BayLDA

Bayerisches Landesamt für Datenschutzaufsicht

82. Sitzung des GDD-Erfa-Kreises Bayern

Schrems II
Ist die Sommerpause vorbei ?

Michael Will
Bayer. Landesamt für Datenschutzaufsicht

Schrems-II-Urteil des EuGH und die Folgen

EuGH, Urteil C-311/18 vom 16.07.2020 - massive Konsequenzen für den gesamten Bereich der Übermittlungen personenbezogener Daten in Drittländer

Wichtigste Aussagen und Konsequenzen des Urteils

- EU-U.S. Privacy Shield ist unwirksam und wird aufgehoben
- Standarddatenschutzklauseln und andere vertraglichen Instrumente nach Art. 46 genügen für sich gesehen nicht automatisch als Grundlage für die Übermittlung in ein Drittland
  - und zwar weil vertragliche Instrumente als solche die (drittstaatlichen) Behörden nicht binden und daher deren Datenzugriffe nicht verhindern können

Schrems-II-Urteil des EuGH und die Folgen

Übermittlungen auf Grundlage von Art. 46-Instrumenten sind nur zulässig,

- wenn **Datenzugriffe durch drittstaatlichen Behörden nur in einem Umfang** stattfinden können, **der auch nach EU-Recht zulässig wäre** (Maßstab ist Art. 52 EU-Grundrechtecharta, d.h. Zugriffe nur im Rahmen einer ausreichend *klaren gesetzlichen Grundlage* sowie von *Erforderlichkeit und Verhältnismäßigkeit*)
- und zudem wenn den betroffenen Personen **effektive Rechtsbehelfe** gegen solche Zugriffe zur Verfügung stehen (Maßstab ist Art. 47 EU-Grundrechtecharta; in der Regel ist *gerichtlicher* Rechtsschutz nötig)

Schrems-II-Urteil des EuGH und die Folgen

Speziell für Übermittlungen in die USA hat der EuGH in „Schrems II“ schon selbst das Schutzniveau in Sachen Zugriffe durch Nachrichtendienste bewertet und für nicht ausreichend befunden:

- Die Zugriffsbefugnisse von US-Nachrichtendiensten nach **FISA Section 702** und **Executive Order 12.333** sind zu weitgehend und überschreiten das nach EU-Recht akzeptable Maß, d.h. entsprechen nicht den Maßstäben des EU-Rechts (Art. 52 GRCh) an Erforderlichkeit und Verhältnismäßigkeit.
- Ferner stehen den Betroffenen kein ausreichender Rechtsschutz zur Verfügung, d.h. die Anforderungen des Art. 47 GRCh sind nicht erfüllt:
    - weder steht gerichtlicher Rechtsschutz zur Verfügung
    - noch genügt die Anrufung der sog. Ombudsperson genügt nicht den Anforderungen an ausreichenden Rechtsschutz

Schrems-II-Urteil des EuGH und die Folgen

Was heißt das nun?

Für Übermittlungen in die USA ist zunächst genauer zu prüfen, ob die Daten Zugriffen nach E.O. 12.333 und/oder nach FISA Section 702 ausgesetzt sein können.

E.O.12.333

- Dazu ist nur sehr wenig bekannt.
- Im Wesentlichen handelt es sich hier um Auslandsaufklärung (Spionage), etwa durch das Anzapfen von Kabeln (laut US-Regierung finde E.O. 12.333 nur außerhalb des US-Territoriums Anwendung)
- Datenexporteure sollten hier also vor allem prüfen, ob solche Zugriffe etwa durch **Verschlüsselung** (nach menschlichem Ermessen hinreichend sicher) ausgeschlossen werden können („zusätzliche Garantien“!)
- Für den Herbst sind Aussagen des Europ. Datenschutzausschusses zu möglichen „zusätzlichen Maßnahmen“ angekündigt.

Schrems-II-Urteil des EuGH und die Folgen

FISA Section 702

- es handelt sich um „erzwungene Zugangsgewährung“ für Nachrichtendienste zu Daten
- betrifft zunächst einmal Daten, die auf US-Territorium sind
- derzeit nicht ganz klar, ob auch auf Daten außerhalb der USA anwendbar
- Grundsätzlich sind wohl nur Electronic Communication Service Provider (ECSP) zur o.g. „Zusammenarbeit“ mit US-Nachrichtendiensten verpflichtet.
- Cloud Provider scheinen darunter zu fallen, auch TK-Provider
- Auch hierzu werden Aussagen des EDSA noch im Herbst angestrebt
- Möglicherweise sind somit Übermittlungen an US-Unternehmen, die keine ECSP sind, von diesen Zugriffen nicht betroffen.
    - Anders allerdings, wenn die Daten dann durch Weiter-Übermittlung letztendlich doch bei einem ECSP als Subunternehmen landen!
    - Zudem anders, wenn die Daten durch Leitungen solcher ECSP fließen!

Schrems-II-Urteil des EuGH und die Folgen

Was heißt das nun?

Empfehlungen für Datenexporteure bei Übermittlungen in Drittländer

1.) Bestandsaufnahme aller Übermittlungen Drittländer machen:

- In welche Länder wird übermittelt?
- Welche Daten?
- Welches „Instrument“ wird für die jeweilise Übermittlung genutzt?
  - angemessenes Datenschutzniveau (Art. 45)?
  - Vertragliche Garantie-Instrumente nach Art. 46, z.B. Standarddatenschutzklauseln, BCR,…?
  - Ausnahmeerlaubnisse nach Art. 49?

Schrems-II-Urteil des EuGH und die Folgen

Was heißt das nun?

Empfehlungen für Datenexporteure bei Übermittlungen in Drittländer

2.) Klärung der Rechtslage in Sachen Datenzugriffsmöglichkeiten der Behörden im Drittland

- Kontaktaufnahme mit dem jeweiligen Datenimporteur (Empfänger)
- Darstellung der Problematik
- Frage, in welchem Umfang Behörden dort Zugriff auf die übermittelten Daten nehmen können – i.d.R. wird man um eine genauere rechtliche Analyse / Gutachten nicht herumkommen
- Klären im Einzelfall, anhand des konkreten Datentransfers, inwieweit gerade in diesem Fall Zugriffsmöglichkeiten der Drittstaatsbehörden bestehen
  - bei USA: Klären, ob der Empfänger unter die Pflichten zur Zugangsgewährung an Nachrichtendienste nach FISA Section 702 fällt
  - **Achtung: Auch die Weiterübermittlung an Sub-Dienstleister prüfen!**

Schrems-II-Urteil des EuGH und die Folgen

Was heißt das nun?

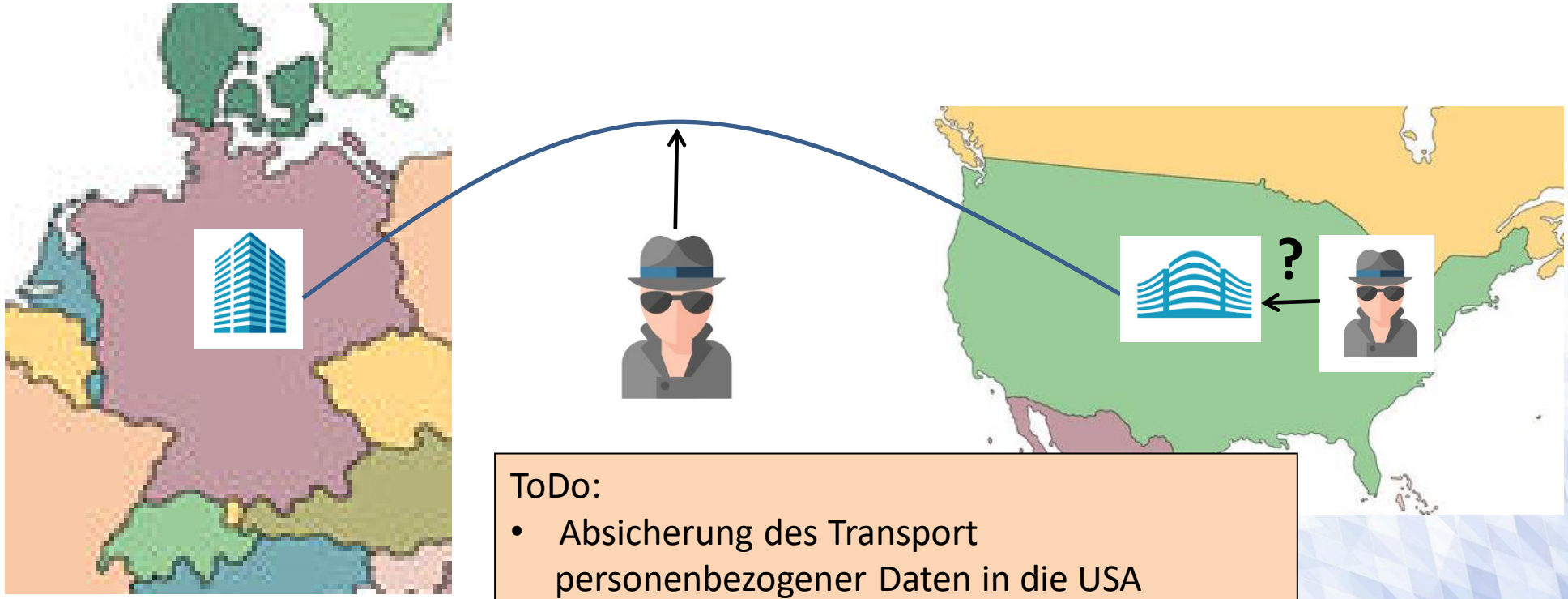
Empfehlungen für Datenexporteure bei Übermittlungen in Drittländer

3.) Risikoanalyse für den konkreten Datentransfer

- Können Drittstaatsbehörden Zugriff gerade auf diese Daten nehmen? In welchem Umfang?
- Entsprechen die Zugriffsmöglichkeiten dem Standard des EU-Rechts (Erforderlichkeit, Verhältnismäßigkeit) – hierzu meist nähere rechtliche Analyse nötig -> Anfordern!
- Haben die betroffenen Personen Rechtsschutzmöglichkeiten? – auch hier meist nähere Analyse nötig
- Wenn im Ergebnis kein vergleichbares Schutzniveau mit der EU besteht, muss nach zusätzlichen Maßnahmen gesucht werden, z.B. Verschlüsselung.
- Wenn auch diese nicht ausreichen, ist der Transfer **unzulässig**.
- Wenn der Transfer fortgesetzt werden soll, muss die Datenschutzbehörde informiert werden (siehe EDSA-FAQ zu Schrems II).

Schrems-II-Urteil des EuGH und die Folgen: die Sicht der IT-Experten

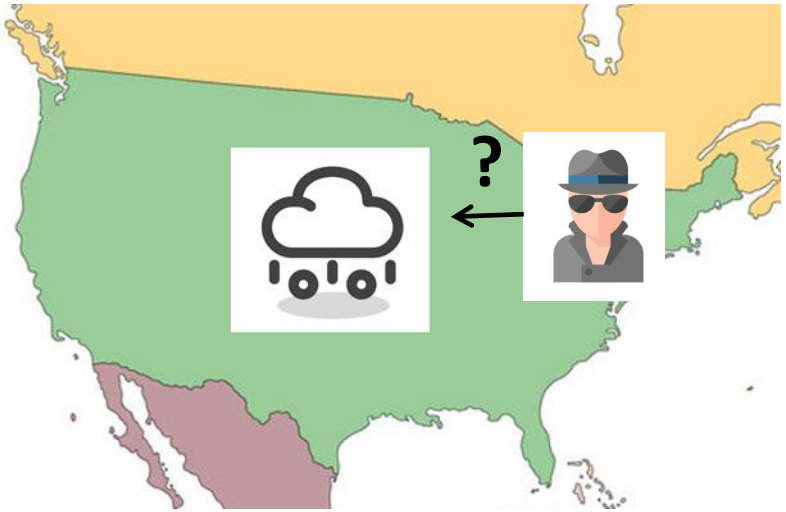
Angreifermodellierung



ToDo:

- Absicherung des Transport personenbezogener Daten in die USA
- Absicherung des Zugiffs in den USA auf Basis einer Rechtsgrundlage noch in Prüfung.

Schrems-II-Urteil des EuGH und die Folgen: die Sicht der IT-Experten



ToDo:

- Absicherung von bei einem US-Unternehmen gespeicherte personenbezogene Daten

Schrems-II-Urteil des EuGH und die Folgen. Die Sicht der IT-Experten

Zwei Varianten:

- Einsatz von **Verschlüsselungsverfahren**
- Einsatz von **Pseudonymisierungsverfahren** (ggf. Anonymisierungsverfahren)

Verschlüsselungsverfahren:

- **Entschlüsselungsschlüssel** ist **nicht** beim US-Unternehmen **vorhanden**. Problem: US-Dienstleister kann nicht auf den Daten arbeiten, z.B. einfache Suchfunktionen
- Verarbeitung verschlüsselter personenbezogener Daten (**Homomorphe Verschlüsselung**) ist noch nicht Stand der Technik
- **Reine verschlüsselte Dateiablage** stark verschlüsselter Daten geht grundsätzlich, wirft aber die Frage nach den Algorithmen, der Implementierung und der Hardware auf
- **Speziellere Lösungen** (z.B. Zeitweiser Transfer eines Entschlüsselungsschlüssel ohne Speicherung) werden wohl demnächst geprüft.

Schrems-II-Urteil des EuGH und die Folgen: die Sicht der IT-Experten

<u>Zwei Varianten:</u>

- Einsatz von **Verschlüsselungsverfahren**
- Einsatz von **Pseudonymisierungsverfahren** (ggf. Anonymisierungsverfahren)

Pseudonymisierungsverfahren:

- Im Einzelfall vorstellbar, wenn eine **De-Pseudonymisierung nur beim Verantwortlichen möglich** ist. Schutzniveau kann theoretische dazu im Einzelfall ausreichend werden.

Vielen Dank für Ihre Aufmerksamkeit

Bayer. Landesamt für Datenschutzaufsicht
Promenade 18, 91522 Ansbach,

www.lda.bayern.de