Datenübertragungen in die USA – Auswirkungen des Angemessenheitsbeschlusses zum Data Privacy Framework

Datenschutz in der Praxis
Studiengang „Informationstechnologie und Recht“
Universität des Saarlandes
19. Dezember 2023

Prof. Dr. Alexander Roßnagel
Der Hessische Beauftragte für
Datenschutz und Informationsfreiheit
Gustav-Stresemann-Ring 1
65189 Wiesbaden
Telefon: 0611 / 1408-0
Internet: https://datenschutz.hessen.de
E-Mail: poststelle@datenschutz.hessen.de

Übersicht

- Drittlandübermittlung
- Zulässigkeit des internationalen Datenverkehrs
- Data Privacy Framework und Angemessenheitsbeschluss der EU-Kommission
- Allgemeine Anforderungen an Datenübermittlungen
- Keine Geltung des Angemessenheitsbeschlusses
- Langfristige Orientierung für Investitionen und Fortentwicklungen

Drittlandübermittlung

Drittlandübermittlung

- Notwendige Datentransfers in der globalisierten Welt
  - Internationaler Handel (Güter, Dienstleistungen und Informationen, …)
  - Internationale Mobilität (Geschäftsreisen, Tourismus, …)
  - Internationale staatliche Zusammenarbeit (Polizeien, Geheimdienste, …)
  - Internationale Konzerne (Produktions- und Personaldaten, …)

- Unbekannte und unbewusste internationale Datentransfers
  - Cloud Computing (Speicher, Software, Services, …)
  - Dienste der GAFAM (Plattformen, Werkzeuge, Informationen, …)
  - Übermittlungsdienste (Telekommunikation, Mobilfunk, …)
  - Arbeitsmittel (Bürosoftware, Videokonferenzen, …)

Zulässigkeit des internationalen Datentransfers

Anforderungen des Kapitel V DSGVO

- Allgemeine Zulässigkeit der Datenübertragung nach Art. 6 und 9 DSGVO
- Besondere Anforderungen für Datenübertragungen ins EU-Ausland
  - Grundsatz nach Art. 44 DSGVO: Datenerlaubnis nach Art. 45 bis 49 DSGVO notwendig
  - Anerkennung der Angemessenheit des Schutzniveaus im Drittland nach Art. 45 DSGVO
  - Geeignete Garantien nach Art. 46 und 47 DSGVO – z.B. Standardvertragsklauseln oder BCR
  - Ausnahmen für bestimmte Fälle nach Art. 49 DSGVO: einmalige Einwilligung oder Vertrag
- Entscheidend: Art. 44 Satz 2 DSGVO
  - „Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird."

Sonderregelungen für USA

- Datenschutz in USA
  - Kein Grundrecht auf Datenschutz, kein allgemeines Datenschutzgesetz
  - Grundsatz der freien Datenverarbeitung (Meinungsfreiheit)
  - Vorrang für innere Sicherheit
- Safe Harbor (2000)
  - Erklärungen der US-Regierung, Anerkennung grundlegender Prinzipien, Selbstzertifizierung
  - EuGH: Urteil vom 6.10.2015 (Schrems I): unionsrechtswidrig und nichtig
- Privacy Shield (2016)
  - Weitgehende Wiederholung von Safe Harbor, kosmetische Verbesserungen
  - EuGH: Urteil von 16.7.2020 (Schrems II): unionsrechtswidrig und nichtig

Unsichere Drittländer

- EuGH: Prüfung des Schutzniveaus und Vergleich mit DSGVO
  - EuGH: In USA fehlt angemessenes Datenschutzniveau, weil
    - unbestimmte und unangemessene Zugriffsrechte staatlicher Behörden und
    - fehlender Rechtsschutz für US-Ausländer
  - Untersucht: FISA und EO 12333: Zugriff auf Daten in USA
  - Ergebnis muss auch für Zugriff auf Datenverarbeitung von US-Unternehmen und ihren Töchter in Europa gelten (nach FISA und Cloud Act) im Rahmen von Art. 28 DSGVO
- Weitere unsichere Drittländer
  - z.B. Russland, China, Indien, …
- Jüngste Untersuchungen
  - Vladek, Memo on Current State of U.S. Surveillance Law and Authorities (DSK)
  - Czarnocki/Giglio/Kun u.a., Government access to data in third countries (EDSA)
  - Roßnagel/Geminn/Johannes/Müller, Auswirkungen ausländischer Gesetzgebung auf die deutsche Cybersicherheitsstrategie, DuD 2022, 156 (NCSR)

Aufgaben des Verantwortlichen

- Schrems-II-Urteil des EuGH
- EDSA-Empfehlung 1/2020
  - zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten
- Sechs Prüfschritte für Datenexporteur

1. Kennen der eigenen Datenübermittlungen (Empfänger, Zwecke)
2. Überprüfung des gewählten rechtlichen Übermittlungsinstruments
3. Beurteilung der Rechtslage im Drittland (beeinträchtigt Schutzniveau?)
4. Auswahl und Anwendung der zusätzlichen Schutzmaßnahmen
5. Einleitung aller förmlichen Verfahrensschritte
6. Dokumentation der Prüfungen und regelmäßige Wiederholung

Data Privacy Framework und Angemessenheitsbeschluss

Beschluss der EU-Kommission vom 10.7.2023

- Keine Gesetzesänderungen in USA
- Kein Vertrag mit der Europäischen Union
- Einseitige Erklärungen der US-Regierung (Data Privacy Framework – DPF)
  - EO 14086: Enhancing Safeguards for United States Signal Intelligence Activities (7.10.2022)
  - Erklärungen des US Dep. of Transportation (DOT) und des US Dep. of Commerce (DOC)
- Feststellung der EU-Kommission nach Art. 45 DSGVO
  - auf der Grundlage des DPF
  - angemessenes Schutzniveau, das mit der DSGVO vergleichbar ist

Geltung des Angemessenheitsbeschlusses

- Nicht für gesamte USA
- Nur sektoral für bestimmte Empfänger
  - Aufsicht der Federal Trade Commission (FTC) oder des US Department of Transportation (DOT) (zB nicht Banken, Versicherungen und Telcos)
  - Selbstzertifizierung, dass sie die Regeln des DPF einhalten
  - In Liste des US Department of Commerce (DOC) zusammen mit erfassten Datenarten aufgenommen, https://www.dataprivacyframework.gov/s/
- Ausnahmen
  - journalistische Daten
  - Beschäftigtendaten, es sei denn gelistet als HR Data (gilt für alle übermittelten HR-Data)
- Prüfpflicht des Datenexporteurs

Wirkung des Angemessenheitsbeschlusses in EU

- Feststellungswirkung
  - Bindende Feststellung, dass für Teilnehmer am DPF das Datenschutzniveau angemessen ist
  - Datenübermittlung an diese Empfänger erfüllt die Anforderung des Art. 44 DSGVO
  - Aufsichtsbehörden sind an diese Feststellung gebunden
  - Schrems-II-Regelungen gelten für die Übermittlung an diese Empfänger nicht mehr
- Ausnahme
  - Aufsichtsbehörden haben konkrete Hinweise, dass angemessenes Niveau verfehlt wird
- Keine Auswirkung auf Rechtmäßigkeit und auf andere Vorgaben der DSGVO an normale Übermittlung. Diese müssen gegeben sein.

Wirkung des Angemessenheitsbeschlusses in USA

- Geltung der DPF Principles (Annex I des Angemessenheitsbeschlusses)
  - Rechtmäßigkeit (statt Art. 6 DSGVO) „Notice and Choice“-Mechanismus. Weiterübermittlungen an Dritte und Zweckänderungen sind nur zulässig, wenn der Importeur die betroffenen Personen ua über die Kategorien der erhobenen Daten, die Zwecke sowie die Empfänger informiert („Notice“) und eine Opt-out-Möglichkeit („Choice“) anbietet
  - Für besondere Kategorien ist ausdrückliche Einwilligung („Opt-in“) notwendig
  - Transparenz: Datenschutzrichtlinie veröffentlicht
  - Zweckbindung: nur vereinbare Zwecke nach Erwartungen einer vernünftigen Person
  - Erforderlichkeit: für jeweiligen Zweck
  - Sicherheit: geeignete und angemessene technische und organisatorische Maßnahmen
  - Rechenschaftspflicht: ausreichende Dokumentation
  - Betroffenenrechte: Rechte auf Berichtigung, Löschung und Auskunft (eingeschränkt)

Datenverarbeitung durch staatliche Stellen in USA

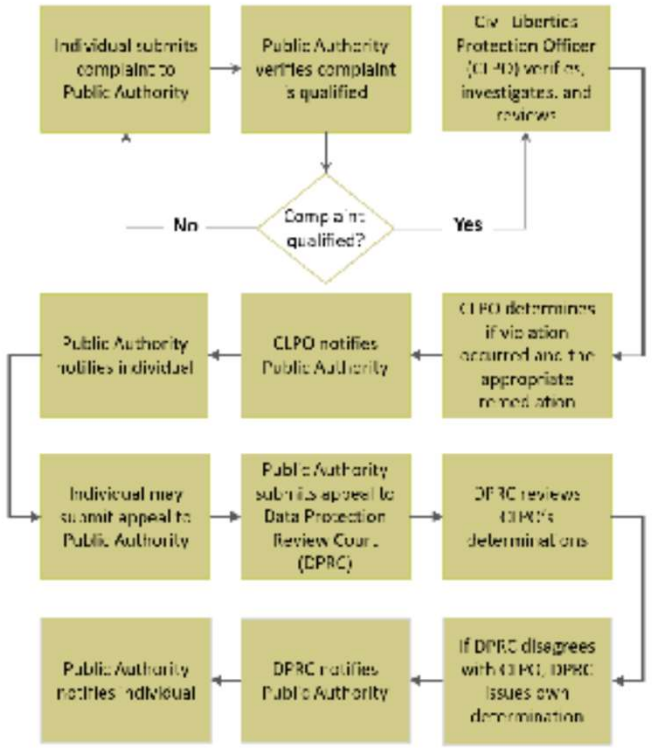
- Strafverfolgung
  - Gerichtliche Anordnung auf Grundlage hinreichender Verdachtsgründe im Einzelfall
  - Begrenzung des Umfangs auf das für die Zwecke der Strafverfolgung erforderliche Maß
- Nationale Sicherheit
  - EO 14086: Enhancing Safeguards for United States Signal Intelligence Activities
  - Beschränkung der Überwachungsaktivitäten
    - Sicherungs- und Aufklärungsinteressen haben höchste Priorität
    - Necessity and Proportionality: Auf Überwachungsziel zugeschnittene erforderliche Maßnahmen
    - Beibehaltung FISA sec. 702 und EO 12333, bulk surveillance (wie PRISM und UPSTREAM) möglich

Rechtsbehelfe in USA

- Zivil- und Strafgerichte
  - Normale Rechtsbehelfe – Problem des „Standing“: Nachweis unmittelbarer persönlicher Betroffenheit notwendig
  - Maßstab allein US-Recht
- Nationale Sicherheit
  - Zweistufiger Beschwerdemechanismus nach EO 14086
    - Beschwerde über eine anerkannte Organisation (Aufsichtsbehörde in EU) wegen Verstoß gegen US-Recht
    - Überprüfung durch Civil Liberties Protection Officer (CLPO) beim Director of National Intelligence
    - Zweite Überprüfung beim Data Protection Review Board (DPRB) beim Attorney General
    - Vorgegebene Entscheidungsformel: „Die Untersuchung konnte entweder keine Grundrechtsverletzung identifizieren oder hat zu einer angemessenen Abhilfe geführt“

Data Privacy Framework: Redress Mechanism

Steps to review complaints concerning U.S. signals intelligence activities for any covered violation of U.S. law and, if necessary, order remediation.



See Executive Order 14086 §§ 3, 4(d), and 4(k), Intelligence Community Directive 126, and 28 CFR Part 201.

Civil Liberties Protection Officer (CLPO)
More about the CLPO's Office at DNI.gov/CLPT

Allgemeine Anforderungen an Datenübermittlung

Anforderungen der Kapitel II bis IV DSGVO

- Gewährleistung der Datenschutzgrundsätze nach Art. 5 DSGVO
- Allgemeine Zulässigkeit der Datenübertragung nach Art. 6 und 9 DSGVO
- Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO
- Pflichten des Verantwortlichen
  - Datenschutz bei Design, Art. 25 DSGVO
  - Gemeinsame Verantwortung, Art. 26 DSGVO
  - Auftragsdatenverarbeitung, Art. 28 DSGVO
  - Sicherheitsmaßnahmen, Art. 32 DSGVO

Probleme mit Auftragsverarbeitern (Art. 28 DSGVO)

- Beispiele: Cloud, Videokonferenzsysteme, MS 365

- Unzureichende Möglichkeit zur Zweck- und Mittelbestimmung durch Auftraggeber
- Zustimmung zur Verarbeitung von Daten zu eigenen Zwecken von MS
- Erlaubnis, Daten nach US-Gesetzen (z.B. Cloud-Act, FISA 702) offen zu legen
- Einverständnis, nicht alle Daten entsprechend Art. 32 DSGVO sicher zu verarbeiten
- Unzureichende Informationen über Unterauftragsverarbeiter
- Unzureichend Zusicherung der Datenlöschung nach Vertragsende

Insbesondere MS 365

- Feststellung der DSK vom 24.11.2022
  - Wegen AGB zu Auftragsverarbeitung ist ein rechtmäßiger Betrieb von MS 365 nicht möglich
- Verantwortung des Verantwortlichen
  - Art. 5 Abs. 2 DSGVO: Erfüllung und Nachweis der Einhaltung der DSGVO-Anforderungen
- Einschreiten
  - Beschwerde wegen rechtswidriger Datenverarbeitung mit MS 365
- Systematische Prüfung
  - Verantwortliche müssen ihre Möglichkeiten nutzen, auf datenschutzkonforme Vereinbarungen mit MS hinzuwirken
  - Handreichung zur rechtmäßigen Vereinbarung über Auftragsverarbeitung

Keine Geltung des Angemessenheitsbeschlusses

Gründe für Nicht-Geltung

- Falsche Branche
  - Behörden, Kreditinstitute, Versicherungen, Telekommunikationsanbieter – z.B. Zoom
- Fehlende Zertifizierung
  - Nicht in Liste des Dep. of Commerce aufgeführt
- Falsche Daten
  - Journalistische Daten, Beschäftigtendaten

Weitergeltung des Schrems-II-Regimes

- Es gelten die Regeln gemäß der Schrems II-Entscheidung des EuGH
- Garantien nach Art. 46 und 47 DSGVO notwendig
  - Standardvertragsklauseln
  - Verbindliche unternehmensinterne Datenschutzvorschriften
- Zusätzliche Schutzmaßnahmen notwendig
  - EDSA-Empfehlungen 1/2020 und 2/2020
  - Transfer Impact Assessment – Bewertung der Rechtslage im Empfängerland
  - EO 14086 gilt auch außerhalb des DPF
  - Auswahl geeigneter technisch-organisatorischer Schutzmaßnahmen

Langfristige Orientierung für Investitionen

Bestand des Angemessenheitsbeschlusses?

- Mögliche Rechtsmittel
  - Keine direkte Anrufung des EuGH durch betroffene Personen
  - Möglichkeit der Vorlage an den EuGH durch Gerichte nach Art. 267 AEUV
  - Klage einer Aufsichtsbehörde nach § 21 BDSG beim BVerwG und Vorlage an EuGH
- Entscheidung des EuGH
  - Maßstab: Art. 8, 47 GRCh sowie Art. 45 und 44 II DSGVO
  - Große Zweifel an der Angemessenheit des DPF (Argumente des EDSA und des EP)
  - Rechtssicherheit erst nach EuGH-Entscheidung

Langfristige rechtssichere Lösung

- Aufhebung des Angemessenheitsbeschlusses durch EuGH
  - Nichtigkeit der Beschlusses ex nunc
  - Unzulässigkeit jeder Datenübertragung ohne Rechtsgrundlage und geeignete Schutzvorkehrungen
- Aufhebung des DPF und der EO durch Präsidenten der USA
  - Notwendige Folge: Widerruf des Angemessenheitsbeschlusses
- Notwendige Vorsorge
  - Abhängigkeit von „unsicheren Staaten“ soweit möglich vermeiden (digitale Souveränität)
  - Beibehaltung und Vereinbarung von Rechtsgrundlagen (z.B. Datenschutzklauseln)
  - Beibehaltung etablierter Schutzmaßnahmen