

Cloud-managed Solutions nach dem EuGH Urteil zum Privacy Shield Abkommen

Am 16. Juli 2020 hat der Europäische Gerichtshof das Privacy-Shield-Abkommen zwischen Europa und den USA für unzulässig erklärt. Darf ich Zoom, Skype und Co. jetzt noch nutzen? Worauf muss ich zukünftig als Entscheider achten?

Was sagt das Urteil?

- > Die bisherige Rechtsgrundlage zur Verarbeitung personenbezogener Daten von EU-BürgerInnen in den USA ist ungültig.
- > Es besteht kein ausreichender Schutz der Grundrechte vor dem Zugriff der US-Behörden.
- > Das informelle Abkommen „Privacy Shield“, das den Schutz bisher garantieren sollte, ist nicht ausreichend.
- > Die Anwendung der Standardvertragsklauseln der EU-Kommission als alternative Möglichkeit zum Schutz ist weiterhin erlaubt. Allerdings müssen Maßnahmen faktisch umsetzbar sein, was in den USA nicht gegeben ist.
- > Das Urteil muss umgehend umgesetzt werden – es gibt keine Gnadenfrist!
- > Das Urteil im Original hier: <http://curia.europa.eu/juris/documents.jsf?num=C-311/18>

Das heißt...

Es dürfen aktuell eigentlich keine Nutzerdaten aus der EU mehr in die USA übertragen und dort verarbeitet werden!

Betroffen sind neben typischen Cloud-Diensten auch Unternehmensnetze, die aus der Cloud gemanagt werden, z. B. SD-WAN-Infrastrukturen und Cloud-managed WLANs.

Die Nutzung von Cloud-Lösungen in öffentlichen Einrichtungen wie z. B. Schulen mit der aktuell hohen Nachfrage nach Online-Unterricht, Lernplattformen, aber auch das Management von Schulnetzen ist unzulässig.

Werden weiterhin Cloud-Dienste von US-Anbietern genutzt, muss sichergestellt sein, dass alle personenbezogenen Daten auf Servern innerhalb der EU oder einem sicheren Drittland verarbeitet werden. Das bezieht auch sog. Metadaten ein. Metadaten sind nicht der eigentliche Dateinhalt (z. B. ein Mailtext), sondern Informationen wie „wer hat wann an wen gesendet“. Selbst wenn die eigentlichen Nutzdaten in EU-Rechenzentren gespeichert werden, erfolgt eine Übertragung der Metadaten an die zentralen (US-) Verwaltungsserver der Anbieter.

Cloud-managed Solutions nach dem EuGH Urteil zum Privacy Shield Abkommen

Betroffene Dienste

- Cloudflare
- Facebook-Connect
- Facebook Plugins
- Twitter Plugin
- Instagram Plugin
- Tumblr Plugin
- LinkedIn Plugin
- Pinterest Plugin
- Google Analytics
- WordPress Stats
- GoogleAds
- Google Adsense
- Google Adsense (nicht personalisiert)

- Google Remarketing
- Google Conversion Tracking
- Google Doubleclick
- Facebook Pixel
- MailChimp
- MailChimp mit deaktivierter Erfolgsmessung
- ActiveCampaign
- YouTube
- YouTube mit erweitertem Datenschutz
- **Vimeo**
- **Vimeo ohne Tracking**
- SoundCloud

- Spotify
- **Zoom**
- **Skype for Business**
- GoToMeeting
- **Microsoft Teams**
- **Google Hangouts**
- **Google Meet**
- Google Web Fonts
- Adobe Fonts
- Google Maps
- Google reCAPTCHA
- Amazon Partnerprogramm

Was sind die Folgen für Unternehmen?

- > Alle Unternehmen, die personenbezogene Daten in die USA übermitteln, müssen sich mit neuen Voraussetzungen auseinandersetzen.
- > Entscheidungsträger von privaten und öffentlichen Einrichtungen dürfen bei der Auswahl ihrer Hersteller und Anbieter das Thema Datenschutz nicht außer Acht lassen.
- > Bei weiterer unberechtigter Datenübermittlung drohen Sanktionen der Aufsichtsbehörden in Form von Verboten und/oder Bußgeldern.
- > Das wirtschaftliche Risiko durch einen hohen Verwaltungsaufwand sowie drohende Strafzahlungen steigt.

Was können Sie tun?

Prüfen Sie zeitnah Ihre Datentransfers und stellen Sie ein angemessenes Datenschutzniveau her.

Dringender Handlungsbedarf besteht, wenn bisher nur das Privacy-Shield genutzt wurde. Stellen Sie schnellstmöglich auf die Standard-Vertragsklauseln um. Auch wenn diese keinen vollständigen Schutz bieten, stellen sie jedoch bis zu einer finalen Regelung eine Überbrückung dar.

Prüfen Sie, ob ein Wechsel auf europäische oder sogar lokale Anbieter möglich ist.

Legen Sie Verantwortliche fest, die die aktuellen Empfehlungen der europäischen Datenschutzbehörden beobachten und Maßnahmen mit den eigenen Datenschutzbeauftragten abstimmen.

Prüfen Sie auch, ob Subunternehmer Daten in die USA übermitteln.

Passen Sie Ihre Datenschutzbestimmungen an.

Sichere datenschutzkonforme Lösungen von effexx

- > Erledigung sämtlicher Aktivitäten unmittelbar per Chatfunktion, Audio oder Videoanruf
- > Bildung von Projektgruppen
- > Verbindung mit Standorten und mobilen Mitarbeitern
- > Nahtlose Anbindung an vorhandene TK-Anlage
- > Zahlreiche APIs für benutzerspezifische Anpassung
- > Integration in Smartphone-Apps oder Webseiten für direkten Kundenkontakt

Alcatel-Lucent Rainbow



Cloudtelefonie - stimme



- > Telefonieren so individuell wie Ihr Unternehmen selbst ist
- > Kommunikationslösung ohne komplexe und kostspielige Infrastruktur
- > Besonders interessant für den Mittelstand
 - Bündelung aller Kommunikationskanäle von der Email bis zur Voicemail in einem einzigen Posteingang (UMS)
 - Integration von Telefon und PC
 - Integration von mobilen Clients als vollwertige Nebenstellen (Mobility)
 - Detaillierte Informationen zur Erreichbarkeit der Kollegen
 - Vielfältige Kommunikationsmöglichkeiten
 - DSGVO-konform

- > sichere Alarmierungslösung mittels Cloud- und On-Premise-Technologie
- > Krisensituationen mit Hilfe eines zentralen Dashboards professionell managen
- > einfache Bedienung und individuelle Konfiguration
- > schnelle Koordination aller wichtigen Akteure
 - Unterschiedliche Alarmempfangsmöglichkeiten (inkl. redundanter Alarmierungswege)
 - Direkte Rückruffunktion bei Alarmempfang
 - Multimediale Alarmauslösung ohne Zeitverlust
 - Personalisierte Auslösung mit Pin
 - Alarmquittierung mit allen Empfangsmedien
 - Individuelle Rufkonfiguration nach Gruppen und Prioritäten
 - Personalisierte Alarmtexterstellung (inkl. text-to-speech)
 - Ausführliche Alarmreports

effexx guard

Alarmszenarien
professionell meistern

EFF-XX GUARD