DSGVO-konform in die Cloud nach Schrems II

Das Schrems II Urteil - Nun endlich klare Handlungsvorgaben

Im Juli 2020 erließ der Europäische Gerichtshof das Urteil “C-311/18” (Schrems II Urteil) und kippte damit das US-Privacy Shield. Dies regelte bis dato den Datenaustausch von Europa in Drittländer, wie die USA.

Nach diesem Urteil herrschte eine weitreichende Unsicherheit in Bezug auf die Nutzung amerikanischer Cloud-Dienste. Im Juni 2021 schließlich veröffentlichte der Europäische Datenschutzausschuss (EDSA) seine finalen Empfehlungen zum Transfer personenbezogener Daten nach dem Schrems II Urteil.

Damit wurden klare und verlässliche Richtlinien geschaffen, an welchen sich Unternehmen orientieren müssen. Zusammengefasst bedeutet dies, dass

- die Nutzung amerikanischer Cloud-Dienste ohne weitere Maßnahmen nicht DSGVO-konform ist (auch wenn die Server in Europa stehen).
- Standardvertragsklauseln nicht mehr ausreichend sind, um DSGVO-Konformität zu erreichen.
- die von Cloud-Anbietern angebotenen Sicherheitslösungen (wie bspw. Microsoft E5 Lizenz) nicht ausreichend sind, um DSGVO-Konformität zu erreichen.

In diesem Dokument erfahren Sie, was sich nun für Unternehmen ändert und welche Möglichkeiten es gibt, Cloud-Anwendungen DSGVO-konform zu nutzen.

Der Europäische Gerichtshof (EuGH) erinnert in seinem Urteil daran, dass der Schutz, der personenbezogenen Daten im Europäischen Wirtschaftsraum gewährt wird, mit den Daten reisen muss - wohin diese auch gehen.

Wichtige Begriffe

DSGVO
Die Datenschutz-Grundverordnung (DSGVO) von 2016 (Inkrafttreten) bzw. 2018 (Anwendung) vereinheitlicht die Regeln zur Verarbeitung personenbezogener Daten durch Unternehmen, Behörden und Vereine, die innerhalb der Europäischen Union einen Sitz haben. Die englische Entsprechung des Begriffs ist "General Data Protection Regulation (GDPR)", die offizielle Bezeichnung "Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG". Der Umgang mit Kunden- und Mitarbeiterdaten, Daten von Bürgern etc. wird im Zusammenhang mit dem Datenschutz in elf Kapiteln mit insgesamt 99 Artikeln geklärt.
Quelle

Privacy Shield
In der Vergangenheit erfolgten Datentransfers von europäischen Unternehmen in die USA zunächst auf Grundlage der sogenannten Safe Harbor-Vereinbarung zwischen der EU und den USA aus dem Jahr 2000. Der Europäische Gerichtshof erklärte allerdings die Entscheidung der EU-Kommission, in der festgestellt worden war, dass die USA ein angemessenes Schutzniveau übermittelter personenbezogener Daten gewährleisten, für ungültig.

Mit dem sog. EU-U.S.-Privacy Shield stand seit dem 1. August 2016 eine neue Grundlage für Datenübermittlungen in die USA zur Verfügung.
Quelle

Cloud Act
Mit dem sogenannten CLOUD Act gilt seit Ende März 2018 ein US-Gesetz, das US-Behörden den Zugriff auch auf Daten gestattet, die US-amerikanische IT-Dienstleister oder Internetfirmen im Ausland speichern. Entgegen dem Titel des Gesetzes hat es nicht zwingend etwas mit Cloud-Diensten zu tun. CLOUD steht in diesem Fall für „Clarifying Lawful Overseas Use of Data Act", auf Deutsch etwa „Gesetz zur Klarstellung des rechtmäßigen Umgangs mit Daten im Ausland". Das Gesetz stellt sicher, dass es keine Rolle mehr spielt, ob Daten „in der Cloud" oder in einem bestimmten Datenzentrum gespeichert sind – ob im In- oder Ausland.
Quelle

Schrems II Urteil
Am 16. Juli 2020 hat der EuGH ein Urteil (Rs. C-311/18) gefällt, das weitreichende Folgen für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittstaaten hat. In erster Linie ist der Datentransfer in die USA betroffen. Denn das Schrems II Urteil hebt den Angemessenheitsbeschluss der Europäischen Kommission „Privacy Shield" auf. Dieser bekundete, dass die USA unter bestimmten Umständen ein der Europäischen Datenschutzgrundverordnung (DSGVO) angemessenes Schutzniveau für die Daten natürlicher Personen bietet. Nur so war ein datenschutzkonformer Datentransfer zwischen den USA und der Europäischen Union (EU) möglich.
Quelle

Standardvertragsklauseln sind nicht ausreichend in Ländern deren Gesetzgebung Daten-Importeure verpflichtet, Daten auf Anordnung von Behörden offen zu legen (bspw. USA).

Handlungsvorgaben und deren Auswirkungen für Unternehmen

Sind Standardvertragsklauseln weiterhin gültig?

Grundsätzlich behalten Standardvertragsklauseln ihre Gültigkeit. Allerdings weist der EDSA ausdrücklich drauf hin, dass "Standardvertragsklauseln nicht in einem Vakuum operieren". Gemeint ist damit, dass Standardvertragsklauseln alleine keine DSGVO-konforme Datenübermittlung ermöglichen.

Vertragliche Maßnahmen können die Anwendung der Gesetzgebung eines Drittlandes nicht ausschalten!

Der EDSA stellt in seinen Empfehlungen fest, dass Standardvertragsklauseln gesetzliche Regelungen von Drittländern zwar in einigen Fällen ergänzen können.
Allerdings

- sind Standardvertragsklauseln niemals bindend für die Behörden des Drittlandes. Denn das Land ist kein Vertragspartner.
- können vertragliche Maßnahmen niemals die Anwendung der Gesetzgebung eines Drittlandes ausschalten.

Vor allem bei Datenübermittlung in Länder mit niedrigerem Sicherheitsniveau als Europa sind Unternehmen daher verpflichtet, zusätzliche technische Maßnahmen zu ergreifen. Der EDSA beschreibt die Verschlüsselung oder Pseudonymisierung von Daten, bevor diese an die Cloud übertragen werden, als adäquate Maßnahme zur Erreichung von DSGVO-Konformität.

Für Unternehmen, die amerikanische Cloud-Dienste wie bspw. Microsoft 365 nutzen, bedeutet dies, dass der weiteren Nutzung dieser Tools grundsätzlich nichts im Wege steht. Der sogenannte Data Controller muss jedoch nachweisen, dass er seiner Verantwortung für die gesetzeskonforme Behandlung personenbezogener Daten vollumfänglich nachkommt. Die Einhaltung dieser Vorgaben müssen bspw. die Landesdatenschützer prüfen.

Wird- wie von der EDSA empfohlen- eine externe Verschlüsselungslösung ohne Zugriffsmöglichkeit durch Dritte wie bspw. den Cloud-Anbieter eingesetzt, ist dieser Beweis erbracht.

Aufgrund des Cloud Acts könnte der Durchgriff von bspw. Microsoft US auch auf Europäischen Instanzen angeordnet werden.

Dies kann nicht in Einklang mit der DSGVO gebracht werden.

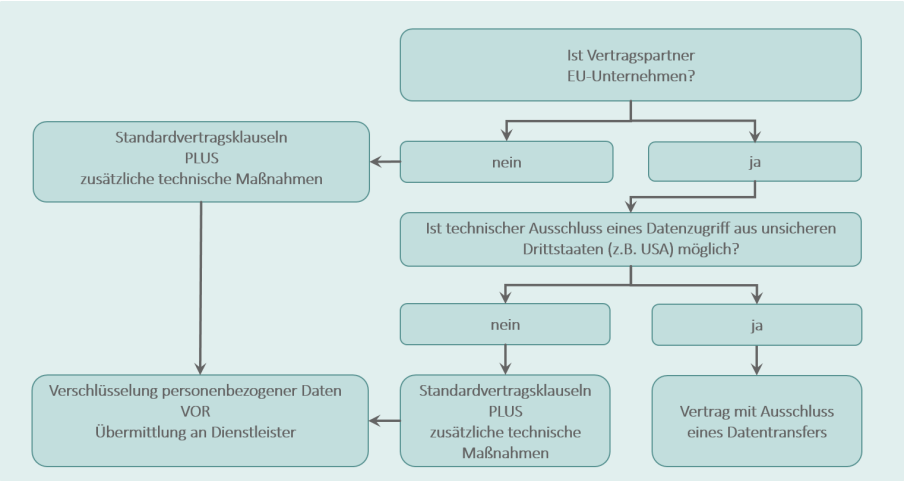
Was bedeutet "Datenaustausch mit unsicheren Drittländern"?

Länder außerhalb der Gültigkeit der DSGVO werden als sog. Drittländer bezeichnet. Als unsicher- im Sinne der DSGVO- gelten die Länder, deren Datenschutzniveau unter dem Europas liegt. Dies trifft bspw. auf die USA zu.

Ein maßgebliches Kriterium für die Einstufung als "unsicheres Drittland" stellt das behördliche Herausgabeverlangen (bspw. basierend auf dem US Cloud Act) dar. Am Beispiel Microsoft gesprochen bedeutet dies, dass Microsoft gezwungen werden kann, auf US-Behördenverlangen hin, personenbezogene Daten offen zu legen.

Diese Herausgabepflicht beschränkt sich nicht auf eine Datenspeicherung auf US-Servern, sondern gilt unabhängig vom Speicherort der Daten. Maßgeblich ist hier, dass Microsoft ein amerikanisches Unternehmen ist. Per behördlicher Anordnung kann sogar die Information des Kunden über die Herausgabe der Daten untersagt werden. Auch wenn Microsoft alle rechtlichen und technischen Mittel ausschöpft, um personenbezogene Daten zu schützen und eine Herausgabe zu verhindern, haben amerikanische Behörden schlussendlich das geltende Recht auf ihrer Seite.

Für europäische Unternehmen stellt die Nutzung von Cloud-Diensten aus unsicheren Drittländern ohne die richtigen zusätzlichen Maßnahmen einen klaren Verstoß gegen die DSGVO dar und kann entsprechend geahndet werden.



Die einzige Möglichkeit hier entgegen zu wirken, besteht in der Verschlüsselung oder Pseudonymisierung vor Übermittlung der Daten in die Cloud. Nur so wird sicher gestellt, dass der Cloud-Anbieter zu keinem Zeitpunkt Zugriff auf die Daten in Klartext erhält. Entsprechend kann der Cloud-Anbieter bei Durchsetzung des Herausgabeverlangens nur verschlüsselte Daten zur Verfügung stellen.

Wichtig in diesem Zusammenhang ist, dass die Kontrolle sowohl über Schlüssel als auch die Verschlüsselung alleine beim sogenannten Data Controller liegen muss. Der Cloud-Anbieter darf hier über keinerlei Zugriffsmöglichkeiten verfügen.

Aktuelle Entwicklungen in Deutschland

> BvD Herbstkonferenz Datenschutz & Behördentag

Folgende wesentlichen Aussagen wurden während der Tagung von Datenschützern auf Landesebene im Oktober 2021 getroffen.

Höhere Strafen
Strafen. die aufgrund von Verstößen gegen die DSGVO ausgesprochen werden, sind als Mahnung zu sehen und sollen abschreckend wirken (Art 83 Absatz 1 EU-DSGVO).

Post-Pandemie
Seit März 2020 haben Datenschutzbeauftragte auf Landes- und Bundesebene aus Rücksicht auf die Herausforderungen der Pandemie Datenschutzverstöße in begrenztem Rahmen geduldet. Vor allem im Bildungsbereich wurde das Recht auf Bildung vor das Recht auf Datenschutz gestellt. Doch nach zwei Jahren Pandiemie sind sich die Datenschützer weitestgehend einig, dass ausreichend Zeit vergangen ist, um datenschutzkonforme Lösungen einzuführen. Entsprechend laufen die offiziellen Duldungen von bspw. Microsoft Teams in den Bundesländern nach und nach aus.

Internationaler Datentransfer
Das Thema internationaler Datenstransfer hatte in der Vergangenheit seinen Fokus auf der Speicherung personenbezogener Daten im Ausland. Nun rückt der Datentransfer in den Mittelpunkt der Betrachtung. Die Auslegung während der Tagung besagt, dass bereits der Zugriff durch einen US-Administrator einen internationalen Datentransfer darstellt- unabhängig vom Standort des Datacenters (bspw. Deutschland/EU).

EU Tochterunternehmen / Dependancen
Die Gründung von EU Tochterunternehmen oder Dependancen wird als nicht ausreichend erachtet, um den Regelungen der DSGVO zu genügen da eine wirtschaftliche Abhängigkeit sowie Weisungsbindung zum Mutterunternehmen besteht. Weiterhin wird der Zugriff von bzw. Durchgriff durch amerikanische Three-Letter-Agencies nicht verhindert. Nach amerikanischem Verständnis gehören Daten dem amerikanischen Unternehmen, unabhängig davon wo diese sich befinden.

> Datenschutz Bayern

Im Dezember 2021 veröffentlichte der Datenschutz Bayern eine Kurz-Information zum Thema Office-Anwendungen aus Drittstaaten bei bayerischen öffentlichen Stellen. Dort werden die Empfehlungen des EDSA explizit bekräftigt. Standardvertragsklauseln werden nur als ausreichend erachtet, wenn der Verantwortliche den Nachweis erbringt, dass die zu übermittelnden personenbezogenen Daten nicht Gegenstand der Zugriffsrechte US-amerikanischer Behörden werden können. Ist dieser Nachweis nicht möchlich, wird eine angemessen starke Verschlüsselungsmethode, besonderer Schutz der Schlüsel sowie der Einsatz eines Verschlüsselungsverfahrens nach aktuellem Stand der Technik gefordert.

Was ist die rechtssichere Lösung?

Verschlüsselung vor der Cloud
Der EDSA beschreibt Verschlüsselung bzw. Pseudonymisierung von Daten als geeignete technische Maßnahme, um auch amerikanische Cloud-Dienste DSGVO-konform nutzen zu können.

Voraussetzung hierfür ist, dass die Verschlüsselung bzw. Pseudonymisierung der Daten erfolgt, bevor diese an die Cloud übertragen werden.

Somit scheiden die meisten nativen Sicherheitslösungen der Cloud-Anbieter per se als geeignete Maßnahmen aus, um DSGVO-Konformität zu erreichen. Denn der Cloud-Anbieter kann die Verschlüsselung bzw. Pseudonymisierung der Daten erst dann vornehmen, wenn diese bereits die Kontrolle des Data Controllers verlassen haben und an die Cloud übertragen wurden.

Kein Zugriff auf Schlüssel & Verschlüsselung durch Cloud-Anbieter
Derjenige, der Zugriff auf die Verschlüsselung hat, hat zwangsläufig auch Zugriff auf die unverschlüsselten Daten. Aus diesem Grund schreibt die EDSA weiterhin vor, dass Cloud-Anbieter zu keinem Zeitpunkt Zugriff auf Schlüssel und Verschlüsselung haben dürfen.

Im Umkehrschluss bedeutet dies, dass die alleinige Kontrolle über die Schlüssel sowie die Verschlüsselung beim Data Controller liegen muss.

Diese Regelung schließt entsprechend BYOK (Bring your own Key) und HYOK (Hold your own Key) Lösungen der Cloud-Anbieter als geeignete technische Maßnahme aus. Weiterhin wird damit das Argument der Verschlüsselung vor der Cloud bestärkt. Denn nur so kann sicher gestellt werden, dass der Cloud-Anbieter zu keinem Zeitpunkt Zugriff auf unverschlüsselte Daten erhält.

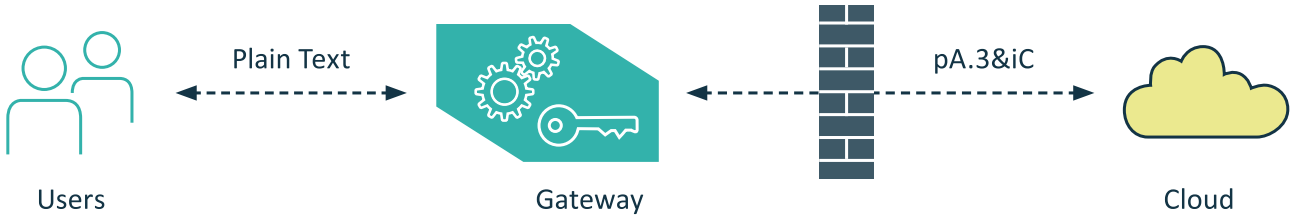
Stand der Technik
Laut EDSA müssen geeignete technische Maßnahmen dem sogenannten "Stand der Technik in der IT-Sicherheit" entsprechen. Hierzu hat die ENISA gemeinsam mit der TeleTrusT eine Handreichung veröffentlicht.

Diese listet sogenannte Verschlüsselungsgateways als Stand der Technik auf, um Daten vor Übertragung in die Cloud DSGVO-konform zu verschlüsseln bzw. zu pseudonymisieren.

Die eperi Lösung
Datenschützer auf Landes- und Bundesebene bezeichnen das eperi Gateway als geeignete technische Maßnahme, um personenbezogene Daten DSGVO-konform in der Cloud zu speichern. Damit ermöglicht das eperi Gateway die gesetzeskonforme Nutzung amerikanischer Cloud-Dienste wie bspw. Microsoft 365 inkl. Teams.

Der Data Controller behält jederzeit die alleinige Kontrolle über Schlüssel und Verschlüsselung. Kritische Daten werden verschlüsselt bzw. pseudonymisiert bevor sie an die Cloud übertragen werden.

Für Anwender ist das eperi Gateway als Proxy vollständig transparent. Gewohnte Arbeitsprozesse bleiben bestehen.



DSGVO-konforme Cloud-Nutzung zusammengefasst

Eine DSGVO-konforme Cloud Nutzung ist auch nach Schrems II möglich- und gar nicht so kompliziert wie es der erste Eindruck vermuten lässt. Mit den richtigen technischen Maßnahmen arbeiten Anwender wie gewohnt, während personenbezogene Daten im Hintergrund ver- und entschlüsselt werden.

Sogar Unternehmen in hochregulierten Branchen wie bspw. Banken können so bedenkenlos in die Cloud migrieren und die Vorteile moderner Multi-Cloud Umgebungen nutzen.

Dank der nun endlich sehr deutlich formulierten Handlungsempfehlungen des EDSA zum Schrems II Urteil ist klar, welche Anforderungen eine Lösung erfüllen muss, um DSGVO-Konformität herzustellen. Einfach zusammengefasst, muss eine geeignete Lösung

- Daten verschlüsseln, bevor diese an die Cloud übertragen werden.
- dem Cloud-Anbieter zu keinem Zeitpunkt Zugriff auf Schlüssel und Verschlüsselung gewähren.
- dem Stand der Technik entsprechen.

Mit dem patentierten Multi-Cloud Ansatz deckt das eperi Gateway all diese Punkte ab. Doch eine geeignete Lösung muss nicht nur rechtliche Voraussetzungen erfüllen. Der Arbeitsablauf der Anwender darf nicht unterbrochen, die gewohnte Effizienz muss beibehalten werden. Das eperi Gateway bietet neben DSGVO-Konformität

- eine für den Anwender vollständig transparente Lösung.
- die Beibehaltung gewohnter und effizienter Arbeitsabläufe.
- den Erhalt der wichtigen Anwendungsfunktionen wie bspw. Suche, Sortierung und Kollaboration.

Zusammengefasst bedeutet dies: Jedes Unternehmen kann die Vorteile der Cloud nutzen!

Erhalten Sie weitere Informationen oder buchen Sie eine Live-Demo. Unsere Experten für Cloud-Verschlüsselung freuen sich auf Sie!

Das eperi Gateway

- Verschlüsselung vor der Cloud statt in der Cloud
- Kein Zugriff durch Cloud-Anbieter
- Verschlüsselungsgateway nach Stand der Technik
- Geeignete technische Maßnahme nach DSGVO
- Transparent für Anwender

Quellen & weiterführende Links

european court of justice
Fall C-311/18

(ii)Additionally, the Court affirmed the validity of the SCC Decision and held that SCCs donot, perse, present lawful or unlawful grounds for data transfer (no panacea). The CJEU also stipulates that data controllers or operators that seek to transfer data based on SCCs, must ensure that the data subject is afforded a level of protection *essentially equivalent* to that guaranteed by the GDPR and CFR – if necessary with *additional measures* to compensate for lacunae in the protection of third-country legal systems. Failing that, operators must suspend the data transfer. Supervisory authorities must check transfers and are *required* to prohibit transferswheretheyfindthatdatasubjectsarenotaffordedessentiallyequivalentprotection.

84. A data exporter uses a hosting service provider in a third country to store personal data, e.g. for backup purposes.

If

1. the personal data is processed using strong encryption before transmission, and the identity of the importer is verified, (...)

then the EDPB considers that the encryption performed provides an effective supplementary measure.

Finale Empfehlung 18.06.2021

Rechtliche Hintergründe

Urteil C-311/18 (Schrems II)
Finale Empfehlung EDSA
ENISA/TeleTrusT Stand der Technik
Kontrolle der Umsetzung des EuGH-Urteils "Schrems II" in Unternehmen durch Landesdatenschutzbehörden (Beispiel Niedersachsen)

Weiterführende Informationen und Presseartikel

Kurzinformation des Bayerischen Datenschutzes (01. Dezember 2021)
Informationen und Links zu Stellungnahmen durch Datenschützer auf Landes-, Bundes- und EU-Ebene (eperi)
Presseartikel: Gültigkeit von Standardvertragsklauseln (Security Insider)
Videointerview zu den Folgen des Schrems II Urteils (eperi und SEPPmail)
Blogartikel: Microsoft Teams DSGVO-konform nutzen (IT-Techblog)

Weitere Quellen

Definition DSGVO
Definition Cloud Act
Definition Privacy Shield
Definition Schrems II

Disclaimer

Soweit dieses Dokument juristische Erläuterungen, Empfehlungen und Ratgeber enthält, so stellen diese unverbindliche Informationen ohne jede Gewähr für Vollständigkeit und Richtigkeit dar. Es handelt sich insoweit nicht um Rechtsberatung und die Eperi GmbH erhebt auch keinesfalls den Anspruch eine solche darzustellen oder gar zu ersetzen.

Version 2.0