Drittstaatenverarbeitung
Am Beispiel USA

Dr. Bernd Schütze
Leiter GMDS Arbeitsgruppe Datenschutz und IT-Sicherheit

Fachtagung „Datenschutz im Gesundheitswesen“
4. Mai 2023

Bernd Schütze: (Kurz-) Vita

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.
Dr. Bernd Schütze
Leiter Arbeitsgruppe "Datenschutz und IT-Sicherheit im Gesundheitswesen" (DIG)

☎ +49 (173) 277 11 14
✉ schuetze@medizin-informatik.org

- Studium
  - Informatik (FH-Dortmund)
  - Humanmedizin (Uni Düsseldorf / Uni Witten/Herdecke)
  - Jura (Fern-Uni Hagen)
- Ergänzende Ausbildung
  - Datenschutzbeauftragter (Ulmer Akademie für Datenschutz und IT-Sicherheit)
  - Datenschutz-Auditor (TüV Süd)
  - Medizin-Produkte-Integrator (VDE Prüf- und Zertifizierungsinstitut)
- Berufserfahrung
  - Über 10 Jahre klinische Erfahrung
  - Mehr als 20 Jahre IT im Krankenhäusern
  - > 30 Jahre Datenschutz im Gesundheitswesen
- Mitarbeit in wiss. Fachgesellschaften
  - Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)
  - Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)
  - Gesellschaft für Informatik (GI)
- Mitarbeit in Verbänden
  - Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)
  - Bundesverband Gesundheits-IT e. V (bvitg)
  - HL7 Deutschland e.V.

Angestellt bei: Deutsche Telekom Healthcare – DTHS

T Healthcare Solutions

Wer ist das eigentlich: GMDS?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

GMDS: 4 Fächer, verbunden in einer medizinischen Fachgesellschaft

- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie
- Wirkungsfelder
  - Medizinische Informatik
  - Medizinische Biometrie
  - Medizinische Epidemiologie
  - Medizinische Dokumentation
- Konstituierte sich 1955
  - Älteste Fachgesellschaft in Europa auf dem Gebiet der Medizinischen Informatik
- Unabhängige wissenschaftlich-medizinische Fachgesellschaft
- Etwa 2000 Mitglieder
  - Über 40 fördernde Mitglieder (Organisationen, IT-Hersteller, Pharmaunternehmen)

Agenda

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Was möchte ich heute vorstellen?

- Verarbeitung in einem Drittland: Einführung ins Thema
- Grundsätze (Kap. V DS-GVO)
- Anforderungen des EuGH aus „Schrems II“
- „Angemessenes“ Schutzniveau
  - Interne Datenschutzvorschriften (Binding Corporate Rules)
  - Ausnahmeregelungen
  - Standardvertragsklauseln (inkl. ergänzender Schutzmaßnahmen)
- Sonderfälle im deutschen Recht
- Datenschutzrecht in den USA: Eine (grobe) Übersicht
- Ausblick: Angemessenheitsbeschluss für die USA aufgrund E.O. 14086
  - E.0. 14086 und Anforderungen des EuGH
  - Position LIBE-Ausschuss des EU-Parlaments
- Transfer Impact Assessment: Beispiel

Verarbeitung in einem Drittland:

Einführung ins Thema

Zielrichtung der DS-GVO

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Definition eines Drittlands

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand und Ziele

(1) Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.

(2) Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

(3) Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

Drittland: Was ist das?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Freier Verkehr personenbezogener Daten in der Union

- Keine Definition in Art. 4 DS-GVO („Begriffsbestimmungen“)
- Drittland (oder auch „Drittstaat“):
  - Staaten, die weder der EU angehören, noch zu den Staaten des EWR zählen
- Verarbeitung dort grundsätzlich erlaubt, aber:
  - In diesen Staaten gilt anderes als europäisches Recht
  - Daher Verarbeitung dort **nur unter bestimmten Voraussetzungen erlaubt**

Grundsätze

Kapitel V Datenschutz-Grundverordnung

Verarbeitung personenbezogener Daten in einem Drittstaat

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Information der betroffenen Person: Ansicht der irischen Aufsichtsbehörde*

- Informationspflichten für den Verantwortlichen nach Art. 13 Ab. 1 lit. DS-GVO
  - „[…] verbindliche Informationen bereitzustellen, so dass die betroffene Person entweder
    i. darüber informiert wird, dass die Übermittlung Gegenstand eines Angemessenheitsbeschlusses ist, oder
    ii. darüber, dass die Übermittlung nicht Gegenstand eines Angemessenheitsbeschlusses ist […]“
    → Irische Aufsicht: Die Information muss auf jeden Fall erteilt werden, auch wenn sie nur negativ ausfällt
  - „Um es klar zu sagen: Es reicht nicht aus, einfach einen Link zu einer allgemeinen Webseite der Europäischen Kommission zu setzen. Die Transparenzleitlinien machen deutlich, dass die betroffene Person in der Lage sein sollte, auf das jeweilige Dokument, auf das sie sich beruft, zuzugreifen (oder Zugang zu erhalten, wenn der Zugang nicht direkt gewährt wird), d. h. in diesem Fall auf die **spezifischen Standardvertragsklauseln** oder die **spezifische Angemessenheitsentscheidung**“
    → Irische Aufsichtsbehörde: Verantwortliche müssen ausdrücklich über die verwendeten Klauseln sowie ergänzende Anhänge informieren

* Online, unter https://edpb.europa.eu/system/files/2021-09/dpc_final_decision_redacted_for_issue_to_edpb_01-09-21_en.pdf

Verarbeitung personenbezogener Daten in einem Drittstaat

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Allgemeine Voraussetzungen

- Grundsatz: Schutz personenbezogener Daten europäischer Bürger bleibt auf den Niveau der EU erhalten
- Verantwortlicher und Auftragsverarbeiter gewährleisten, dass
  - bei einer Verarbeitung in einem Drittland
  - oder einer Verarbeitung durch eine internationale Organisation

  das durch die DS-GVO gewährleistete **Schutzniveau** für natürliche Personen **vollumfänglich erhalten bleibt**
- Verantwortlicher und/oder Auftragsverarbeiter in Drittland
  - Bestellten einen schriftlichen Vertreter (Art. 27 DS-GVO)
  - Vertreter ist in dem EU-Land, in dem sich Betroffene befinden, niedergelassen
  - Anlaufstelle für Aufsichtsbehörden und Betroffene

Verarbeitung personenbezogener Daten in einem Drittstaat

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Vor Verarbeitungsbeginn im Drittland ist zu prüfen…

Zwei Voraussetzungen müssen nach Art. 44 DS-GVO erfüllt sein:

1) Die „sonstigen Bestimmungen dieser Verordnung“ müssen eingehalten werden
   - Insbesondere muss die Rechtmäßigkeit der Verarbeitung gewährleistet sein, d.h. ein Erlaubnistatbestand muss vorliegen (Artt. 6,9 DS-GVO)
2) Vorgaben Kap. V (Art. 44ff DS-GVO) erfüllt, insbesondere
   a) Feststellung angemessenes Schutzniveau durch EU-Kommission (Art. 45 DS-GVO)
   b) Datenübermittlung vorbehaltlich geeigneter Garantien (Art.46 DS-GVO)
   c) Verbindliche interne Datenschutzvorschriften (Art. 47 DS-GVO)
   d) Ausnahmen für bestimmte Fälle existieren (Art. 49 DS-GVO)

   Alle Instrumente müssen ein dem EU-Datenschutzniveau angeglichenes Verhältnis im Drittland gewährleisten*

* Siehe auch Urteil EuGH in der Sache Schrems, AZ C-362/14. https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A62014CJ0362

Verarbeitung personenbezogener Daten in einem Drittstaat – Was ist eine „Übermittlung“?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Kapitel V: Übermittlungen pbD an Drittländer oder an internationale Organisationen

- Was ist Übermittlung?

Deutsch	Englisch
Art. 4 Ziff. 2 „Verarbeitung“ jeden […] die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung,	Art. 4 ‘processing’ means […] use, disclosure by transmission, dissemination or otherwise making available,
Kap. V Übermittlung …	Chapter V Transfer…

- „Übermittlung“ der DS-GVO ist nicht die Begrifflichkeit aus dem „alten“ BDSG
- DS-GVO enthält – ebenso wie die DSRL – keine Definition für „Übermittlung“
- Begriff „transfer“ sehr weit zu verstehen*: Alle Handlungen, durch welche ein Empfänger Kenntnis der pbD erhält (z.B. auch Einsichtnahme während einer Fernwartung)

* So z.B. Schantz P.: Art. 44 Rn. 10 in: Simitis/Hornung/Spiecker (Hrsg.) Datenschutzrecht. Nomos Verlag, 1. Auflage 2019. ISBN 978-3848735907

Übermittlung an einen Empfänger

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Kapitel V: Übermittlungen pbD an Drittländer oder an internationale Organisationen

- „transfer“: Alle Handlungen, durch welche ein Empfänger Kenntnis der pbD erhält
  - Empfänger im Sinne von Art. 4 Ziff. 9 DS-GVO, d.h. es spielt keine Rolle
    - ob Empfänger eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, ist oder
    - ob es sich um einen Dritten handelt oder nicht
    - Ausnahme entsprechend Art. 4 Ziff. 9 S. 2 DS-GVO:
      - → Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, sind keine Empfänger
      - → Wird in den seltensten Fällen für Behörden in Drittländern gelten!

Internetseite – Abruf aus einem Drittland: Eine Übermittlung?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Veröffentlichung im Internet

- EuGH in Rechtssache Lindqvist: Urt. v. 2003-11-06, AZ C-101/01 (URL http://curia.europa.eu/juris/liste.jsf?language=de&num=C-101/01#)
- Urteil unter DSRL, aber vergleichbar:
  - Art. 25 Abs. 4 DSRL vs. Art. 45 Abs. 1 DS-GVO
- EuGH unterteilt Vorgang in zwei Phasen
  1. Hochladen der Information auf den Hostprovider: Wenn Hostprovider in EU keine Übermittlung (auf Serverstandort wurde nicht eingegangen)
  2. Abruf der Informationen durch Internetnutzer
- EuGH befasst sich mit Phase 1 und beschränkt dadurch indirekt die Verantwortung des Verantwortlichen auf diese Phase

D.h.

→ Hochladen von Informationen zu einem Hostprovider = Drittlandfrage abhängig vom Standort Hostprovider

→ Aber Aufruf einer Webseite durch Internetnutzer = Keine Übermittlung (in ein Drittland)

Weiterübermittlung im Drittland

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Art. 44 S. 1 HS 2 DS-GVO: Auf Weiterübermittlung achten

- **Alle Vorgaben der DS-GVO müssen** auch **im Falle einer Weiterübermittlung** durch den Drittlandempfänger **gewährleistet werden**
  („ die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden“)
  - ErwGr. 101: „In jedem Fall sind derartige Datenübermittlungen an Drittländer und internationale Organisationen nur unter **strikter Einhaltung dieser Verordnung zulässig**.“
- Dies **gilt** insbesondere **auch, wenn Drittlandempfänger Daten auf Grund für ihn geltenden Rechtsvorgaben die ihm übermittelten Daten an Behörden in einem Drittland weitergeben**
- Hinweis: Weiterübermittlung sollte durch den Verantwortlichen vertraglich ausgeschlossen werden

Anforderungen des EuGH

Erinnerung an das Schrems II Urteil des EuGH

EuGH: Rechtssache „Facebook Ireland und Schrems“ (“Schrems II)

Verarbeitung in einem Drittstaat

- Erinnerung: Art. 2 Abs. 2 lit. c DS-GVO

  „Diese Verordnung findet keine Anwendung auf die Verarbeitung personenbezogener Daten

  …

  c) durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.“
- **Ausnahmetatbestand** in Art. 2 Abs. 2 lit. c DS-GVO **gilt für Behörden in der Union**
- Ausnahmetatbestand gilt **nicht für Behörden in Drittstaaten**
- Zugriffe von Behörden in Drittstaaten müssen der DS-GVO genügen, wenn die in Artt. 2 und 3 (sachlicher und räumlicher Anwendungsbereich) genannten Tatbestände erfüllt sind

EuGH: Rechtssache „Facebook Ireland und Schrems“ (“Schrems II)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

EuGH, Urteil v. 20. Juli 2020, AZ C-311/18 *

Grundsätzliches:

- Rn. 83: Übermittlungen in Drittstaaten sind Verarbeitungen i.S.v. Art. 4 Nr. 2 DS-GVO, die DS-GVO findet Anwendung
- Rn. 87: Die **etwaige Verarbeitung** der betreffenden Daten durch ein Drittland für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates **stellt die Anwendbarkeit der DS-GVO** auf die fragliche Übermittlung **nicht in Frage**.
- Rn. 92: Schutzniveau der DS-GVO muss bei Übermittlung gewährleistet werden

→ Regelungen in Standardvertragsklauseln, BCR usw. müssen im Licht des Schrems II Urteils bewertet werden

* Urteil online abrufbar beim EuGH unter URL
https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1
bzw. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62018CJ0311

EuGH: Rechtssache „Facebook Ireland und Schrems“ (“Schrems II)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

EuGH, Urteil v. 20. Juli 2020, AZ C-311/18

Antwort auf Vorlagefrage 1 (Rn. 89):

> Eine **Übermittlung** personenbezogener Daten durch einen in einem Mitgliedstaat ansässigen Wirtschaftsteilnehmer an einen anderen, in einem Drittland ansässigen Wirtschaftsteilnehmer **fällt in den Anwendungsbereich** dieser Verordnung, **wenn** die Daten **bei ihrer Übermittlung oder im Anschluss daran von den Behörden dieses Drittlands** für Zwecke der öffentlichen Sicherheit, der Landesverteidigung und der Sicherheit des Staates **verarbeitet werden können**.

- Grundsätzlich ist bei einer Beauftragung zu betrachten, ob durch einen Auftragsverarbeiter (= Wirtschaftsteilnehmer) personenbezogene Daten durch Behörden im Drittstaat verarbeitet werden **können**

→ D.h. die alleinige Möglichkeit reicht aus

→ Zugriffsmöglichkeiten von Behörden im Drittland sind aus Sicht der DS-GVO zu berücksichtigen

EuGH: Rechtssache „Facebook Ireland und Schrems“ (“Schrems II)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

EuGH, Urteil v. 20. Juli 2020, AZ C-311/18

Antwort auf Vorlagefragen 2,3 und 6 (Rn. 105):

Aussage 1:

Art. 46 Abs. 1 und Art. 46 Abs. 2 Buchst. c der DSGVO sind dahin auszulegen, dass die nach diesen Vorschriften erforderlichen geeigneten Garantien, **durchsetzbaren Rechte und wirksamen Rechtsbehelfe gewährleisten müssen**, dass die **Rechte der Personen**, deren personenbezogene Daten auf der **Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt werden**, ein **Schutzniveau genießen**, das dem in der Union durch die DSGVO im Licht der Charta garantierten Niveau der Sache nach **gleichwertig ist**.

Kurzer Exkurs: Charta der Grundrechte der Europäischen Union

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht*

- → Rn. 104 EuGH-Urteil Schrems II: „[…] und den betroffenen Personen sollten wirksame und durchsetzbare Rechte sowie wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe eingeräumt werden."
- → Rn. 141 EuGH-Urteil Schrems II: „[…] und gemäß Artikel 47 der Charta einen wirksamen gerichtlichen Rechtsbehelf einzulegen, wenn sie sich in ihren Rechten gemäß dieser Verordnung verletzt sieht […]"

Art. 47 „Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht":

- **Jede Person**, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, **hat das Recht**, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen **bei einem Gericht einen wirksamen Rechtsbehelf einzulegen**.
- Jede Person hat ein Recht darauf, dass ihre Sache von einem unabhängigen, unparteiischen und **zuvor durch Gesetz errichteten Gericht** in einem **fairen Verfahren, öffentlich** und innerhalb angemessener Frist **verhandelt wird**. Jede Person kann sich beraten, verteidigen und vertreten lassen.

* Grundrechtecharta online abrufbar bei EUR-Lex unter URL https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:12012P/TXT&from=DE

Kurzer Exkurs: DS-GVO immer unter Beachtung Grundrechtecharta

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Recht auf einen wirksamen Rechtsbehelf und ein unparteiisches Gericht*

Art. 49 Abs. 1 DS-GVO „Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter “:

- **Jede betroffene Person hat** unbeschadet eines verfügbaren verwaltungsrechtlichen oder außergerichtlichen Rechtsbehelfs einschließlich des Rechts auf Beschwerde bei einer Aufsichtsbehörde gemäß Artikel 77 **das Recht auf einen wirksamen gerichtlichen Rechtsbehelf**, wenn sie der Ansicht ist, dass die ihr aufgrund dieser Verordnung zustehenden Rechte infolge einer nicht im Einklang mit dieser Verordnung stehenden Verarbeitung ihrer personenbezogenen Daten verletzt wurden.
- Rechtsbehelf muss im Sinne von Art. 47 Grundrechtecharta verstanden werden
  - Siehe z.B. EuGH, Urt. v. 12. Januar 2023, Rechtssache C-132/21 https://curia.europa.eu/juris/document/document.jsf?text=&docid=269145&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1&cid=148441
  - Rn. 57: „Nach alledem ist auf die Vorlagefragen zu antworten, dass Art. 77 Abs. 1, Art. 78 Abs. 1 und Art. 79 Abs. 1 der Verordnung 2016/679 in Verbindung mit Art. 47 der Charta dahin auszulegen sind […]“

* Art.78 DS-GVO, online abrufbar bei EUR-Lex unter URL https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE#d1e6150-1-1

EuGH: Rechtssache „Facebook Ireland und Schrems“ (“Schrems II)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

EuGH, Urteil v. 20. Juli 2020, AZ C-311/18

Antwort auf Vorlagefragen 2,3 und 6 (Rn. 105):

- Wirksamer gerichtlichen Rechtsbehelf i.S.v. Art. 47 Grundrechtecharta muss existieren
- Dabei zu beachten:
  - Betroffene Personen MÜSSEN den Rechtsweg gegen Behörden nutzen können
  - Betroffenenrechte MÜSSEN gewährleistet werden, d.h. u.a. es MUSS eine Information betroffener Personen bei einer Verarbeitung ihrer Daten durch Behörden in einem Drittstaat erfolgen
  - US-Behörden belegen i.d.R. US Unternehmen mit „Gag Orders“, d.h. keine Information
  - Wie können betroffene Personen ohne Information einen wirksamen gerichtlichen Rechtsbehelf – sofern überhaupt vorhanden – nutzen?

EuGH: Rechtssache „Facebook Ireland und Schrems“ (“Schrems II)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

EuGH, Urteil v. 20. Juli 2020, AZ C-311/18

Antwort auf Vorlagefragen 2,3 und 6 (Rn. 105):

Aussage 2:

Bei der insoweit im Zusammenhang mit einer solchen Übermittlung vorzunehmenden **Beurteilung sind insbesondere die vertraglichen Regelungen zu berücksichtigen**, die zwischen dem in der Union ansässigen Verantwortlichen bzw. seinem dort ansässigen Auftragsverarbeiter und dem im betreffenden Drittland ansässigen Empfänger der Übermittlung vereinbart wurden, **sowie**, was einen **etwaigen Zugriff der Behörden dieses Drittlands** auf die übermittelten personenbezogenen Daten betrifft, die maßgeblichen Elemente der Rechtsordnung dieses Landes, insbesondere die in Art. 45 Abs. 2 der DSGVO genannten Elemente.

→ „Etwaiger Zugriff“: Möglicher Zugriff reicht aus

→ Verantwortlicher und Auftragsverarbeiter müssen diesen Umstand bei der Bewertung, ob betroffenen Personen ein gleichwertiges Schutzniveau geboten wird, berücksichtigen

EuGH: Rechtssache „Facebook Ireland und Schrems“ (“Schrems II)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

EuGH, Urteil v. 20. Juli 2020, AZ C-311/18

Kurzes Zwischenfazit aus dem EuGH-Urteil:
Standardvertragsklausen, BCR & Co. bleiben gültig, ABER

- → Werden personenbezogene Daten in ein Drittland übermittelt, MUSS ein dem EU-Recht gleichwertiges Schutzniveaus gewährleistet werden
  - ➢ Kein identisches, aber gleichwertiges Schutzniveau
  - ➢ Beurteilungskriterium: Das durch die DS-GVO gewährleistete Schutzniveau für natürliche Personen darf durch Drittland-Verarbeitung nicht untergraben werden (Art. 44 DS-GVO)
- → Dies beinhaltet auch die Existenz eines wirksamen gerichtlichen Rechtsbehelf i.S.v. Art. 47 Charta der Grundrechte der Europäischen Union
  - ➢ Art. 49 Abs. 1 DS-GVO muss im Sinne von Art. 47 Grundrechtecharta verstanden werden
- → Dies gilt auch für die Verarbeitung personenbezogener Daten durch Behörden im Drittland

„Angemessenes“ Schutzniveau

Im Drittland muss ein der EU vergleichbares Schutzniveau existieren

Drittlandverarbeitung nur bei angemessenem Schutzniveau

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Feststellung angemessenes Schutzniveau durch EU-Kommission (Art. 45 DS-GVO)

- Für Drittland, Gebiet oder betreffende internationale Organisation wurde angemessenes Datenschutzniveau festgestellt (vgl. Art. 45 Abs. 1 DS-GVO)
  - Liste online bei der EU Kommission: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
- Aktuell (2023-05-01) vorliegende Angemessenheitsbeschlüsse:
  - Andorra, Argentinien, Kanada (nur kommerzielle Institutionen), Färöer-Inseln, Guernsey, Israel, Isle of Man, Japan, Jersey, Republik Korea, Neuseeland, Schweiz, UK unter Wirkung der DS-GVO, Uruguay

Drittlandverarbeitung nur bei angemessenem Schutzniveau

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Feststellung angemessenes Schutzniveau durch EU-Kommission (Art. 45 DS-GVO)

- Für Drittland, Gebiet oder betreffende internationale Organisation wurde angemessenes Datenschutzniveau festgestellt (vgl. Art. 45 Abs. 1 DS-GVO)
- Regelmäßige Überprüfung erforderlich
  - Mindestens alle 4 Jahre
- Datenübermittlung auf Grund eines Angemessenheitsbeschlusses bedarf keiner besonderen Genehmigung (Art. 45 Abs. 1 S. 2 DS-GVO)
  - Insbesondere auch keine Genehmigung durch eine Datenschutz-Aufsichtsbehörde

„Angemessenes“ Schutzniveau

Art. 47 Interne Datenschutzvorschriften - Binding Corporate Rules

Binding Corporate Rules (BCR)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

BCR kann Auftragsverarbeitern die Verarbeitung im Drittstaat erlauben

Art. 4 Ziff. 20 DS-GVO:

– "verbindliche interne Datenschutzvorschriften"
  - Maßnahmen zum Schutz pbD,
  - zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener
  - Verantwortlicher oder Auftragsverarbeiter
  - verpflichtet im Hinblick auf
  - **Datenübermittlungen** oder eine Kategorie von Datenübermittlungen pbD
  - an einen Verantwortlichen oder Auftragsverarbeiter **derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen**,
  - die eine **gemeinsame Wirtschaftstätigkeit** ausüben,
  - in einem oder mehreren Drittländern;

Binding Corporate Rules (BCR*)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Verbindliche interne Datenschutzvorschriften (Art. 47)

Daher zu unterscheiden

- BCR für Verantwortliche:
  - Regeln Datentransfers durch Verantwortliche an gruppenangehörige Verantwortliche oder Auftragsverarbeiter in einem Drittland
- BCR für Auftragsverarbeiter:
  - Regeln Datenflüsse innerhalb von Unternehmensgruppen, deren Gruppenmitglieder als Auftragsverarbeiter für konzernfremde Auftraggeber agieren.
- Für beide BCR-Arten existieren Leitlinien des EU Datenschutzausschusses

Binding Corporate Rules (BCR*)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Verbindliche interne Datenschutzvorschriften (Art. 47)

- Zuständige Aufsichtsbehörde genehmigte „Verbindliche interne Datenschutzvorschriften“ (Binding Corporate Rules, BCR)
- Voraussetzung: Gemeinsam ausgeübte Wirtschaftstätigkeit durch Mitglieder einer Unternehmensgruppe oder einer Gruppe von Unternehmen (Art. 47 Abs. 1 lit. a)
- Mindestangaben von Art. 47 Abs. 2 vorgegeben, z.B.
  - von BCR erfasste Datenübermittlungen
  - Arten der Daten sowie Art und Zweck der Datenverarbeitung
  - interne und externe Rechtsverbindlichkeit der betreffenden internen Datenschutzvorschriften
- Alle Beschäftigten werden auf Einhaltung BCR verpflichtet

* EU-Kommission: Binding corporate rules - Corporate rules for data transfers within multinational companies. Online https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/binding-corporate-rules_de

Binding Corporate Rules (BCR*)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Verbindliche interne Datenschutzvorschriften (Art. 47)

- Verschiedene Arten
  - Binding Corporate Rules zur Verarbeitung der Daten im Unternehmen
  - Binding Corporate Rules für Verantwortliche und Auftragsverarbeiter
- Voraussetzung zur Nutzung
  - Ausübung gemeinsame Wirtschaftstätigkeit einer
    - Unternehmensgruppe oder
    - Gruppe von Unternehmen
  - Alle Beteiligten müssen die BCR anerkennen, damit BCR die erforderliche Wirkung entfalten
- EDSA Register of approved binding corporate rules (https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_de)

„Angemessenes“ Schutzniveau

Art. 49 Ausnahmeregelungen

Ausnahmeregelungen

Ausnahmen für bestimmte Fälle existieren (Art. 49)

Falls weder Angemessenheitsbeschluss noch geeignete Garantien noch BCR: Übermittlung in Drittland nur unter einer der folgenden Bedingungen zulässig

- **Ausdrückliche Einwilligung** liegt vor
  - Nach Aufklärung über bestehende mögliche Risiken von Datenübermittlungen ohne Vorliegen eines Angemessenheitsbeschlusses und ohne geeignete Garantien
- Übermittlung ist für die **Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen** oder zur D**urchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person** erforderlich
  - Ggf. kann auch ein Behandlungsvertrag eine einmalige Übermittlung genehmigen, z.B. wenn eine bestimmte Methode **nur** in einem Drittland angeboten wird und diese Methode nur **ausnahmsweise** bei einem bestimmten Patienten aufgrund spezieller Symptome/Vorkommnisse bei seiner Erkrankung **erforderlich ist**

Ausnahmeregelungen

Ausnahmen für bestimmte Fälle existieren (Art. 49)

Falls weder Angemessenheitsbeschluss noch geeignete Garantien noch BCR: Übermittlung in Drittland nur unter einer der folgenden Bedingungen zulässig

- Übermittlung ist zum Abschluss oder zur Erfüllung **eines im Interesse der betroffenen Person** von dem Verantwortlichen mit einer anderen Person geschlossenen Vertrags **erforderlich**
  (denkbar z.B. bei ausnahmsweise erforderlicher medizinischer Dienstleistung aus einem Drittland)
- Übermittlung ist aus wichtigen Gründen des öffentlichen Interesses notwendig
  - das öffentliche Interesse muss im Unionsrecht oder im Recht des betreffenden Mitgliedstaates anerkannt sein
- Übermittlung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich

Ausnahmeregelungen

Ausnahmen für bestimmte Fälle existieren (Art. 49)

Falls weder Angemessenheitsbeschluss noch geeignete Garantien noch BCR: Übermittlung in Drittland nur unter einer der folgenden Bedingungen zulässig

- Übermittlung ist zum Schutz **lebenswichtiger Interessen der betroffenen Person** oder anderer Personen erforderlich, sofern die betroffene **Person nicht in der Lage ist, ihre Einwilligung zu geben**
- Übermittlung erfolgt aus einem Register, das gemäß dem Recht der Union oder der Mitgliedstaaten zur Information der Öffentlichkeit bestimmt ist

Ausnahmeregelungen

Ausnahmen für bestimmte Fälle existieren (Art. 49)

- Soweit kein anderer Erlaubnistatbestand (inkl. Ausnahmetatbestand) vorliegt, ist die Übermittlung zulässig (Art. 49 Abs. 1 S. 2), wenn :
  - die Übermittlung nicht wiederholt erfolgt **und**
  - nur eine begrenzte Zahl Personen von der Verarbeitung betroffen sind **und**
  - die Übermittlung zur Wahrung *zwingender* berechtigter Interessen des Verantwortlichen *erforderlich* ist **und**
  - die Interessen oder die Rechte und Freiheiten des einzelnen Betroffenen nicht überwiegen **und**
  - der Verantwortliche *alle* Umstände der Datenübermittlung beurteilt **und**
  - auf der Grundlage dieser Beurteilung geeignete Garantien in Bezug auf den Schutz personenbezogener Daten vorgesehen hat.

Ausnahmeregelungen

Ausnahmen für bestimmte Fälle existieren (Art. 49)

- Der Verantwortliche setzt die Aufsichtsbehörde von der Übermittlung in Kenntnis.
- Der Verantwortliche unterrichtet die betroffene Person über die Übermittlung und seine zwingenden berechtigten Interessen.

Ausnahmeregelungen: Sicht der europäischen Aufsichtsbehörden*

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Leitlinie des Europäischen Datenschutzausschusses

- Ausnahmeregelungen dürfen nur in bestimmten Fällen Anwendung finden
- Ausnahmen sind restriktiv auszulegen, damit die Ausnahme nicht zur Regel wird
- ErwGr. 111: Gelegentliche und nicht wiederholte Übermittlungen
- Art. 48 DS-GVO sowie ErwGr. 115:
  - Behördliche oder gerichtliche Entscheidungen von Drittländern sind keine berechtigenden Grundlagen für die Übermittlung von Daten an ein Drittland
  - Bei Rechtshilfeabkommen: Anforderung muss von nationaler Behörde kommen und von dieser begründet werden

* Datenschutzausschuss: Leitlinien 2/2018 zu den Ausnahmen nach Artikel 49, Online verfügbar unter https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en

Europäische Kommission

„Angemessenes“ Schutzniveau

Art. 46 Abs. 2 lit. c DS-GVO: „Standarddatenschutzklauseln“

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Art. 46 Abs. 2 lit. c DS-GVO: „Standarddatenschutzklauseln“

- Art. 46 Abs. 2 lit. c DS-GVO: „Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Artikel 93 Absatz 2 erlassen werden,“
- Nutzung von der EU Kommission beschlossener Vertragsklauseln: **Keine Anzeigepflicht bei Aufsichtsbehörde**
  („[…] ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre“)
  - Cave: **Jede Abweichung von den Klauseln führt zur Anzeigepflicht**!
- Ergänzungen sind i.d.R. keine Abweichung
  - ErwGr. 109: „[…] noch ihn daran hindern, ihnen weitere Klauseln oder zusätzliche Garantien hinzuzufügen, solange diese weder mittelbar noch unmittelbar im Widerspruch zu den von der Kommission oder einer Aufsichtsbehörde erlassenen Standard-Datenschutzklauseln stehen […]“

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Art. 46 Abs. 2 lit. c DS-GVO: „Standarddatenschutzklauseln“

- Nutzung von Standardvertragsklauseln = Keine Genehmigung einer Aufsichtsbehörde erforderlich (Art. 46 Abs. 2 DS-GVO)
- ABER:
  - Selbstverständlich haben Aufsichtsbehörden ein Kontrollrecht, insbesondere haben sie auch das **Recht** (und **laut EuGH ggf. auch die Pflicht**), **Datenübermittlungen zu kontrollieren**
  - Auf Standardvertragsklauseln basierende Übermittlungen in ein Drittland müssen von Aufsichtsbehörde ggf. **ausgesetzt** oder auch **verboten werden**, wenn durch die Übermittlung EU- oder nationale Datenschutzvorschriften verletzt werden, beispielsweise wenn
    - → der Datenimporteur die Standardvertragsklauseln missachtet,
    - → der Datenimporteur sich weigert, mit den Datenschutzaufsichtsbehörden „redlich“ zusammenzuarbeiten oder
    - → die Datenübermittlung sich wahrscheinlich negativ auf die Rechte betroffener Personen auswirkt

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Vorgabe: Schutzniveau der DS-GVO muss gewährleistet werden

- Werden personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt, so müssen diese daher den **Fortbestand des hohen Schutzniveaus sowohl bei der Übermittlung als auch bei der Verarbeitung in einem Drittland gewährleisten**.
- D. h. werden personenbezogene Daten auf der Grundlage von Standarddatenschutzklauseln in ein Drittland übermittelt, so muss ein Schutzniveau gewährleistet werden, das **dem in der Union garantierten Schutzniveau der Sache nach gleichwertig ist**.

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Vorgabe: Schutzniveau der DS-GVO muss gewährleistet werden

- Bei der im Zusammenhang mit einer Drittland-Übermittlung erforderlichen Beurteilung sind insbesondere
  - die **vertraglichen Regelungen** zu berücksichtigen, die zwischen dem in der **Union ansässigen Verantwortlichen** bzw. seinem dort ansässigen **Auftragsverarbeiter** und dem im betreffenden **Drittland ansässigen Empfänger** der Übermittlung vereinbart wurden, sowie
  - die **maßgeblichen Elemente der Rechtsordnung dieses Landes, soweit diese einen etwaigen Zugriff der Behörden dieses Drittlands auf die übermittelten personenbezogenen Daten betreffen.**

  (Beispielhaft sehen wir uns später gesetzliche Regelungen in den USA an)
- **Können keine hinreichenden zusätzlichen Maßnahmen ergriffen werden**, um einen solchen Schutz zu gewährleisten, muss die **Übermittlung** personenbezogener Daten in das betreffende Drittland **ausgesetzt bzw. beendet werden.**

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Art. 46 Abs. 2 lit. c DS-GVO: „Standarddatenschutzklauseln“

- Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer (Stand 2021-06-07) (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=de&uri=CELEX%3A32021D0914)
- Allgemeine Klauseln werden mit einem modularen Ansatz kombiniert
  - ErwGr. 10: Verschiedenen Datenübermittlungsszenarien und der Komplexität moderner Verarbeitungsketten soll Rechnung getragen werden
- Vier Module
  - Modul 1: Übermittlung von Verantwortlichen an Verantwortliche
  - Modul 2: Übermittlung von Verantwortlichen an Auftragsverarbeiter
  - Modul 3: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter
  - Modul 4: Übermittlung von Auftragsverarbeitern an Verantwortliche

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Art. 46 Abs. 2 lit. c DS-GVO: „Standarddatenschutzklauseln“

Heute im Fokus: **Ausgewählte Bestandteile** von

- Allgemeiner Teil
- Modul 2: Übermittlung von Verantwortlichen an Auftragsverarbeiter
- Ergänzung zur Gewährleistung des Schutzniveaus der EU

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Art. 46 Abs. 2 lit. c DS-GVO: „Standarddatenschutzklauseln“

Allgemeiner Teil

- Klausel 4
  - 4(b): Alle Klauseln sind im Licht der DS-GVO auszulegen
  - 4(c): Klauseln dürfen nicht in einer Art und Weise ausgelegt werden, die in Widerspruch zu den Rechten und Pflichten der DS-GVO stehen

  → **Auch mit Klauseln sind alle Vorgaben der DS-GVO einzuhalten**

  → **Insbesondere muss den Vorgaben von Kap. V DS-GVO genügt werden**
- Klausel 5
  - Bei Widerspruch zwischen vertraglichen Regelungen zwischen Parteien und den Standarddatenschutzklauseln, sind Standarddatenschutzklauseln vorrangig anwendbar

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Art. 46 Abs. 2 lit. c DS-GVO: „Standarddatenschutzklauseln“

Modul 2: Übermittlung von Verantwortlichen an Auftragsverarbeiter

- Klausel 8.3
  - Auf Anfrage stellt der Datenexporteur der betroffenen Person eine Kopie dieser Klauseln, einschließlich der von den Parteien ausgefüllten Anlage, unentgeltlich zur Verfügung
  - Hinweis: An Informationspflichten aus Artt. 13, 14 DS-GVO denken!
- Klausel 8.6(a)
  - Datenexporteur und Datenimporteur treffen entsprechende TOMs während der Datenübermittlung
  - Datenimporteur trifft geeignete TOMs, um die Sicherheit der Daten zu gewährleisten, einschließlich Schutz vor einer Verletzung der Sicherheit inkl. unbefugter Offenlegung
  - Anmerkung: Auch ein Zugriff von Behörden des Drittstaates stellt eine Verletzung dar
- Klausel 8.7
  - Für in **Art. 9 Abs. 1 DS-GVO genannte Kategorien von Daten sind spezielle Beschränkungen und/oder zusätzlichen Garantien erforderlich**!

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Art. 46 Abs. 2 lit. c DS-GVO: „Standarddatenschutzklauseln“

Modul 2: Übermittlung von Verantwortlichen an Auftragsverarbeiter

- Klausel 11(a)
  - Datenimporteur informiert die betroffenen Personen in transparenter und leicht zugänglicher Form mittels individueller Benachrichtigung oder auf seiner Website über eine Anlaufstelle, die befugt ist, Beschwerden zu bearbeiten
  - Datenexporteur muss betroffene Personen entsprechend Artt. 13, 14 DS-GVO informieren
- Klausel 14(a)
  - Datenexporteur und Datenimporteur sichern zu, **keinen Grund zu der Annahme zu haben**, dass durch für den **Datenimporteur geltende Rechtsvorschriften** und Gepflogenheiten im Bestimmungsdrittland, **einschließlich Anforderungen von öffentlichen Behörden zur Offenbarung** oder die den Zugang zu diesen Daten gestatten, **kein Widerspruch** zur **Erfüllung der Pflichten aus den Standarddatenschutzklauseln** bestehen.
  - Hinweis: Mit Unterzeichnung sichert dies auch der Verantwortliche zu.

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Art. 46 Abs. 2 lit. c DS-GVO: „Standarddatenschutzklauseln“

Modul 2: Übermittlung von Verantwortlichen an Auftragsverarbeiter

- Klausel 14(b)
  - Zusicherung berücksichtigt u.a.: relevante Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes (einschließlich solcher, die die Offenlegung von Daten gegenüber Behörden vorschreiben oder den Zugang von Behörden zu diesen Daten gestatten)
  - Datenexporteur muss betroffene Personen entsprechend Artt. 13, 14 DS-GVO informieren
- Klausel 14(c)
  - Datenimporteur versichert, dass er sich im Rahmen der Beurteilung nach Buchstabe b nach besten Kräften bemüht hat, dem Datenexporteur sachdienliche Informationen zur Verfügung zu stellen.
    - Datenimporteur muss sich „bemühen“
    - Laut EuGH Schrems II Urteil muss Verantwortlicher „prüfen“, d.h. „bemühen“ des Datenimporteurs reicht ggf. nicht

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Art. 46 Abs. 2 lit. c DS-GVO: „Standarddatenschutzklauseln“

Modul 2: Übermittlung von Verantwortlichen an Auftragsverarbeiter

- Klausel 15
  - 15(a): Datenimporteur muss Verantwortlichen und (wenn möglich) betroffene Person informieren, wenn behördliche Anfragen des Drittlandes eine Offenlegung oder Weitergabe von Daten verlangen
  - 15(b): Außer, Rechtsvorschriften des Bestimmungslandes untersagen dies
  - Frage: Wie entspricht dies den Vorgaben der DS-GVO, wenn Betroffenenrechte nicht gewährleistet werden können?
- Klausel 17
  - Klauseln unterliegen dem Recht eines der EU Mitgliedstaaten
- Klausel 18
  - Gerichtsstand ist ein Gericht in einem EU Mitgliedstaat

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Art. 46 Abs. 2 lit. c DS-GVO: „Standarddatenschutzklauseln“

Anhänge

- Anhang I(A)
  - Liste der Parteien, also Benennung Datenexporteur und Datenimporteur
- Anhang I(B)
  - Beschreibung der Übermittlung
  - Kategorien betroffener Personen, Kategorien von Daten, Häufigkeit der Übermittlung, Art der Verarbeitung, Zwecke, Dauer, Übermittlungen an Unter-Auftragsverarbeiter (wenn zutreffend)
  - Cave: **Sensible Daten erfordern „Beschränkungen für Weiterübermittlungen oder zusätzliche Sicherheitsmaßnahmen“**
- Anhang I(C)
  - Zuständige Aufsichtsbehörde

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Art. 46 Abs. 2 lit. c DS-GVO: „Standarddatenschutzklauseln“

Anhänge

- Anhang II
  - Beschreibung TOM
  - Einschließlich Beschreibung der Gewährleistung der Sicherheit der Daten
- Anhang III
  - Liste der Unterauftragsverarbeiter

Standarddatenschutzklauseln (EU Kommission: „Vertragsklauseln“)

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Fazit: Standarddatenschutzklauseln alleine reichen nicht

- Betroffenenrechte können alleine durch die Klauseln nicht immer gewährleistet werden
- Zugriffe von Behörden ohne Kenntnis des Verantwortlichen können bei entsprechender Rechtslage im Drittland vertraglich nicht ausgeschlossen werden
- Gewährleistung der Vorgaben des EuGH alleine durch Klauseln der EU Kommission daher nicht immer gegeben

→ Ergänzende Maßnahmen erforderlich

→ EDSA nennt zwei Möglichkeiten

1) Pseudonymisierung, wobei Datenimporteur keine Möglichkeit zur De-Pseudonymisierung haben darf
2) Verschlüsselung in einer Art und Weise, dass Datenimporteur keine Möglichkeit zum Zugriff auf die Daten haben darf

Ergänzende Schutzmaßnahmen

Pseudonymisierung und Verschlüsselung

Ergänzende Schutzmaßnahmen

Anonymisierung

Zur Erinnerung: Art. 2 Ziff. 7 DS-GVO Richtlinie (EU) 2019/1024*

– „Anonymisierung“ ist der Prozess,
  - in dessen Verlauf Dokumente in anonyme Dokumente umgewandelt werden,
  - die sich **nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen**,

  oder

  - personenbezogene Daten so anonym gemacht werden, dass
  - die **betroffene Person nicht oder nicht mehr identifiziert werden kann**;

* Richtlinie (EU) 2019/1024 des Europäischen Parlaments und des Rates vom 20. Juni 2019 über offene Daten und die Weiterverwendung von Informationen des öffentlichen Sektors . Online, unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32019L1024

Ergänzende Schutzmaßnahmen

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Pseudonymisierung

Zur Erinnerung: Art. 4 Ziff. 5 DS-GVO

- "Pseudonymisierung" die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten
  - ohne Hinzuziehung zusätzlicher Informationen
  - nicht mehr einer spezifischen betroffenen Person zugeordnet werden können,
- sofern diese zusätzlichen Informationen
  - gesondert aufbewahrt werden und
  - technischen und organisatorischen Maßnahmen unterliegen,
- die gewährleisten, dass
  - die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden

Ergänzende Schutzmaßnahmen

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Pseudonymisierung

- Pseudonymisierung liegt also nur vor, wenn
  - weder Verantwortlicher noch Auftragsverarbeiter
  - die personenbezogenen Daten
  - einer identifizierten oder identifizierbaren natürlichen Person zuordnen können
- Die Identifizierung einer Einzelperson ohne Kenntnis des Namens reicht also aus, damit personenbezogene Daten vorliegen
- Pseudonymisierung im Rahmen medizinischer Daten vermutlich eher in seltenen Einzelfällen sinnvoll einsetzbar

Ergänzende Schutzmaßnahmen

Verschlüsselung

- Verschlüsselung von Daten: Was wird wann verschlüsselt?
  - Verschlüsselung von „Data at Transit“, d.h. Transportverschlüsselung während einer Übertragung
  - Verschlüsselung von „Data at Rest“, d.h. Verschlüsselung im gespeicherten Zustand
  - Verschlüsselung von „Data in Use “, d.h. Verschlüsselung während der Nutzung

Sonderfälle im deutschen Recht

Vorgaben der Sozialgesetzbücher

Sozialdaten und Verarbeitung im Auftrag

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

§ 80 SGB X: Verarbeitung von Sozialdaten im Auftrag

- § 80(2): Der Auftrag zur Verarbeitung von Sozialdaten darf nur erteilt werden, wenn die Verarbeitung
  - im Inland,
  - in einem anderen Mitgliedstaat der Europäischen Union,
  - in einem diesem nach § 35 Abs. 7 SGB I gleichgestellten Staat,
  - oder, **sofern ein Angemessenheitsbeschluss gemäß DS-GVO** vorliegt, in einem Drittstaat oder in einer internationalen Organisation erfolgt.

→ Sozialdatenverarbeitung im Auftrag in einem Drittland:
Nur Art. 45 DS-GVO anwendbar

Sozialdaten und Verarbeitung im Auftrag

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Was sind eigentlich Sozialdaten?

- § 67 Abs. 2 SGB X
  - „Sozialdaten sind personenbezogene Daten (Art. 4 Nr. 1 DS-GVO), die von einer in § 35 des Ersten Buches genannten Stelle im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden.
  - Betriebs- und Geschäftsgeheimnisse sind alle betriebs- oder geschäftsbezogenen Daten, auch von juristischen Personen, die Geheimnischarakter haben.“
- § 67 Abs. 2 SGB X definiert Sozialdaten nur i.S.v. Art. 4(1) DS-GVO
  - In der Literatur finden sich Meinungen, dass demnach pseudonyme Daten keine Sozialdaten sind, da diese in Art. 4(5) DS-GVO definiert werden (BeckOK SozR/Gutzler, 51. Ed. 1.12.2018, SGB I § 35 Rn. 18)
  - In den Kommentaren zur DS-GVO werden pseudonyme Daten jedoch Art. 4(1) DS-GVO zugeordnet

Sozialdaten und Verarbeitung im Auftrag

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Was sind eigentlich Sozialdaten?

- „im Hinblick auf ihre Aufgaben nach diesem Gesetzbuch verarbeitet werden“
- Nicht als Sozialdaten sind dementsprechend z.B. folgende Datenkategorien anzusehen*
  - im Rahmen eines Dienst- oder Arbeitsverhältnisses anfallende Daten,
  - im Rahmen eines Werkvertrags mit einem Arzt anfallende Daten,
  - im Rahmen eines Werkvertrags mit einem Dolmetscher anfallende Daten,
  - Daten, die einem Sachbearbeiter nur privat bekannt werden oder auch
  - Dritten (z.B. Arztpraxis, Krankenhaus) bekannt gewordene Daten.

* BeckOK SozR/Gutzler, 51. Ed. 1.12.2018, SGB I § 35 Rn. 13

Sozialdaten und Verarbeitung im Auftrag

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Sozialgeheimnisträger in § 35 SGB I abschließend genannt

- Normadressat ist der Sozialleistungsträger oder einer sonst in § 35 Abs. 1 S. 4 bzw. Abs. 6 abschließend genannten Institution oder Einrichtung
  - Sozialleistungsträger ergeben sich aus § 12 i.V.m. §§ 18–29 SGB I
  - → Leistungserbringer, insbesondere Krankenhäuser oder Arztpraxen sind somit grundsätzlich keine Sozialgeheimnisträger!
- Normadressat des Schutzauftrags ist nicht der einzelne Mitarbeiter
  - Eine gesetzliche Pflicht des einzelnen Mitarbeiters zur Geheimniswahrung kann sich aber z.B. aus §§ 203, 353b Abs. 2 StGB bzw. § 85 SGB X ergeben
- Entsprechend § 35 Abs. 4 SGB I **stehen Betriebs- und Geschäftsgeheimnisse Sozialdaten gleich**, d.h. die Schutzregelungen der SGB sind analog anzuwenden

Sonderfälle im deutschen Recht

Digitale Gesundheitsanwendungen-Verordnung - DiGAV

§ 4 DiGAV

- § 4(3): Die Verarbeitung von personenbezogenen Daten zu den Zwecken nach Abs. 2 darf im Rahmen einer digitalen Gesundheitsanwendung durch die digitale Gesundheitsanwendung selbst sowie bei einer Verarbeitung personenbezogener Daten im Auftrag nur
  - im Inland,
  - in einem Mitgliedstaat der Europäischen Union oder
  - in einem diesem nach § 35 Abs. 7 SGB I gleichgestellten Staat oder,
  - sofern ein **Angemessenheitsbeschluss gemäß DS-GVO** vorliegt, in einem Drittstaat erfolgen.

Sonderfälle im deutschen Recht

Digitale Pflegeanwendungen-Verordnung - DiPAV

§ 5 DiPAV

- § 5(4): Die Verarbeitung personenbezogener Daten zu den Zwecken nach Abs. 3 S. 1 darf im Rahmen der Versorgung mit einer digitalen Pflegeanwendung oder sie erforderlichenfalls ergänzenden Unterstützungsleistungen durch die digitale Pflegeanwendung selbst sowie bei einer Verarbeitung personenbezogener Daten im Auftrag nur
  - im Inland,
  - in einem Mitgliedstaat der Europäischen Union oder
  - in einem diesem nach § 35 Abs. 7 SGB I gleichgestellten Staat oder,
  - sofern ein **Angemessenheitsbeschluss gemäß Artikel 45 der DSGVO** vorliegt, in einem Drittstaat erfolgen.

Sonderfälle im deutschen Recht

Sonderfälle im deutschen Recht: Einschränkung aufgrund Art.9 Abs. 4 DS-GVO

- Sozialdaten nach § 67 SGB X (und entsprechende Betriebs- und Geschäftsgeheimnisse nach § 67 SGB X),
- Daten, die im Rahmen einer DiGA nach § 33a SGB V verarbeitet werden

sowie

- Daten, die im Rahmen einer DiPA nach § 40a SGB XI verarbeitet werden

→ **dürfen nur in Drittländern verarbeitet werden, für die ein Angemessenheitsbeschluss der EU-Kommission vorliegt!**

Datenschutzrecht in den USA: Eine (grobe) Übersicht

Ausgewählte Aspekte im amerikanischen Datenschutzrecht

Unterschiede zwischen deutschen und amerikanischem Datenschutzrecht

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Einige wesentliche Unterschiede

- USA: Erstes Datenschutzgesetz 1974
  aktuell gültige Fassung 5 U.S.C. § 552a*
- Europa: Datenschutz ist Grundrecht
  USA: Datenschutz ist Verbraucherschutzrecht
- Europa: DS-GVO, dazu Landesrecht der Mitgliedsstaaten
  USA: Bundesländer können eigenes Recht erlassen, einige taten dies, z.B.
  - California Consumer Privacy Act
  - Colorado Privacy Act
  - Oklahoma Privacy Act
  - Virginia Consumer Data Protection Act
  - Washington Privacy Act

*Verfügbar unter https://www.govinfo.gov/content/pkg/USCODE-2018-title5/pdf/USCODE-2018-title5-partI-chap5-subchapII-sec552a.pdf
Überblick über das Privacy Act von 1974 in der Ausgabe von 2020 unter https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition

Unterschiede zwischen deutschen und amerikanischem Datenschutzrecht

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Einige wesentliche Unterschiede: Geschützte natürliche Person

Europa	USA
• Charta der Grundrechte • Art. 7 Jede Person hat das **Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation**.	• Vierter Verfassungszusatz Das **Recht der Menschen**, in ihren Personen, Häusern, Papieren und Effekten **vor unangemessenen Durchsuchungen und Beschlagnahmungen sicher zu sein**, **darf nicht verletzt werden**, und es dürfen keine Durchsuchungsbefehle ausgestellt werden, es sei denn, es liegt ein wahrscheinlicher Grund vor, der durch einen Eid oder eine eidesstattliche Erklärung gestützt wird und in dem der zu durchsuchende Ort und die zu beschlagnahmenden Personen oder Dinge genau beschrieben sind

Unterschiede zwischen deutschen und amerikanischem Datenschutzrecht

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Einige wesentliche Unterschiede: Geschützte natürliche Person

Europa	USA
• Charta der Grundrechte • **Person = irgendein Mensch**, egal, wo er lebt oder woher er kommt	• Art. 3 Abschnitt 2 der Verfassung Die richterliche Gewalt erstreckt sich [...] für Streitigkeiten zwischen zwei oder mehreren Staaten; zwischen einem Staat und Bürgern eines anderen Staates; zwischen Bürgern verschiedener Staaten; -zwischen Bürgern desselben Staates, [...] • Art. 4 Abschnitt 2 der Verfassung Die Bürger eines jeden Staates haben Anspruch auf alle Vorrechte und Immunitäten der Bürger in den einzelnen Staaten. • **Person = Bürger der USA**

Unterschiede zwischen deutschen und amerikanischem Datenschutzrecht

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Einige wesentliche Unterschiede: Geschützte natürliche Person

- Europa:
  'Betroffene Person‘ bezeichnet eine identifizierte oder identifizierbare natürliche Person, egal wo sie lebt
- USA: Definition in B. 5 U.S.C. § 552a(a)(2)
  Der Begriff 'Einzelperson' bezeichnet einen **Bürger der Vereinigten Staaten** oder einen **Ausländer, der rechtmäßig zum dauerhaften Aufenthalt in den USA zugelassen ist**.

Unterschiede zwischen deutschen und amerikanischem Datenschutzrecht

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Unterschied im Recht: USA Datenschutz = Verbraucherrecht

- Aufsichtsbehörde Federal Trade Commission (FTC)
- „Wenn Ihr Unternehmen Versprechungen zum Datenschutz macht - entweder ausdrücklich oder stillschweigend -, sind Sie nach dem FTC Act* verpflichtet, diese Versprechungen einzuhalten."
  (https://www.ftc.gov/business-guidance/privacy-security)
- FTC hat Kommission zu Datenschutzverletzungen durch Gesundheits-Apps und andere vernetzte Geräte
  (https://www.ftc.gov/legal-library/browse/statement-commission-breaches-health-apps-other-connected-devices)
- FTC nimmt Beschwerden** von Konsumenten oder Unternehmen gegen einzelne Unternehmen
  - Grundsätzlich auch von Menschen, die nicht amerikanische Bürger sind, wenn die Unternehmen entsprechende Zusagen trafen
- Beispiel: FTC Imposes $5 Billion (~4,5 Mrd. €) Penalty and Sweeping New Privacy Restrictions on Facebook
  (https://www.ftc.gov/news-events/news/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions-facebook)

* 15 USC Chapter 2, Subchapter I: Federal Trade Commission. Online, unter https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-chapter2-subchapter1&edition=prelim

** How to File a Complaint with the Federal Trade Commission. Online, unter https://consumer.ftc.gov/media/video-0054-how-file-complaint-federal-trade-commission

Unterschiede zwischen deutschen und amerikanischem Datenschutzrecht

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Health Insurance Portability and Accountability Act (HIPAA)*

- HIPAA Privacy Rule** ist in 45 CFR Teil 160 und den Unterabschnitten A und E von Teil 164 zu finden
- § 160.103 Definitions
  - Gesundheitsinformationen sind alle Informationen, einschließlich genetischer Informationen, unabhängig davon, ob sie mündlich oder in irgendeiner Form oder auf einem Medium aufgezeichnet wurden, die:
    (1) von einem Gesundheitsdienstleister, einem Gesundheitsplan, einer Gesundheitsbehörde, einem Arbeitgeber, einem Lebensversicherer, einer Schule oder Universität oder einer Clearingstelle für das Gesundheitswesen erstellt oder empfangen werden;
  - Gesundheitsdienstleister usw. verweisen auf andere Regelungen (z.B. 42 U.S.C. 1395x(u)), die i-D.R. nur auf amerikanische Anbieter zutreffen

* Online, unter https://www.govinfo.gov/app/details/CRPT-104hrpt736/CRPT-104hrpt736/context

** Übersicht zur Privacy Rule inkl. konsolidierter Version z.B. unter https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

Unterschiede zwischen deutschen und amerikanischem Datenschutzrecht

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Analoge Regelung zu § 203 StGB in HIPAA?*

Abschnitt 1177 HIPAA (inoffizielle Übersetzung)

a) Straftat: Eine Person, die wissentlich und unter Verstoß gegen diesen Teil
   (1) einen eindeutigen Gesundheitsidentifikator verwendet oder verwenden lässt;
   (2) individuell identifizierbare Gesundheitsinformationen in Bezug auf eine Person erlangt; oder
   (3) individuell identifizierbare Gesundheitsinformationen an eine andere Person weitergibt,

   wird wie in Unterabschnitt (b) vorgesehen bestraft.

b) Sanktionen: Eine in Unterabschnitt (a) beschriebene Person muss...
   (1) mit einer Geldstrafe von nicht mehr als $50.000, einer Freiheitsstrafe von nicht mehr als 1 Jahr oder beidem bestraft werden;
   (2) wenn die Straftat unter Vorspiegelung falscher Tatsachen begangen wird, mit einer Geldstrafe von nicht mehr als $100.000, einer Freiheitsstrafe von nicht mehr als 5 Jahren oder beidem belegt werden; und
   (3) wenn die Straftat mit der Absicht begangen wird, individuell identifizierbare Gesundheitsinformationen zum kommerziellen Vorteil, persönlichen Gewinn oder böswilligen Schaden zu verkaufen, zu übertragen oder zu verwenden, mit einer Geldstrafe von nicht mehr als $250.000, einer Freiheitsstrafe von nicht mehr als 10 Jahren oder beidem.

* HIPAA wurde durch verschiedene Rechtakte geändert. Eine übersichtliche Darstellung des Themas „HIPAA and Penalty“ findet man bspw. unter https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/, https://www.strongdm.com/blog/hipaa-violation-penalties oder https://www.hipaajournal.com/civil-penalty-for-knowingly-violating-hipaa/

Unterschiede zwischen deutschen und amerikanischem Datenschutzrecht

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Analoge Regelung zu § 203 StGB in HIPAA?*

Abschnitt 1177 HIPAA (inoffizielle Übersetzung)

a) Straftat: Eine Person, die wissentlich und
   (1) einen eindeutigen Gesundheitsidentifikat
   (2) individuell identifizierbare Gesundheitsin
   (3) individuell identifizierbare Gesundheitsin
   wird wie in Unterabschnitt (b) vorgesehen be

b) Sanktionen: Eine in Unterabschnitt (a) bes
   (1) mit einer Geldstrafe von nicht mehr als $50.000, einer Freiheitsstrafe von nicht mehr als 1 Jahr oder beidem bestraft werden;
   (2) wenn die Straftat unter Vorspiegelung falscher Tatsachen begangen wird, mit einer Geldstrafe von nicht mehr als $100.000, einer Freiheitsstrafe von nicht mehr als 5 Jahren oder beidem belegt werden; und
   (3) wenn die Straftat mit der Absicht begangen wird, individuell identifizierbare Gesundheitsinformationen zum kommerziellen Vorteil, persönlichen Gewinn oder böswilligen Schaden zu verkaufen, zu übertragen oder zu verwenden, mit einer Geldstrafe von nicht mehr als $250.000, einer Freiheitsstrafe von nicht mehr als 10 Jahren oder beidem.

Erinnerung § 203 StGB und Strafregelung:
„wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft."
Gegen Entgelt usw.: 2 Jahre oder Geldstrafe

* HIPAA wurde durch verschiedene Rechtakte geändert. Eine übersichtliche Darstellung des Themas „HIPAA and Penalty" findet man bspw. unter https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/, https://www.strongdm.com/blog/hipaa-violation-penalties oder https://www.hipaajournal.com/civil-penalty-for-knowingly-violating-hipaa/

Zugriffsmöglichkeiten auf Daten für US-Behörden

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Clarifying Lawful Overseas Use of Data Act (Cloud Act)*

- Ergänzung des Stored Communications Act („S.C.A.") von 1986
- Erleichtert den grenzüberschreitenden Zugriff US-amerikanischer Ermittlungsbehörden auf elektronische Daten
- U.a. Offenlegungspflicht für US-Anbieter bezüglich außerhalb der USA gespeicherter Daten:
  - Staatliche Stellen können unter bestimmten Voraussetzungen die Herausgabe gespeicherter Inhalte (contents), Aufzeichnungen zur Kommunikation (records) inkl. Metadaten zum Kommunikationsverhalten verlangen.
  - Informationspflicht für betroffene Personen, wenn Herausgabe von content auf einer Vorladung (subponea) oder einem Gerichtsbeschluss (court order) beruht
  - Keine Informationspflicht, wenn content-Herausgabe auf einem Durchsuchungsbeschluss (warrant) beruht
  - Grundsätzlich keine Informationspflicht bei Herausgabe von records

* H.R.4943 - CLOUD Act, online unter https://www.congress.gov/bill/115th-congress/house-bill/4943

Zugriffsmöglichkeiten auf Daten für US-Behörden

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Clarifying Lawful Overseas Use of Data Act (Cloud Act)

- Anbieter kann Widerspruchsrecht gegen die Anordnung einlegen, wenn
  - der Eigentümer der Daten kein US-Bürger ist,
  - nicht in den USA lebt und
  - das Unternehmen durch die Herausgabe der Daten gegen geltendes Recht in anderen Ländern verstößt.
- Widerspruchrecht besteht jedoch nur, wenn das jeweilige Land mit den USA ein Abkommen unter dem CLOUD Act (“Executive Agreement“) abgeschlossen hat
  - Executive Agreement sieht nur Anforderungen an die Rechtsstaatlichkeit und das Rechtssystem der anderen Vertragspartei vor, nicht für die USA
  - D.h. USA hat keinerlei Verpflichtungen, nur Vertragspartner muss auf Anforderung Unterlagen an die USA herausgeben
  - Europa: Ausschließlich UK hat entsprechendes Abkommen abgeschlossen

Zugriffsmöglichkeiten auf Daten für US-Behörden

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Foreign Intelligence Surveillance Acts (FISA)*

- Section 702 des FISA gilt für „Electronic Communication Service Provider“ im Sinne von 50 U.S. Code § 1881 (siehe Absatz 4)

  Electronic communication service provider

  The term “electronic communication service provider” means—

  a) a telecommunications carrier, as that term is defined in section 153 of title 47;
  b) a provider of electronic communication service, as that term is defined in section 2510 of title 18;
  c) a provider of a remote computing service, as that term is defined in section 2711 of title 18;
  d) any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or
  e) an officer, employee, or agent of an entity described in subparagraph (A), (B), (C), or (D).

* Foreign Intelligence Surveillance Acts (FISA), online unter https://www.govtrack.us/congress/bills/110/hr6304/text

Zugriffsmöglichkeiten auf Daten für US-Behörden

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

FISA und electronic communication service provider

- Bei ECS ist zu beachten, dass dies ein sehr weitreichender Begriff ist
  - 18 U.S.C. § 2510(15)*:
    Ein „elektronischer Kommunikationsdienst“ ist jeder Dienst, der seinen Nutzern die Möglichkeit bietet, drahtgebundene oder elektronische Nachrichten zu senden oder zu empfangen
  - Der Dienst **muss nicht** der Öffentlichkeit oder Dritten zur Verfügung gestellt werden
  - Ein Unternehmen wie beispielsweise ein Krankenhaus fällt unter die Regelung, wenn es seinen Mitarbeitern einen E-Mail-Dienst zur Verfügung stellt

    Siehe z.B.
    - U.S. v. Mullins (1993) https://casetext.com/case/us-v-mullins-5/
    - Fraser v. Nationwide Mut. Ins. Co. (2004) https://casetext.com/case/fraser-v-nationwide-mut-ins-co
    - Shefts v. Petrakis (2011) https://casetext.com/case/shefts-v-petrakis-2

* 18 U.S.C. § 2510(15): Online unter https://uscode.house.gov/view.xhtml?req=(title:18%20section:2510

Zugriffsmöglichkeiten auf Daten für US-Behörden

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Foreign Intelligence Surveillance Acts (FISA)

- Keine proaktive Pflicht des Anbieters, Daten einer Behörde zu übergeben
- Aber auf Anweisung einer Behörde:
  - Pflicht, Daten an einen US-Dienst weiterzugeben oder diesem Zugang zu den Daten zu gewähren
  - Dies betrifft alle Daten, auf die ein Anbieter Zugriff hat, auch Daten von Kunden
- Abschnitt 702 FISA sowohl für Daten in Übertragung wie auch ruhende Daten anwendbar
- Amerikanische Konzerne: 702 FISA auch auf Daten anwendbar, die auf europäischen Servern gespeichert sind
- FISA-Gericht gestattete schon Zugriff von Metadaten und auch Kommunikationsinhalten
- ABER: Anweisung kann von einem Anbieter elektronischer Kommunikationsdienste vor dem FISA-Gericht angefochten werden

Schutz Gesundheitsdaten

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Gesundheitsdaten auch in USA besonders geschützt

- Health Insurance Portability and Accountability Act of (HIPAA)
  - 1996 eingeführt, 2003 durch Privacy Rule umgesetzt
- Health Information Technology for Economic and Clinical Health Act (HITECH)
  - Praktische Durchsetzung von HIPAA gering
  - 2009 HITECH eingeführt, wodurch u.a. Geldstrafen bei Verstößen erhöht wurden
  - Zugleich Vertragspartner der Leistungserbringer direkt verpflichtet, d.h. neben Ärzten & Co werden auch Unternehmen in die Pflicht genommen
  - Gleichzeitig leichtere Nutzung von Daten zu Forschungszwecken ermöglicht

Schutz Gesundheitsdaten

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Gesundheitsdaten auch in USA besonders geschützt

- Genetic Information Nondiscrimination Act (GINA)
  - GINA ergänzt Privacy Rule bzgl. Umgang mit genetischen Daten
  - Schutzbereich nur für krankheitsrelevante Gesundheitsinformationen, Alter oder Geschlecht bspw. nicht geschützt
  - Forschung bzgl. Nutzung genetischer Informationen privilegiert

Schutz Gesundheitsdaten

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Gesundheitsdaten auch in USA besonders geschützt

- Landesrecht
  - Die meisten US Bundesstaaten erließen ergänzende Regelungen
  - Schutzniveau variiert daher erheblich von Bundesstaat zu Bundesstaat
- Kritik
  - Keine einheitliche Interpretation
  - Schutzvorschriften gelten allerdings nach wie vor nicht für alle Formen der Gesundheitsversorgung und -forschung
  - Es existieren Widersprüche zu anderen gesetzlichen Regelungen
  - Aktuelle Regelungen wie der Coronavirus Aid, Relief, and Economic Security Act (CARES Act) schwächen die Schutzwirkung von HIPAA

Schutz Gesundheitsdaten

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Gesundheitsdaten auch in USA besonders geschützt

- Fazit:
  - Andere Zielrichtung der Gesetzgebung
  - Um ein der DS-GVO angemessenes Schutzniveau zu erzielen, müssen ergänzende vertragliche Vereinbarungen getroffen werden
  - Weiterhin: Definitionen beachten
    - Wer wird geschützt?
    - Was wird vor wem geschützt?
    - …

    Nicht-Amerikaner ohne dauerhafte Aufenthaltsgenehmigung in vielen Fällen vom Schutz ausgenommen

E.O. 14086 von Präsident Biden zum Schutz europäischer Daten

Ausgewählte Aspekte, dargestellt mit inoffizieller Übersetzung

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

E.O. 14086 Präsident Biden vom 7. Oktober 2022*

Vorbemerkung

- Executive Order („Durchführungsverordnung“) ist ein Dekret des US-Präsidenten, hat jedoch keinen Gesetzescharakter
  - Amerikanische Verfassung und Bundesgesetze enthalten keine Bestimmungen zu E.O.
  - E.O. auch ohne Parlament für den Bereich gültig, wo der Präsident Verfügungsgewalt hat
  - US-Präsident oberste Instanz der amerikanischen Exekutivorgane, daher E.O. für entsprechende Organe gültig
  - E.O. können vor US-Gerichten angefochten und von Gerichten außer Kraft gesetzt werden
  - ABER: E.O. können keine Gesetze außer Kraft setzen
- Im Folgenden: Ausgewählte Punkte der E.O. vom 2022-10-07

*Online verfügbar unter https://www.federalregister.gov/executive-order/14086

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

E.O. 14086 Präsident Biden vom 7. Oktober 2022

Sec. 1 Purpose

- Sicherheitsorgane der USA müssen Informationen zusammentragen
- Auch digitale Informationen
- Insbesondere auch aus Ländern außerhalb der USA
- USA erkennen an, dass
  - alle Personen mit Würde und Respekt behandelt werden sollten, ungeachtet ihrer Nationalität oder ihres Wohnsitzes
  - alle Personen ein legitimes Interesse an der Wahrung der Privatsphäre im Umgang mit ihren persönlichen Daten haben
- E.O. soll Rahmenbedingungen festlegen, dass allen Interessen Rechnung bei der Informationsbeschaffung durch amerikanische Behörden getragen wird

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

E.O. 14086 Präsident Biden vom 7. Oktober 2022

Sec. 2(a) Principles

- Nachrichtendienstliche Tätigkeiten müssen legal erfolgen, also durch Gesetz, Erlass o.ä. legitimiert werden
- Schutz der Privatsphäre und der bürgerlichen Freiheiten bei der Planung und Durchführung solcher Tätigkeiten soll umfassend berücksichtigt werden
- Nachrichtensignaltätigkeiten werden nur durchgeführt, nachdem auf der Grundlage einer angemessenen Bewertung aller relevanten Faktoren festgestellt wurde, dass die Tätigkeiten erforderlich sind, um Aspekte der nachrichtendienstlichen Priorität voranzubringen

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

E.O. 14086 Präsident Biden vom 7. Oktober 2022

Sec. 2(b, i) Legitimate objectives
(insgesamt 12 Ziele), hier nur exemplarische Darstellung

- Die Fähigkeiten, Absichten oder Aktivitäten einer ausländischen Regierung, Militär, Einrichtung, Organisation usw. zu verstehen oder zu bewerten, um die nationale Sicherheit der Vereinigten Staaten und ihrer Verbündeten und Partner zu schützen
- Schutz vor Cybersicherheitsbedrohungen, die von einer ausländischen Regierung usw. geschaffen oder ausgenutzt werden,
- Schutz vor Bedrohungen für das Personal der Vereinigten Staaten oder ihrer Verbündeten oder Partner

→ Präsident kann Aktualisierungen der Liste der Ziele genehmigen, wenn neue nationale Sicherheitserfordernisse dies erfordern

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

E.O. 14086 Präsident Biden vom 7. Oktober 2022

Sec. 2(b, ii) Prohibited objectives

- Keine nachrichtendienstlichen Aktivitäten zu Zwecken der
  - Unterdrückung von Kritik, abweichenden Meinungen oder der freien Äußerung von Ideen oder politischen Meinungen durch Einzelpersonen oder die Presse;
  - Unterdrückung oder Einschränkung der legitimen Interessen der Privatsphäre;
  - Unterdrückung oder Einschränkung des Rechts auf Rechtsbeistand; oder
  - Benachteiligung von Personen aufgrund ihrer ethnischen Zugehörigkeit, ihrer Rasse, ihres Geschlechts, ihrer Geschlechtsidentität, ihrer sexuellen Orientierung oder ihrer Religion
- Es ist kein legitimes Ziel, ausländische private Geschäftsinformationen oder Geschäftsgeheimnisse zu sammeln, um US-amerikanischen Unternehmen und Wirtschaftszweigen in den USA einen Wettbewerbsvorteil zu verschaffen

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

E.O. 14086 Präsident Biden vom 7. Oktober 2022

Sec. 2(c) Privacy and civil liberties safeguards

- Die **Vereinigten Staaten führen nachrichtendienstliche Erhebungen** nur dann durch, wenn sie auf der **Grundlage einer angemessenen Bewertung aller relevanten Faktoren** zu dem Schluss gekommen sind, dass **eine bestimmte Erhebungsmaßnahme notwendig ist**
- Nachrichtendienstliche Erhebungsmaßnahmen sind **so weit wie möglich** auf die Förderung von genehmigten nachrichtendienstlichen Schwerpunkten zuzuschneiden und dürfen **unter gebührender Berücksichtigung relevanter Faktoren die Privatsphäre und die bürgerlichen Freiheiten nicht unverhältnismäßig beeinträchtigen**

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

E.O. 14086 Präsident Biden vom 7. Oktober 2022

Sec. 2(c) Privacy and civil liberties safeguards (Bulk collection)

- Nachrichtendienstliche Massenerhebung wird nur genehmigt, wenn dies **für die Bearbeitung** nachrichtendienstlichen Schwerpunkts **erforderlich ist und** die **Informationen vernünftigerweise** nicht **durch gezielte Erhebung gewonnen werden können**
- Massenerhebung nur für Zwecke
  - Schutz vor Terrorismus, Geiselnahme und Gefangenschaft von Personen durch ausländische Kräfte
  - Schutz vor Spionage, Sabotage, Attentaten oder anderen nachrichtendienstlichen Aktivitäten durch ausländische Organisationen oder Personen
  - Schutz vor Cybersicherheitsbedrohungen durch ausländische Organisationen oder Personen
  - Schutz vor Bedrohungen für das Personal der Vereinigten Staaten oder ihrer Verbündeten oder Partner
  - Schutz vor grenzüberschreitenden kriminellen Bedrohungen, einschließlich der illegalen Finanzierung und der Umgehung von Sanktionen

→ Der Präsident kann die Liste aktualisieren

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

E.O. 14086 Präsident Biden vom 7. Oktober 2022

Sec. 5 General Provisions

- Keine Bestimmung dieser Anordnung **darf so ausgelegt werden**, **dass sie** die **Befugnisse**, **die** einer Exekutivabteilung, einer Agentur oder deren Leiter **gesetzlich eingeräumt werden, beeinträchtigt oder anderweitig beeinflusst**
- Diese **Anordnung zielt nicht darauf ab**, die für US-Personen geltenden Vorschriften zu ändern, **die gemäß FISA, Executive Order 12333 oder anderen geltenden Gesetzen erlassen wurden**.
- Diese **Anordnung verleiht keine Befugnis zur Aufhebung des Geheimhaltungsgrades oder zur Offenlegung von als Verschlusssache** eingestuften nationalen Sicherheitsinformationen, es sei denn, dies ist aufgrund anderer Bestimmungen zulässig.

Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

E.O. 14086 Präsident Biden vom 7. Oktober 2022

Sec. 5 General Provisions

- Diese Anordnung begründet einen Anspruch darauf,
  - qualifizierte Beschwerden beim Office of the Director of National Intelligence (CLPO) einzureichen und
  - eine Überprüfung der Entscheidungen des CLPO durch das Datenschutz-Überprüfungsgericht zu erwirken.
- Diese **Anordnung soll und wird keine anderen Ansprüche, Rechte oder Vergünstigungen materieller oder verfahrensrechtlicher Art schaffen**, die **von einer Partei gegen die Vereinigten Staaten, ihre Ministerien, Behörden oder Einrichtungen, ihre Beamten, Angestellten oder Vertreter oder eine andere Person rechtlich oder nach Billigkeit durchgesetzt werden können**.

E.0. 14086 und Anforderungen des EuGH

Was sagen verschiedene Akteure dazu?

Schafft die E.O. 14086 ein dem EU-Recht gleichwertiges Schutzniveaus?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Erste Überlegungen

- E.O. 14086 muss für Angemessenheitsbeschluss natürlich am EU Recht gemessen werden
- Aber insbesondere auch an den Anforderungen der Schrems II Entscheidung des EuGH
  - Rn. 173: Art. 8 Abs. 2 GRCh: Daten dürfen nur „für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage“ verarbeitet werden
  - Rn 177: Art. 45 Abs. 2 Buchst. a der DSGVO verlangt, dass „wirksame und durchsetzbare Rechte der betroffenen Person“ existieren
  - Leitsatz 3: Art. 46 Abs. 1 und Art. 46 Abs. 2 Buchst. c DS-GVO sind dahin auszulegen, dass die nach diesen Vorschriften erforderlichen geeigneten Garantien, durchsetzbaren Rechte und wirksamen Rechtsbehelfe gewährleisten müssen […], das dem in der Europäischen Union durch diese Verordnung im Licht der Charta der Grundrechte der Europäischen Union garantierten Niveau der Sache nach gleichwertig ist.

Schafft die E.O. 14086 ein dem EU-Recht gleichwertiges Schutzniveaus?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Erste Überlegungen

- Wird sicherlich unterschiedlich beurteilt
- Die EU-Kommission erkannte ein gleichwertiges Schutzniveau schon für Safe Harbour und Privacy Shield an
- Vermutlich wird sie aus politischen Gründen auch hier einen Angemessenheitsbeschluss aussprechen

Schafft die E.O. 14086 ein dem EU-Recht gleichwertiges Schutzniveaus?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Unterschiedliche Bewertungen, z.B.:

- Der heutige IAPP Vice President (früher Privacy Shield Director beim U.S. Department of Commerce) z.B. sieht die Vorgaben des EuGH erfüll (https://iapp.org/news/a/the-eu-u-s-data-privacy-framework-a-new-era-for-data-transfers/)
- Max Schrems / NOYB
  - Executive Order zur US-Überwachung reicht wohl nicht https://noyb.eu/de/executive-order-zur-us-ueberwachung-reicht-wohl-nicht
  - Statement zur Angemessenheitsentscheidung der Europäischen Kommission https://noyb.eu/de/statement-zur-angemessenheitsentscheidung-der-eu-kommission-zur-usa
- Daher ist mit einer Klage vor dem EuGH zu rechnen

→ Der EuGH wird dann (vermutlich) wieder einmal der EU-Kommission bescheinigen, die europäische Gesetzgebung ignoriert zu haben und den Beschluss aufheben

Schafft die E.O. 14086 ein dem EU-Recht gleichwertiges Schutzniveaus?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Klage vor dem EuGH …?

- EuGH im Schrems II Urteil
  - Rn. 120: Die **zuständige nationale Aufsichtsbehörde**, an die sich eine Person mit einer Beschwerde wendet, **muss in völliger Unabhängigkeit prüfen**, **ob** bei der Übermittlung dieser Daten **die in der DS-GVO aufgestellten Anforderungen gewahrt werden**
  - Rn. 120: Die **zuständige nationale Aufsichtsbehörde muss gegebenenfalls Klage vor den nationalen Gerichten erheben**, **damit diese**, wenn das Gericht die Zweifel der Aufsichtsbehörde an der Gültigkeit des Angemessenheitsbeschlusses teilt, **um eine Vorabentscheidung über dessen Gültigkeit ersucht**

Schafft die E.O. 14086 ein dem EU-Recht gleichwertiges Schutzniveaus?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Klage vor dem EuGH …?

- § 21 BDSG: Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Rechtswidrigkeit eines Beschlusses der Europäischen Kommission
  - Abs. 3: Über einen Antrag der Aufsichtsbehörde nach Absatz 1 entscheidet im ersten und letzten Rechtszug das Bundesverwaltungsgericht.
  - Abs. 6 S. 3: Teilt das BVerwG die Auffassung der Aufsichtsbehörde, legt es die Frage dem EuGH vor
- Es muss nicht immer Herr Schrems klagen, auch die Aufsichtsbehörden könnten sich mal damit beschäftigen
  - Von deutschen Aufsichtsbehörden vermutlich nicht zu erwarten
  - Aber es existieren vergleichbare Regelungen in anderen Ländern, die weniger auf wirtschaftliche Interessen achten, als deutsche Aufsichtsbehörden

Schafft die E.O. 14086 ein dem EU-Recht gleichwertiges Schutzniveaus?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Falls es einen Angemessenheitsbeschluss der EU Kommission gibt…

- EuGH im Schrems II Urteil
  - Rn. 117: Ein Angemessenheitsbeschluss der Kommission bindet alle Mitgliedstaaten und ist für alle Organe verbindlich, soweit darin festgestellt wird, dass das betreffende Drittland ein angemessenes Schutzniveau gewährleistet, und die Übermittlung personenbezogener Daten im Ergebnis genehmigt wird
  - Rn. 118: Solange der Angemessenheitsbeschluss vom Gerichtshof nicht für ungültig erklärt wurde, können die Mitgliedstaaten und ihre Organe, zu denen ihre unabhängigen Aufsichtsbehörden gehören, keine diesem Beschluss zuwiderlaufenden Maßnahmen treffen
  - Rn. 119: Ein nach Art. 45 Abs. 3 der DSGVO ergangener Angemessenheitsbeschluss der Kommission kann Personen, deren personenbezogene Daten in ein Drittland übermittelt wurden oder werden könnten, nicht daran hindern, gemäß Art. 77 Abs. 1 DSGVO die zuständige nationale Aufsichtsbehörde mit einer Beschwerde bezüglich des Schutzes ihrer Rechte und Freiheiten bei der Verarbeitung solcher Daten zu befassen

Schafft die E.O. 14086 ein dem EU-Recht gleichwertiges Schutzniveaus?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Falls es einen Angemessenheitsbeschluss der EU Kommission gibt…

- … so gilt der Angemessenheitsbeschluss, bis ihn entweder die Kommission widerruft
- oder der EuGH den Angemessenheitsbeschluss für ungültig erklärt

→ Zu beachten: Mit Urteil des EuGH-Urteils und einem darin enthaltenen Widerruf des Angemessenheitsbeschlusses

(1) War der Angemessenheitsbeschluss nie gültig: In seinen Entscheidungen zu „Schrems I“ und „Schrems II“ wurde beide Male festgestellt, dass die EU-Kommission die Angemessenheit widerrechtlich erklärte und die Beschlüsse daher nie gültig waren

(2) In Deutschland gilt i.d.R., dass angewendetes Recht nicht nachteilig für Rechtsanwender ausgelegt werden darf

(3) Aber ab Urteil ist Angemessenheitsbeschluss keine Rechtsgrundlage für Datentransfer in die USA

(4) Es muss **sofort** ein Transfer eingestellt oder auf andere Rechtsgrundlage gestellt werden

Position LIBE-Ausschuss des EU-Parlaments

E.O. 14086 von Präsident Biden zum Schutz europäischer Daten

Angemessenheitsbeschluss der EU-Kommission

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

EU-Kommission veröffentliche Entwurf eines Angemessenheitsbeschlusses

- 13. Dezember 2022: Pressemitteilung „Data protection: Commission starts process to adopt adequacy decision for safe data flows with the US" https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631
- Adequacy decision for the EU-US Data Privacy Framework https://commission.europa.eu/document/e5a39b3c-6e7c-4c89-9dc7-016d719e3d12_en
  - 134 Seiten
  - Dabei vielfach Wiederholung von Inhalten der DS-GVO und des EuGH-Urteils "Schrems II"
  - Darstellung der Erfüllung der Vorgaben durch US-Recht dabei nur sehr oberflächlich
- EDSA und Mitgliedstaaten müssen angehört werden
- ABER: Negative Stellungnahmen von EDSA und Mitgliedstaaten sind für die Kommission jedoch nicht bindend

Angemessenheitsbeschluss der EU-Kommission

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

LIBE-Ausschuss empfiehlt Ablehnung US-EU Privacy-Abkommen

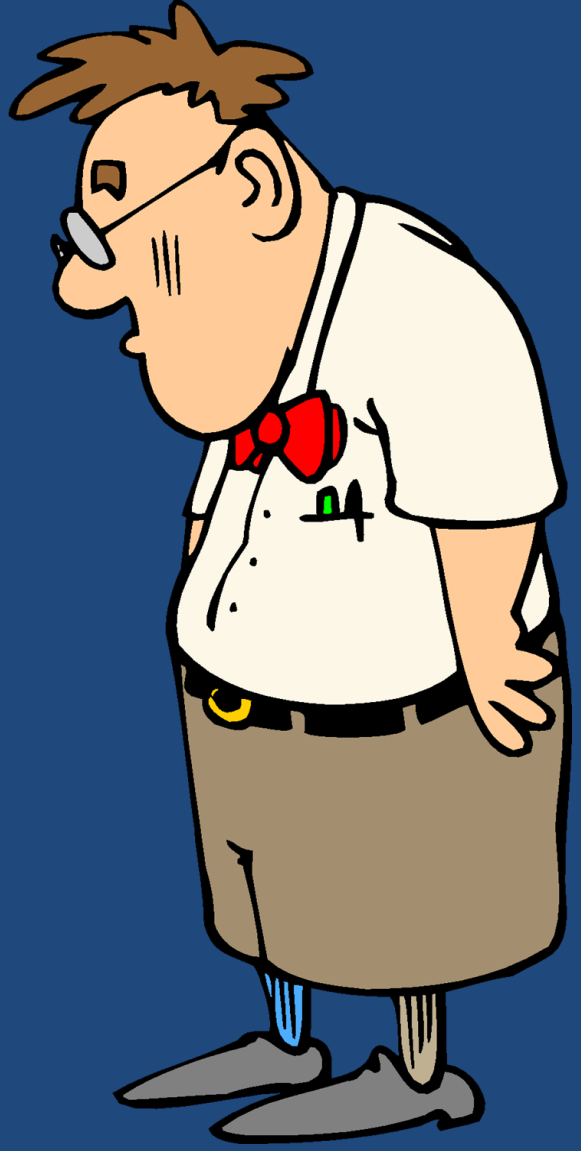
- 14. Februar 2023: Ausschuss für bürgerliche Freiheiten, Justiz und innere Angelegenheiten des EU-Parlaments (LIBE) empfiehlt, , den Entwurf für das Data Privacy Framework abzulehnen
  https://www.europarl.europa.eu/doceo/document/LIBE-RD-740749_EN.pdf

Angemessenheitsbeschluss der EU-Kommission

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

LIBE-Ausschuss empfiehlt Ablehnung US-EU Privacy-Abkommen

- Zusammenfassende Schlussfolgerung des LIBE-Ausschusses
  - Rn. 10: das EU-Parlament forderte die Kommission auf (Beschluss vom 20. Mai 2021), keine neue Angemessenheitsentscheidung in Bezug auf die USA zu erlassen, wenn nicht grundlegende Änderungen, insbesondere für die Zwecke der nationalen Sicherheit und der Nachrichtendienste, vorgenommen werden
  - Rn. 11: der EU-US-Datenschutzrahmen stellt keine tatsächliche Gleichwertigkeit des Schutzniveaus her
  - die EU-Kommission wird aufgefordert, die Verhandlungen mit ihren US-amerikanischen Partnern fortzusetzen, um einen entsprechenden Mechanismus zu schaffen, der eine solche Gleichwertigkeit gewährleistet und ein angemessenes Schutzniveau bietet, wie es das Datenschutzrecht der Union und die Charta in der Auslegung des EuGH vorsehen
  - die EU-Kommission wird aufgefordert, die Feststellung der Angemessenheit nicht zu treffen



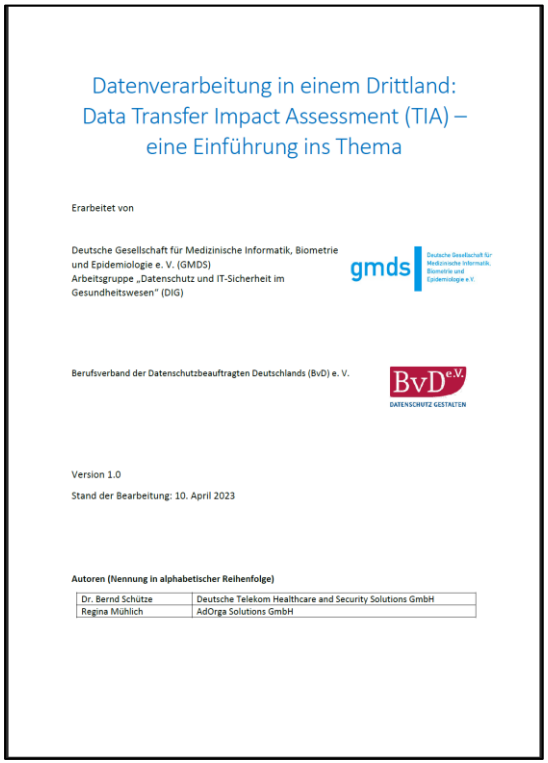
Transfer Impact Assessment

Ein praktisches Beispiel

TIA: „Werbeblock“

TIA-Ausarbeitung von GMDS und BvD

- Praxishilfe „Datenverarbeitung in einem Drittland: Data Transfer Impact Assessment (TIA) – eine Einführung ins Thema“
- Stand: 10. April 2023
- Anforderungen an TIA aus DS-GVO, Schrems II und Standardvertragsklauseln
- Vorgehen bei einer TIA
- Copyright: Creative Commons-Lizenz CC BY-SA 4.0, zur freien (auch kommerziellen) Nutzung
- URL: https://gesundheitsdatenschutz.org/html/tia.php



Datenverarbeitung in einem Drittland:
Data Transfer Impact Assessment (TIA) –
eine Einführung ins Thema

Erarbeitet von

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)
Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Version 1.0

Stand der Bearbeitung: 10. April 2023

Autoren (Nennung in alphabetischer Reihenfolge)

Dr. Bernd Schütze	Deutsche Telekom Healthcare and Security Solutions GmbH
Regina Mühlich	AdOrga Solutions GmbH

Also: Verschlüsselt = Und weiter?

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Suche in verschlüsselten Dateien

- 2012/2013 erste Versuche mit eterministischen endlichen Automaten (DFA)
- Stichwort: „Searchable symmetric encryption“ (SSE) oder „Searchable encryption schemes“
  - Effektive Möglichkeit, verschlüsselte Daten nach Schlüsselwörtern zu durchsuchen
- Patientenakten können so auf **zuvor definierte** Schlüsselwörter durchsucht werden*, während alle Daten verschlüsselt sind
  - Man sucht mittels Schlüsselwort (z.B. „Patient Schütze“) und
    - lädt dann nur die gefundenen verschlüsselten Dateien herunter,
    - entschlüsselt diese auf seinem Client,
    - führt die Verarbeitung durch,
    - verschlüsselt die Datei und lädt sie wieder hoch.
  - Cloud-Provider hat nie Zugriff auf unverschlüsselte Datei

* Siehe z.B. Niu et al. (2022) Specified keywords search scheme for EHR sharing. Soft comput. 26(18): 8949-8960. https://doi.org/10.1007/s00500-022-07292-5

Also: Verschlüsselt = Und weiter?

Suche in verschlüsselten Dateien

- 2012/2013 erste Versuche mit eterministischen endlichen Automaten (DFA)
-
-

Heute suchen Verantwortliche in verschlüsselten Dateien, morgen …?

Fortsetzung folgt… 😉

  - Cloud-Provider hat nie Zugriff auf unverschlüsselte Datei

*Siehe z.B. Niu et al. (2022) Specified keywords search scheme for EHR sharing. Soft comput. 26(18): 8949-8960. https://doi.org/10.1007/s00500-022-07292-5

Fragen / Diskussion

gmds Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V.

Kontakt:

Dr. Bernd Schütze

Leiter GMDS AG „Datenschutz und IT-Sicherheit im Gesundheitswesen“ (DIG)

mailto:schuetze@medizin-informatik.org

https://gesundheitsdatenschutz.org