

Herzlich willkommen!



**Schrems II – Fluch oder doch Segen?
Lösungen für die Praxis mit Microsoft 365 & Co.**

Bettina Schwarz, Stephan Albern, Tobias Pustal

lmbit 

Was ist Schrems II?

- **Urteil des Europäischen Gerichtshofs, benannt nach dem Datenschutzjurist Maximilian Schrems**
- **Entscheidungsgegenstand: Zulässigkeit der Übertragung personenbezogener Daten in ein Drittland / in die USA**
- **Wann ist eine Datenübertragung in ein Drittland überhaupt erlaubt?**

Datenübertragung in Drittländer

Grundregel: Datenübertragungen in Drittländer sind unzulässig – Art 44 DSGVO

Ziel: Europäischer Datenschutz soll nicht ausgehöhlt werden – „Untergrabungsverbot“

Ausnahmen: Art 45 bis 49 DSGVO



Relevante Ausnahmen

Angemessenheitsbeschluss der Europäischen Kommission (Art 45)

Geeignete Garantien: SCC (Art 46) / Binding Corporate Rules (Art 47)

Bestimmte Fälle (Art 49)

Notwendig und nicht strukturiert Beispiele: E-Mail-Korrespondenz; Hotelbuchung, Flugreservierung

Wird von EDPB restriktiv ausgelegt



- **Bilateraler Vertrag: Safe Harbor/Privacy Shield**
- **Selbstzertifizierung: Einseitige Erklärung, sich Datenschutzrecht zu unterwerfen**
- **Problem: Grundrechte vs. Überwachung**



- FISA 702/EO 12.333
- „Anbieter elektronischer Dienste“
- Upstream/Downstream (früher PRISM)
- Auch wenn Server in Europa stehen (CLOUD Act)



- **„Anbieter elektronischer Dienste“**
 - › Telekommunikationsanbieter
 - › Anbieter von elektronischen Kommunikationsdiensten
 - › Anbieter eines Remote-Computing-Dienstes
 - › Jeder andere Kommunikationsdienstleister, der Zugang zu drahtgebundener oder elektronischer Kommunikation hat, entweder während diese Kommunikationen übertragen oder gespeichert werden oder
 - › Leitende Angestellte oder Vertreter dieser Anbieter.
 - › -> Denkbar weite Definition

Wie kam es zu Schrems II



- Verfahren zwischen Max Schrems und Facebook
- Aufhebung von Safe Harbor wegen Unvereinbarkeit mit Kernpunkten des Datenschutzes
- Einführung Privacy Shield
- Adaptierte Beschwerde von Max Schrems
- Vorlage an den EuGH

Ergebnis Schrems II

Überwachung durch USA ist unverhältnismäßig:
Aufhebung des Privacy Shields

Standardvertragsklauseln sind prinzipiell gültig
und anwendbar

Individuelle Durchsetzung gegen Unternehmen
die FISA unterliegen



- **Übertragung nicht personenbezogener Daten weiterhin möglich**
- **Übertragung in bestimmten Einzelfällen weiterhin möglich (z.B. Ausdrückliche Einwilligung)**
- **Übertragung an Unternehmen die nicht FISA unterliegen - auf Basis der SCC weiterhin möglich**
- **Übertragung an Unternehmen die FISA unterliegen - nicht mehr ausschließlich auf Basis von SCC möglich**

Konsequenz

Wenn Bezug zu Unternehmen gegeben ist, die FISA 702 unterliegen:

(1) Vereinbarung von SCC

(2) Ergreifen ergänzender Maßnahmen



Reaktion der europäischen Kommission

Veröffentlichung neuer SCC

Ziel: sollen die Erfordernisse an die Rechtslage nach Schrems II besser abbilden

(-) können aber eine Überprüfung der Rechtslage im Drittland und das Ergreifen von ergänzenden Maßnahmen nicht ersetzen.



Neue SCC: Zeitrahmen

SCC müssen neu abgeschlossen werden!

Alte SCC wurden am 27.09.2021 aufgehoben

Neue SCC seit 4.6.2021/ veröffentlicht am
7.6.2021/ **einsetzbar seit 27.6.2021**

Übergangsfrist bis 27.12.2022 für bereits
abgeschlossene SCC



Ergänzende Maßnahmen – Praxis Microsoft 365



Tobias Pustal
Teamleiter Cloud-Infrastruktur

Fon +49 431 6703-124
Tobias.Pustal@lmbit.de



Microsoft
Partner

Silver Cloud Productivity
Silver Small and Midmarket Cloud Solutions

- **Es gibt NICHT „die EINE Lösung“**
- **Die Anbieter entwickeln sich laufend weiter**
- **Es wird darauf hinauslaufen, dass (Microsoft bis Ende 22 ?) sämtliche Daten in der EU gespeichert werden**
- **Aufsichtsbehörden argumentieren zumeist sehr pauschal**
- **Keine Berücksichtigung von möglichen Modifikationen oder Security Optimierungen**
- **Keine Differenzierung zwischen Verantwortlichkeit des Anbieters und Verantwortlichkeit des einsetzenden Unternehmens**
- **Keine Berücksichtigung der Lizenzmodelle und Zusatz-Software**

- **Juli 20: „Schrems II“**
 - › MS nutzt nur noch SCC für Transfers

- **Dezember 20: „Defending Your Data“**
 - › Commitment zur juristischen Anfechtung behördlicher Anordnungen

- **Mai 21: „EU Data Boundary“**
 - › Ankündigung zu Verarbeitung und Speicherung der Daten in der EU bis Ende 22

- **September 21: „Neue SCC“**
 - › Erweiterung auf Produkte & Services (davor galt eine Trennung von Online Services)

Wie handelt Microsoft?

- **CLOUD Act**
 - › Clarifying Lawfull Overseas Use of Data
 - › Es wird immer zuerst an das betroffene Unternehmen verwiesen
- **Law Enforcement Requests Report**

2021 (Jan-Jun) - Global

Requests

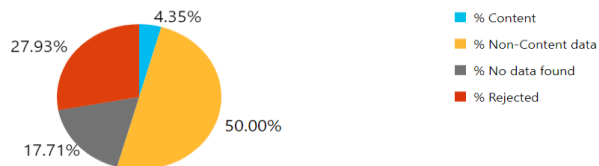
Total number of requests



Accounts/users specified in request



Disclosures



2021 (Jan-Jun) - Germany

Requests

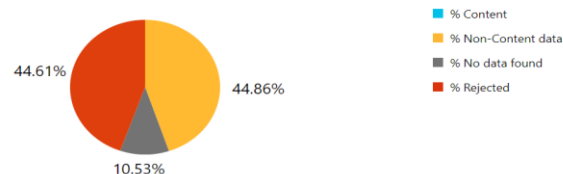
Total number of requests



Accounts/users specified in request



Disclosures



Auf dem Weg zur Compliance

- 1. Daten(Typen) Identifizieren**
- 2. Transferwege identifizieren**
- 3. Lokale und globale Bestimmungen identifizieren**
- 4. Mögliche Maßnahmen bewerten**
- 5. Maßnahmen treffen**
- 6. Laufende Anpassungen durchführen**

Damit müssen sich Unternehmen beschäftigen

1. Wo befinden sich die Daten (Data Residence)
2. Welche Einstellungen wurden gesetzt
3. Welche Apps werden genutzt
4. Klassifizierung der Daten (Information Protection)
5. Verschlüsselung
6. Audits – Log Auswertung

→ Daraus resultieren die TOM's für ein Unternehmen

- **Prüfen Sie die Einstellungen Ihrer Organisation im MS 365 Admin Center**
- **Beschränken Sie die eingesetzten Apps auf ein Minimum**
- **Deaktivieren Sie Integrationen mit anderen Diensten (z.B. LinkedIn-Integration)**
- **Prüfen Sie die globalen Admins und reduzieren Sie diese**
- **Beschäftigen sie sich mit dem Compliance Center**
- **Beschäftigen Sie sich mit den Reports**
- **Aktivieren Sie ggf. Anonymisierungen in Reports**
- **Aktivieren Sie den Identitätsschutz (u.a. MFA)**

Weiterführenden Maßnahmen

- Arbeiten Sie mit Priviledged Access und Conditional Access
- Implementieren Sie Daten Klassifizierungen (Informationsschutz, AIP)
- Implementieren Sie Data Loss Prevention (DLP)
- Implementieren Sie Verschlüsselung (Customer Key, BYOK, HYOK, Double Key Encryption)
- Implementieren Sie Datenschutzmanagement (Microsoft Priva)
- Nutzen Sie ergänzende Produkte – z.B. 365 Total Protection (Hornetsecurity)

Beachten Sie, dass die meisten dieser Maßnahmen Einschränkungen bei den Benutzern verursachen und zusätzliche Lizenzen erfordern

Sprechen Sie daher unbedingt vorher mit einem Microsoft Experten

- 1. Nutzung von Bordmitteln (Azure Key Vault, BYOK, HYOK)**
Pro: moderater Implementationsaufwand, hohe Kompatibilität
Contra: weitere Lizenzen erforderlich, Herstellerabhängigkeit
- 2. Nutzung einer weiteren SaaS Lösung (HornetSecurity, Sophos)**
Pro: geringer Implementationsaufwand
Contra: POC/Demo empfohlen, Herstellerabhängigkeit
- 3. Nutzung eines Verschlüsselungsgateway (Eperi)**
Pro: Multifunktional für unterschiedliche Cloud Services
Contra: POC erforderlich, Einschränkung der Usability möglich



Herzlichen Dank !

#FutureIsMore