprüfen, ob die in den EU-Standarddatenschutzklauseln enthaltenen vertraglichen Verpflichtungen für seine Datenübermittlung auch tatsächlich umgesetzt werden können. Für die meisten Unternehmen in den USA ist dies gemäß der Feststellung des EuGH nicht der Fall: Die meisten US-Clouds wie Apple, Google, Amazon AWS, Dropbox, Facebook, Microsoft fallen unter das US Geheimdienstgesetz Foreign Intelligence Surveillance Act (FISA 702 – siehe Kasten).

Glossar: Standarddatenschutzklauseln

Standarddatenschutzklauseln sind von der EU-Kommission genehmigte Vertragsklauseln, die sich unverändert in das Vertragswerk der Vertragspartner (Datenexporteur in der EU/EWR und Datenimporteur in einem Drittland ohne angemessenen Datenschutz) einbinden lassen. Mit ihnen verpflichtet sich der Datenimporteur im Drittland, ein Schutzniveau sicherzustellen, das dem der EU entspricht. Auch nach dem EuGH-Urteil sind Standarddatenschutzklauseln eine zulässige Grundlage für die Datenübermittlung in Drittländer.

Der Europäische Gerichtshof hat in seinem Urteil jedoch darauf hingewiesen, dass der Verantwortliche im Einzelfall prüfen muss, ob mit den vertraglichen Regelungen unter Nutzung der Standarddatenschutzklauseln tatsächlich sichergestellt werden kann, dass das Schutzniveau für personenbezogene Daten tatsächlich dem in der EU entspricht.

Es reicht also nicht mehr aus, diese Vertragsklauseln einfach in einen Dienstleistungsvertrag hinein zu kopieren. Vielmehr hat der Verantwortliche im Einzelfall das tatsächliche Datenschutzniveau zu prüfen und ggf. zusätzliche Maßnahmen zu ergreifen.

Der Standort der Server ist dabei irrelevant. Setzen US-Unternehmen für den Betrieb von Servern Tochterunternehmen in der EU ein, so muss auch in diesem Fall in einer Einzelfallprüfung belegt werden, dass die US-Muttergesellschaft keinen Zugriff auf die Daten in der EU hat. Da diese Beschränkung die US-Unternehmen in ihrem Geschäftsmodell beschneidet und technisch häufig noch nicht umgesetzt wird (denn alle Verarbeitungsformen sind betroffen, nicht nur die Speicherung der Daten), kann man nicht von einer Rechtskonformität bei EU-Tochtergesellschaften von US-Unternehmen ohne Einzelfallprüfung ausgehen.

Ergibt die Einzelfallprüfung, dass die EU-Standarddatenschutzklauseln keine ausreichende Garantie darstellen, um ein angemessenes Datenschutzniveau zu gewährleisten, muss das verantwortliche Unternehmen zusätzliche Garantien bieten.

Eine mögliche und von Aufsichtsbehörden empfohlene Maßnahme wäre die Verschlüsselung der Daten, welche nach den Prinzipien BYOK (bring your own key) und BYOE (bring your own encryption) umgesetzt ist, sodass der Dienstleister oder andere Akteure keine Möglichkeit haben, die Daten zu entschlüsseln. Allerdings sind viele US-Dienste mit verschlüsselten Daten in ihrer Funktion nur eingeschränkt nutzbar, etwa bei Suchalgorithmen oder Analysefunktionen.

Eine alternative Maßnahme wären ergänzende vertragliche Bestimmungen, die zusätzlich zu den Standarddatenschutzklauseln den Datenimporteur in den USA oder einem anderen Drittland noch strenger zur Einhaltung des Datenschutzes verpflichten. Solch ergänzende Bestimmungen benötigen meist wegen der Genehmigungsvorgabe eine Vorlaufzeit und unterliegen den gleichen Anforderungen an die Einzelfallprüfung wie die Standarddatenschutzklauseln. Deshalb stellen sie für kleine und mittlere Unternehmen meist keine Alternative dar. Vertragliche Regelungen zwischen Datenexporteur und US-Datenimporteur können US-Behörden zudem nicht binden. Unternehmen, die individuelle Verträge mit US-amerikanischen Partnern schließen, müssen damit rechnen, dass bei einer behördlichen Überprüfung der Datentransfer verboten werden kann.

Binding Corporate Rules

Bei Binding Corporate Rules handelt es sich um verbindliche, von der Aufsichtsbehörde genehmigte unternehmensinterne Datenschutzvorschriften, die für alle Mitglieder einer Unternehmensgruppe gelten und nachweisbar durchgesetzt werden. Mit verbindlichen internen Datenschutzvorschriften (Binding Corporate Rules) können sich Unternehmensgruppen zur Sicherstellung eines dem EU-Niveau entsprechenden Datenschutz verpflichten.

Die Möglichkeit geeigneter Garantien durch Bindung Corporate Rules steht nur Unternehmensgruppen oder einer Gruppe von Unternehmen offen. Abgedeckt sind dabei Datenübermittlungen zwischen den Unternehmen der Gruppe. Für Datenübermittlungen an gruppenfremde Dritte bilden Binding Corporate Rules keine geeignete Garantie. Binding Corporate Rules stehen unter einem Genehmigungsvorbehalt durch die zuständige Aufsichtsbehörde.

Glossar: CLOUD Act

Der CLOUD Act (**C**larifying **L**awful **O**verseas **U**se of **D**ata Act) von 2018 hat entgegen seines Namens nicht zwingend etwas mit Clouds zu tun. Er betrifft anders gelagerte Sachverhalte als FISA. Im Gegensatz zu nachrichtendienstlicher Überwachung wird die Erhebung von elektronischen Beweismitteln für Strafverfahren geregelt. Darauf gestützt werden können strafverfahrensrechtliche Durchsuchungs- und Beschlagnahmungsbeschlüsse einer US-Behörde zur Herausgabe von Daten als Beweismittel, auch wenn diese außerhalb des US-Territoriums gespeichert sind.

Der CLOUD Act verpflichtet US-Unternehmen selbst dann zur Datenherausgabe, wenn lokale Gesetze am Ort des Datenspeichers dies verbieten. Der übliche Weg eines Rechtshilfeersuchens auf Basis von Rechtshilfeabkommen ist aus US-Sicht nach dem CLOUD Act nicht mehr erforderlich - was im Konflikt mit dem Recht der EU und ihrer Mitgliedsstaaten steht.

Auch diese Möglichkeit unterliegt einer Einzelfallprüfung und ist beim Datentransfer in die USA aus den oben bereits genannten Gründen zumeist nicht mehr ausreichend. Wegen der Genehmigungsvorgabe benötigen auch Binding Corporate Rules eine Vorlaufzeit und unterliegen letztlich denselben Anforderungen an die Einzelfallprüfung wie die Standarddatenschutzklauseln.

Alternativen

Kann keine der geeigneten Garantien und Maßnahmen angewendet werden, ist die Datenübermittlung in die USA unzulässig. Gemäß den Leitlinien der Aufsichtsbehörden muss die Datenübermittlung mit sofortiger Wirkung gestoppt werden. Werden Auftragsverarbeiter eingesetzt, so müssen diese angewiesen werden, die Übermittlung personenbezogener Daten mit sofortiger Wirkung auszusetzen. Wird beabsichtigt, die Datenübermittlungen weiterhin durchzuführen, muss das Unternehmen dies der zuständigen Aufsichtsbehörde mitteilen.

Grundsätzlich sollten Datenverarbeitungen von Diensten aus den USA dahingehend untersucht werden, ob sie notwendig sind und tatsächlich in Anspruch genommen werden müssen. In vielen Fällen haben Unternehmen US-Anbieter gewählt, ohne die Auswirkungen zu berücksichtigen und ohne gleichwertige datenschutzkonforme Alternativanbieter in die Evaluation einzubeziehen.

Das Zurückholen der Daten in die EU oder ein Drittland mit Angemessenheitsbeschluss ist ein sicherer und nachhaltiger Weg, den zeitaufwändigen Maßnahmen für die rechtskonforme Verarbeitungen in Drittländern zu vermeiden. Wer auf der sicheren Seite sein und Stabilität in seine Datenübermittlungen und Verarbeitungen bekommen möchte, sollte das Zurückholen der Daten in Erwägung ziehen. Die Berliner Beauftragte für den Datenschutz fordert die Unternehmen auf, zu Dienstleistern in der EU oder in einem Land mit angemessenem Datenschutzniveau zu wechseln.

Aber selbst dann ist Vorsicht geboten. Auch europäische Anbieter können US-amerikanische Dienstleister als Subunternehmen in ihr Angebot einbinden oder personenbezogene Daten an Dritte in den USA übermitteln . Als Unternehmen mit Sitz in der EU müssen Sie dies im Rahmen der Transparenz- und Informationspflichten offenlegen. Eine Überprüfung ist bei proprietären Closed Source Anbietern im Regelfall nicht möglich. Eine vollumfängliche Kontrollmöglichkeit bieten Open Source Lösungen.

Open Source Software – eine gute Alternative

Open Source Software bietet durch den offengelegten Quellcode maximale Transparenz und Kontrollfähigkeit. So lässt sich prüfen und sicherstellen, dass keine rechtswidrigen Datenabflüsse erfolgen und die Daten nur für die zulässigen Zwecke verarbeitet werden.

Diese Transparenz und Nachvollziehbarkeit greift gleichermaßen für Inhouse-betriebene Systeme (On Premises) wie auch für Open-Source-Anwendungen in der Cloud. Meist gibt es für jede Open-Source-Anwendung mehrere Hosting- oder Cloud-Anbieter, aus denen Unternehmen auswählen und sich so für den Betrieb in der EU oder einem Drittland mit Angemessenheitsbeschluss entscheiden und den Anbieter gegebenenfalls sogar wechseln können. Der Nutzer kann selbst prüfen, einschätzen und entscheiden, wo und wie seine Daten verarbeitet werden. Open Source Software ist damit eine wesentliche Grundlage für eine rechtskonforme IT-Firmenlandschaft.

Transparenz ist Pflicht

Vollständige und transparente Information über die sowohl innerhalb des Unternehmens stattfindenden aber auch der ausgelagerten Verarbeitungen, ist eine wesentliche Grundlage für die Compliance. Wie der Datenschutz steht auch Open Source für das Prinzip der Transparenz, ein in der DSGVO verbürgtes Recht. Jede Person muss nachvollziehen können, wie die Personendaten verarbeitet werden. Nur mit diesem Wissen ist eine selbstbestimmte Entscheidung und die Kontrolle der Datennutzung möglich. Unternehmen sind verpflichtet, das Einhalten der gesetzlichen Vorgaben zu überprüfen und im Rahmen der Rechenschaftspflicht nachzuweisen. Die Beherrschbarkeit und Rechtmäßigkeit einer Datenverarbeitung setzt voraus, dass transparent ist, welche Daten in welcher Weise verarbeitet werden.

Bei Open Source Softwarelösungen ist der Quellcode frei zugänglich – jedermann kann einsehen und prüfen, wie Daten verarbeitet werden. Nun ist ja nicht jeder Bürger ein gewiefter Programmierer, daher werden diese Prüfungen im Regelfall von beauftragten oder aus eigener Initiative handelnden Spezialisten vorgenommen, die genauso Zugang zum Quellcode haben wie die betroffenen Personen und die ihre Prüfungen veröffentlichen, um so die gemeinsam genutzten Werkzeuge verbessern zu helfen. Das bedeutet, es gibt keine verborgenen Räume und Türen in der Software, die nicht offengelegt werden können. Anders ist das bei proprietärer (Closed Source) Software, wo der Hersteller den Zugang zum Quellcode verwehrt. Ein Unternehmen, das proprietäre Closed Source Software einsetzt oder auch nur in der Cloud nutzt, mag zwar seiner Informationspflicht nachkommen – überprüfbar ist das allerdings nicht.

Open Source erlaubt es verantwortlichen Unternehmen viel weitgehender, die notwendigen Einschätzungen vorzunehmen. Selbst oder mit Hilfe von Experten lassen sich Datenverarbeitungen bis auf die Ebene des Quellcodes prüfen und sicherstellen, dass keine rechtswidrigen Datenabflüsse stattfinden und die Daten nur entsprechend der zulässigen Zwecke verarbeitet werden. Die umfassende Transparenz und die absolute Kontrollmöglichkeit schaffen Vertrauen und Wettbewerbsvorteile – umso mehr, je breiter die Sensibilisierung in der Bevölkerung fortschreitet und je stärker die Forderung nach digitaler Souveränität wird.

Keine gute Idee: Das Urteil ignorieren

Der Europäische Gerichtshof hat keine Übergangs- bzw. Schonfrist eingeräumt und die Datenschutzbehörden ausdrücklich in die Pflicht genommen, Datenübermittlungen auszusetzen oder zu verbieten, sollte eine gültige Rechtsgrundlage fehlen. Gemeinnützige Organisationen, Betriebsräte und auch Nutzer können Beschwerden oder Klagen einreichen und Schadenersatz für unzulässige Datenexporte verlangen, was auch immaterielle Schäden umfassen kann.

Die DSGVO sieht Bußgelder vor, sollten weiterhin Daten ohne ein gültiges Rechtsinstrument übermittelt werden (Artikel 83 Absatz 5 Buchstabe c) DSGVO). Aufsichtsbehörden können einen Datentransfer mit sofortiger Wirkung untersagen.

Der Landesdatenschutzbeauftragte in Baden-Württemberg hat publiziert, dass seine Behörde einen Datentransfer nicht untersagt, wenn belegt werden kann, dass der genutzte US-Dienstleister bzw. Vertragspartner kurz- und mittelfristig unersetzlich ist durch einen Dienstleister bzw. Vertragspartner ohne Datentransferproblematik, also beispielsweise aus der EU oder einem Drittland mit Angemessenheitsbeschluss. Im Zentrum dieser Beurteilung steht also die Frage, ob das verantwortliche Unternehmen zumutbare rechtskonforme Alternativangebote gehabt hätte. Hier ist anzumerken, dass der Landesdatenschutzbeauftragte Baden-Württemberg seine Position laufend überprüft und daher zu einem späteren Zeitpunkt zu einer anderen Einschätzung kommen kann.

Die wichtigsten Dos und Dont`s

In der Realität unternehmen viele Unternehmen nur unzureichende Anstrengungen, um die Software- und Service-Lieferkette nachzuvollziehen. Erst im Zuge von Datenschutz-Analysen stellt man fest, dass Daten in Ländern und Unternehmen ohne angemessenen Datenschutz verarbeitet werden, was den Verantwortlichen im Unternehmen bis dahin nicht bekannt war.

Ein Unternehmen ist jedoch für die rechtskonforme Verarbeitung aller personenbezogenen Daten im eigenen Unternehmen wie auch bei Auftragsverarbeitern verantwortlich, haftbar, auskunfts- und rechenschaftspflichtig. Gegenüber betroffenen Personen, Auftraggebern oder Aufsichtsbehörden muss lückenlos angegeben werden können, wo welche Verarbeitungen durchgeführt werden und wer die jeweiligen Empfänger der Daten sind.

Don't:

- X Keine Auslagerung von Verarbeitungen, Nutzung von Cloud-Services oder sonstigem Outsourcing ohne "Durchblick" – immer auf Klarheit, Transparenz und Nachvollziehbarkeit achten. Kein Einsatz von IT-Services, Cloud-Services etc. ohne vorherige Prüfung des Dienstleisters, wozu transparente Informationen über den Dienstleister und dessen Leistungen zwingend notwendig sind.
- X Kein Einsatz von IT-Services und Cloud-Services von Anbietern aus Drittländern ohne vorherige Prüfung der Rechtsgrundlagen und zusätzlich erforderlichen Maßnahmen.
- X Kein Einkauf von Software-Services, Cloud-Leistungen etc. ohne vertragliche Verpflichtung der Auftragnehmer zur Einhaltung des erforderlichen Datenschutzniveaus.

Do:

- √ Überblick über alle Datenströme und die Betriebsstandorte der Datenverarbeitung verschaffen. Das ist nicht nur für den Datenschutz relevant, sondern auch für die IT-Sicherheit, die Betriebssicherheit sowie Wartung und Support.
- √ EU-Unternehmen müssen sich über die Rechtslage des Dienstleisters in einem Drittland ohne angemessenes Datenschutzniveau informieren. Die Non-Profit-Organisation NOYB (Europäisches Zentrum für digitale Rechte, www.noyb.eu) hat dafür Musterfragebögen zur Verfügung gestellt.
- √ Subunternehmen ebenfalls darauf prüfen – und vertraglich oder durch andere Maßnahmen verpflichten.
- √ Für jede Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau Rechtsgrundlage, Garantien und Maßnahmen bestimmen.
- √ Bei der Auswahl neuer IT-Services und Software auf grösstmögliche Transparenz und Prüfbarkeit achten, damit keine rechtswidrigen Datenabflüsse in Drittländer erfolgt und die Daten nur für die zulässigen Zwecke verarbeitet werden.
- √ Bei jedem Entwicklungsprozess – ob IT-Systeme, Produkte oder Dienstleistungen, frühzeitig einen Experten aus den Bereichen Datenschutz und IT-Sicherheit hinzuziehen. Der Aufwand dafür ist vergleichsweise gering im Vergleich zu Maßnahmen, die bei Fehlentwicklungen ergriffen werden müssen.
- √ Die Berliner Beauftragte für den Datenschutz fordert die Unternehmen auf, zu Dienstleistern in der EU oder in ein Land mit angemessenem Datenschutzniveau zu wechseln.

Informationen zum Whitepaper

Zur Autorin

Henriette Baumann ist Diplom-Betriebswirtin (DH), Informatikerin und zertifizierte Datenschutz-Expertin. Sie ist Partnerin beim Beratungsunternehmen integratio GmbH und Datenschutzbeauftragte verschiedener länderübergreifend tätiger Unternehmen. Seit 2009 ist Henriette Baumann im Vorstand der OSB Alliance vertreten, seit 2020 als zweite stellvertretende Vorstandsvorsitzende.

Quellen

- European Data Protection Board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Adopted on 10 November 2020
- European Data Protection Board, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, Adopted on 10 November 2020
- Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 in der Rechtssache C-311/18. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:62018CJ0311&qid=1606948270244&from=DE
- Wissenschaftlicher Dienst des Deutschen Bundestages, Dokumentation US-Datenrecht, Zugriff US-amerikanischer Behörden auf Daten, WD 3 - 3000 - 181/20 vom 3. August 2020

Lizenz

Zur Open Source Business Alliance

Die Open Source Business Alliance (OSB Alliance) ist der Verband der Open Source Industrie in Deutschland. Dabei vertreten wir rund 170 Mitgliedsunternehmen, die in Deutschland ca. 10.000 Mitarbeiter beschäftigen und jährlich mehr als 1,7 Milliarden Euro erwirtschaften. Gemeinsam mit wissenschaftlichen Einrichtungen und Anwenderorganisationen setzen wir uns dafür ein, die zentrale Bedeutung von Open Source Software und offenen Standards für einen erfolgreichen digitalen Wandel im öffentlichen Bewusstsein nachhaltig zu verankern. Dieser digitale Wandel soll Unternehmen, Staat und Gesellschaft gleicherweise zugutekommen. Zudem sollen Innovationen im Bereich Open Source vorangetrieben werden. Unser Ziel ist es, Open Source als Standard in der öffentlichen Beschaffung und bei der Forschungs- und Wirtschaftsförderung zu etablieren. Denn Open Source und offene Standards sind zwingende Grundlagen für digitale Souveränität, Innovationsfähigkeit und Sicherheit im digitalen Wandel und damit die Antwort auf eine der größten Herausforderungen unserer Zeit.

Kontakt

OSB Alliance – Bundesverband für digitale Souveränität e.V.
Breitscheidstraße 4
D-70174 Stuttgart

Tel: +49 (0) 711 / 90 715-390
Fax: +49 (0) 711 / 90 715-350
E-Mail: info@osb-alliance.com