US-Privacy Shield annulliert - Smart Home stranguliert?

Was das Kippen des Privacy Shield Abkommens mit den USA bedeutet und was Hersteller von SmartHome Systemen jetzt unbedingt beachten müssen

Hallo, ich bin Switchy, ein IoT-Gerät.

Nichts Besonderes, nur ein einfacher Lichtschalter im Smart Home. Ich habe gehört, dass das **Privacy Shield Abkommen mit den USA vom europäischen Gerichtshof gekippt worden ist,** und das sogar ohne Übergangsfrist.

Was geht mich das an?

Es geht um den Transfer personenbezogener Daten in die USA. Meine Kollegen Aktoren, die schon etwas länger im Dienst sind, erinnern sich, dass es dafür das Safe-Harbor-Abkommen gab. Das galt immerhin rund 15 Jahre und wurde vor fünf Jahren ebenfalls vom EUGH gekippt und durch das Privacy Shield Abkommen ersetzt, das nun auch nicht mehr gilt. **Personenbezogene Daten europäischer Nutzer seien auf Servern in den USA nicht hinreichend vor dem Zugriff von US-Geheimdiensten und Behörden geschützt,** so die Begründung.

Aber ich, Switchy, habe doch gar nichts mit personenbezogenen Daten zu tun? Mein Gateway klärt mich auf: Immer wenn ich gedrückt werde, wird dies als Info an einen zentralen Server übertragen. Meine Anwender können dann von überall auf deren Smart Home-App sehen, in welchem Zustand ich bin und mich umschalten. **Die Daten im Server könnten aber auch für andere Zwecke verwendet werden:**

Damit mein Anwender die App nutzen kann, hat er sich registriert. Die Daten der App sind auf seine Person bezogen. Der Anbieter weiß zu jeder Zeit, welche Leuchte bei dem Anwender in welchem Zustand ist. Die Leuchten sind bei der Konfiguration den Räumen zugeordnet. Damit ist theoretisch bereits eine Menge über das Verhalten des Anwenders ableitbar: **Wann steht er morgens auf, wann verlässt er das Haus, und wann kommt er zurück, oder ist er verreist? Zusammen mit den eingestellten Licht-Szenarien lässt sich ableiten, was er wann und wie lange macht: Schaut er Fernsehen, benutzt er die Toilette, isst er zu Abend oder gibt er etwa eine Party? Falls er danach schlafen geht: Wann geht er schlafen, wie lange liest er vielleicht noch, und wie oft steht er nachts auf?** Sein Verhalten kann einfach mit dem statistischen Durchschnitt verglichen werden. Zusammengefasst könnte der Anbieter mit den Daten schon ein recht detailliertes Profil über den Anwender erstellen und zur Vervollständigung mit anderen Datenquellen kombinieren.

Genau das darf er aber alles nicht. Die in allen EU-Ländern geltende Datenschutzgrundverordnung (DSGVO) schützt den Anwender und gibt sehr enge Grenzen vor, wofür und wie die Daten verwendet werden dürfen. Neben dem Datenschutz kümmert sich die DSGVO auch um die Datensicherheit, also Maßnahmen zum Schutz vor Hackern. Wenn der Anbieter die DSGVO nicht einhält, sind die Strafen drastisch: Bis zu 20 Mio. Euro oder 4% des weltweiten Gesamtjahresumsatzes, die größere Zahl von beiden. Während die Verfolgung von Verstößen bei Inkrafttreten der DSGVO 2018 noch schleppend anlief, sind die Aufsichtsbehörden mittlerweile erkennbar aktiv.

Was ist aber, wenn der Server außerhalb der EU steht? Auch für den Fall gibt es Regelungen in der DSGVO: Daten dürfen nur in Drittländer übermittelt werden, wenn dort ein vergleichbares „angemessenes" Datenschutzniveau herrscht (vgl. Artikel 44–49 DSGVO). Hier müssen laut DSGVO zusätzliche Garantien vorliegen, um das europäische Datenschutzniveau zu gewährleisten. Für die USA wurde diese Vergleichbarkeit bisher mit dem Privacy-Shield-Beschluss attestiert, sofern US-Unternehmen sich dazu verpflichteten, das EU-Recht auf Grundlage des EU-US Privacy Shields einzuhalten. Das haben 5.378 US-Unternehmen getan. Eine entsprechende Liste findet sich hier auf der Webseite des US-Handelsministeriums. Bekannte Namen sind dabei, die als Anbieter oder Plattform-Betreiber auch im Smart Home Umfeld bedeutend sind, wie Amazon und Amazon Web Services (AWS), Google, Microsoft Azure oder Ring.

Den Privacy Shield hat der EuGH nun jedoch für unwirksam erklärt und damit entfällt diese Rechtsgrundlage für die Datenübertragung. Das wäre noch nicht dramatisch, denn die DSGVO kennt noch weitere Rechtsgrundlagen. Im Regelfall sollte es der „Angemessenheitsbeschluss" sein (Art. 45 DSGVO), mit dem einem Drittland ein angemessenes Datenschutzniveau bescheinigt wird. Auf der Liste stehen unter anderem Andorra, Argentinien, Israel, Neuseeland, die Schweiz und Uruguay, **aber eben nicht die USA.** Nach dem EUGH-Urteil ist nicht zu erwarten, dass die USA in die Liste aufgenommen werden kann. **Sie gilt damit als unsicheres Drittland, wie auch China.**

Das heißt aber nicht, dass der Datenverkehr mit der USA eingestellt werden muss. Smart Home wird nicht stranguliert, auch wenn Daten in die USA fließen. Wenn es kein generelles Abkommen gibt, wie den Privacy Shield oder den Angemessenheitsbeschluss, dann müssen Einzel-Vereinbarungen der Unternehmen den Datentransfer legalisieren. Das sind die jeweiligen Nutzungsverträge zwischen dem Dienstanbieter und dem Nutzer. Die gibt es natürlich bereits längst, müssen aber jetzt ganz konkret sagen, wie die DSGVO eingehalten wird. In manchen der Nutzungsverträge war das schon immer der Fall, andere müssen nachgebessert werden. Die Aufsichtsbehörden können weitreichender eingreifen, als sie es unter dem Abkommen konnten.

Der Vollständigkeit halber sei noch erwähnt, dass der Datentransfer auch über sogenannte „Binding Rules" oder „Ausnahmen für bestimmte Fälle" legalisiert werden kann**.** Beides ist im Smart Home Umfeld bisher praktisch nicht relevant.

Ich, Switchy, weiß nicht, ob meine Daten in den USA landen. Selbst mein Gateway ist sich da nicht sicher. **Unser Anbieter, ein seriöses europäisches Unternehmen, sollte und muss es aber wissen und in seiner Datenschutzerklärung darauf hinweisen.** Darin steht dann eine Formulierung der Art, dass sich der Empfänger der Daten in den USA dem Privacy Shield unterworfen hat. Das reichte bisher aus, jetzt nicht mehr. **Hier besteht Handlungsbedarf: Prüfen Sie, ob die Nutzungsvereinbarung mit Ihren Datenempfänger in USA der DSGVO genügt. Gegebenenfalls sind Anpassungen erforderlich. Passen Sie Ihre eigene Datenschutzerklärung an, indem Sie sich mehr auf das Privacy Shield beziehen, sondern auf die Nutzungsverträge.**

Der Europäische Datenschutzausschuss (EDSA) hat eine Checkliste zu den häufigsten Fragen in Sachen Datenübermittlung in Drittländer zusammengestellt. Die wichtigsten Aussagen sind in dem Kasten unten zusammengestellt.

- Unternehmen sollten alle Datenübermittlungsvorgänge in Drittländer dokumentieren, prüfen und die Rechtsgrundlage ermitteln.
- Alle Datenempfänger in Drittländern, vor allem mit Sitz in den USA, müssen vor weiterem Datentransfer auf geeignete Garantien (Art. 44-49 DSGVO) überprüft werden.
- Für Datenübermittlungen, die bislang auf Basis des Privacy Shield erfolgten, sollte geklärt werden, ob künftig Standarddatenschutzklauseln, Binding Corporate Rules o.ä. als Rechtsgrundlage genutzt werden können, oder ob ein Ausnahmetatbestand nach Art. 49 DSGVO infrage kommt.
- Sollte die Datenübermittlung auf Basis von Standarddatenschutzklauseln oder von Binding Corporate Rules erfolgen, müssen die Unternehmen sicherstellen, dass durch diese Instrumente ein dem EU-Datenschutzrecht adäquates Schutzniveau hergestellt wird.
- Sollte dieses nicht der Fall sein, wäre in einem weiteren Schritt zu überprüfen, ob ein angemessener Datenschutz ggf. durch ergänzende Maßnahmen wie beispielsweise Verschlüsselung oder Vertragsergänzungen ermöglicht werden kann.
- Ist ein angemessenes Schutzniveau nicht zu erreichen, muss geprüft werden, ob „Ausnahmen für bestimmte Fälle“ (nach Art. 49 DSGVO) zur Anwendung kommen können. Sollte auch dies nicht möglich sein, ist der Datentransfer auszusetzen.
- Wird die Datenübermittlung ohne angemessenes Schutzniveau im Drittland fortgesetzt, muss der für den Transfer Verantwortliche die zuständige Aufsichtsbehörde darüber informieren.

Kasten: Hinweise des Europäische Datenschutzausschuss (EDSA) zur Datenübermittlung in Drittländer.

Der Autor:

Dipl.-Inform. Günter Martin ist Geschäftsführer bei der CorDev GmbH. Das Unternehmen wurde 2016 von der Smart Home Initiative Deutschland als bestes Start-Up Unternehmen ausgezeichnet. CorDev erhielt die Auszeichnung für sein Zertifikat Protected Privacy und hat das Thema seitdem mit dem TÜV-Rheinland zu einem TÜV-Zertifikat weiterentwickelt. CorDev unterstützt Unternehmen beim Thema Datenschutz und Datensicherheit im IoT-Umfeld.