Hacker, der

Geschlecht: männlich, weiblich oder divers

Alter: vorhanden

Interesse: Gesundheitsdaten stehlen und missbrauchen

Wohnort: Außerhalb der EU

...

Verarbeitung in Drittstaaten

Dr. Bernd Schütze

2. Fachtagung „Datenschutz im Gesundheitswesen“

Vita

HEALTHCARE SOLUTIONS

Deutsche Telekom Healthcare and Security Solutions GmbH
Dr. Bernd Schütze
Senior Experte Medical Data Security

☎ +49 (160) 9566 - 3145
Bernd.Schuetze@T-Systems.com

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
- > 20 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)
- Berufsverband Medizinischer Informatiker e.V. (BVMI)
- Fachverband Biomedizinische Technik e.V. (fbmt)
- HL7 Deutschland e.V.
- HE Deutschland e.V.

Agenda

Was ich heute vorstellen möchte ...

- Verarbeitung in einem Drittland: Einführung ins Thema
- Grundätze
- „Angemessenes“ Schutzniveau
- Standardvertragsklauseln
- Interne Datenschutzvorschriften - Binding Corporate Rules
- Ausnahmeregelungen
- Praxisteil: Controller–Processor Standardvertragsklauseln
- Praxisteil: Controller –Controller Standardvertragsklauseln
- Diskussion/Fragen

Grundsätzlicher Hinweis

Diskussion/Fragen

Virtuelle Seminare stellen besondere Herausforderungen an die Interaktion. Deshalb:

- Einzelne Blöcke sind abgetrennt voneinander
  (graue Trennfolie mit Überschrift des folgenden Blockes)
- Nach jedem Block gibt es Zeit, Fragen zu dem gerade besprochenen Block zu stellen
- Zum Schluss gebt es dann die Gesamtdiskussion

Verarbeitung in einem Drittland: Einführung ins Thema

Zielrichtung der DS-GVO: Freier Verkehr personenbezogener Daten in der Union

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?

Definition eines Drittlands

- 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

Verarbeitung personenbezogener Daten in einem Drittstaat

Allgemeine Voraussetzungen

- Grundsatz: Schutz personenbezogener Daten europäischer Bürger bleibt 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

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)

b) Datenübermittlung vorbehaltlich geeigneter Garantien (Art.46)

c) Verbindliche interne Datenschutzvorschriften (Art. 47)

d) Ausnahmen für bestimmte Fälle existieren (Art. 49)

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“?

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 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

* 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

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?

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

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

„Angemessenes“ Schutzniveau

Drittlandverarbeitung nur bei angemessenem Schutzniveau

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 (2020-06-23) vorliegende Angemessenheitsbeschlüsse:

  Andorra, Argentinien, Kanada, Färöer-Inseln, Guernsey, Israel, Isle of Man, Japan, Jersey, Neuseeland, Schweiz, Uruguay und Vereinigte Staaten von Amerika (beschränkt auf Privacy Shield)

Drittlandverarbeitung nur bei angemessenem Schutzniveau

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

Cave: Verarbeitung von Sozialdaten in einem Drittland

§ 80 SGB X: Verarbeitung von Sozialdaten im Auftrag

– § 80 Abs. 2 SGB X:

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 Absatz 7 des Ersten Buches gleichgestellten Staat *(= EWR oder Schweiz)*, oder,
- **sofern ein Angemessenheitsbeschluss gemäß Artikel 45** der Verordnung (EU) 2016/679 vorliegt, in einem Drittstaat oder in einer internationalen Organisation erfolgt.

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

Drittlandverarbeitung nur bei angemessenem Schutzniveau , auch ohne Angemessenheitsbeschluss

Datenübermittlung vorbehaltlich geeigneter Garantien (Art.46)

- **Mit** Genehmigung einer Aufsichtsbehörde können Garantien bestehen in
  - Vertragsklauseln, die zwischen dem Verantwortlichen und dem Empfänger der Daten vereinbart wurden
  - Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind

Drittlandverarbeitung nur bei angemessenem Schutzniveau, auch ohne Angemessenheitsbeschluss

Datenübermittlung vorbehaltlich geeigneter Garantien (Art.46)

– **Ohne** Genehmigung einer Aufsichtsbehörde können Garantien bestehen in
  - einem rechtlich bindenden und durchsetzbaren Dokument zwischen den Behörden oder öffentlichen Stellen,
  - verbindlichen **internen Datenschutzvorschriften** (Art. 47)
  - **Standarddatenschutzklauseln der EU Kommission**
  - von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der Kommission genehmigt wurden
  - genehmigten Verhaltensregeln zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland
  - einem genehmigten Zertifizierungsmechanismus zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland

Standarddatenschutzklauseln (Standardvertragsklauseln)

Standarddatenschutzklauseln

Standarddatenschutzklauseln oder Standardvertragsklauseln?

- 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 beschlossenen 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 [...]“
- Bisherige Vertragsklauseln von der Kommission beibehalten*, was nach Art. 46 Abs. 5 S. 2 DS-GVO auch legitim ist. Daher wird im Folgenden von den existierenden Standardvertragsklauseln gesprochen

* Durchführungsbeschluss (EU) 2016/2297 der Kommission vom 16. Dezember 2016 zur Änderung der Entscheidung 2001/497/EG und des Beschlusses 2010/87/EU über Standardvertragsklauseln. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016D2297

Standardvertragsklauseln (standard contractual clauses, SCC)

Datenverkehr mit Drittstaaten*

- Zwei Arten Klauseln
  - EU Verantwortlicher und nicht-EU or EWR Verantwortlichen
    - Klauseln der Kommission vom 15. Juni 2001 https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32001D0497
    - Klauseln der Kommission vom 27. Dezember 2004 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32004D0915
  - EU Verantwortlicher und nicht-EU or EWR Auftragsverarbeiter
    - Klauseln der Kommission vom 5. Februar 2010 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32010D0087

* EU Commission: International data transfers using model contracts. Online unter https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_de

Standardvertragsklauseln (standard contractual clauses, SCC)

Datenverkehr mit Drittstaaten*

- 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, **Datenübermittlungen** zu **kontrollieren**
  - Auf Standardvertragsklauseln basierende **Übermittlungen** in ein Drittland **können** von Aufsichtsbehörde **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.

* EU Commission: International data transfers using model contracts. Online unter https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_de

Controller - Controller

Unterschiede Set I vs. Set II

- Beide Sets weiterhin gültig
- Set II („alternative Vertragsklauseln“)
  - Von verschiedenen Wirtschaftsverbänden entwickelt und von der EU Kommission genehmigt
  - Enthalten neuere Regelungen, welche den Erfordernissen der Wirtschaft besser Rechnung tragen
- Beispiel Haftung
  - Set I sieht gesamtschuldnerische Haftung von Datenexporteurs und Datenimporteurs für Schäden vor, die nur eine der Parteien bei einer betroffenen Person verursachte
  - Set II beinhaltet Klausel, dass jede Partei grundsätzlich nur für selbst verursachte Schäden verantwortlich ist

→ Einzelfallprüfung erforderlich, welches Set für das jeweilige Vertragsverhältnis besser passt

Controller - Processor

Standardvertragsklauseln: Controller - Processor

- Klauseln zwischen Verantwortlichem in EU und Auftragsverarbeiter in Drittland
- Vertrag muss direkt zwischen diesen abgeschlossen werden, d.h. **kein Vertrag zwischen Auftragsverarbeiter und Unter-Auftragsverarbeitung**
- Optionaler Anhang 3 zur Gewährleistung nat. Rechts möglich
- Rahmenbedingungen beachten, z.B.
  - ErwGr. 12: Standardvertragsklauseln sehen technische und organisatorische Sicherheitsmaßnahmen vor, die Datenverarbeiter in einem Drittland ohne angemessenes Schutzniveau anwenden, um EU Schutzniveau zu gewährleisten
    → Anhang 2 der Klauseln
  - Entschädigungsklauseln *können* vorhanden sein
    - In Anbetracht der Regelungen der DS-GVO ist fraglich, ob diese unter RL 95/46 EG getroffene Vorgabe weiter so gelten kann
    - Im Zweifelsfall übernimmt der Verantwortliche alleinige Verantwortung gegenüber betroffener Person

Controller - Processor

Pflichten für Datenexporteur

- Klausel 4 enthält Pflichten für Datenexporteur, (= Verantwortlicher)
- Z.B.
  - Datenexporteur sorgt für die Einhaltung der Sicherheitsmaßnahmen
  - Datenexporteur informiert betroffene Person vor oder sobald wie möglich nach der Übermittlung von Drittstaatenverarbeitung
  - Datenexporteur stellt betroffener Person auf Anfrage Klauseln sowie Kopie des Vertrages über Datenverarbeitungsdienste zur Verfügung

Controller - Processor

Pflichten für Datenimporteur

- Klausel 5 enthält Pflichten für Datenimporteur (= Auftragsverarbeiter)
- Z.B.
  - Datenimporteur garantiert, dass er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt
  - Datenimporteur garantiert, dass er bei der Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt und seine vorherige schriftliche Einwilligung eingeholt hat

Standardvertragsklauseln

Apropos Pflichten ...

- Standardvertragsklauseln werden **immer** zwischen Verantwortlichen in der EU und Auftragsverarbeiter bzw. Verantwortlichen im Drittland abgeschlossen
- D.h. Verantwortlicher in der EU ist **immer** Vertragspartner und verantwortlich für den Vertragsabschluss
- Hinweis:
  - Verträge zwischen Auftragsverarbeiter und Unterauftragsverarbeiter in der EU werden häufig zwischen diesen abgeschlossen
  - Bei Drittländern lassen sich Auftragsverarbeiter häufig **vom Verantwortlichen das Recht übertragen**, **für diesen** einen Standardvertrag mit dem Auftragsverarbeiter im Drittland abzuschließen

  ➔ Vertragspartner ist trotzdem der Verantwortliche, also Krankenhaus & Co in Deutschland

Standardvertragsklauseln: Hinweis zu „Schrems II“

Rechtssache „Facebook Ireland und Schrems“, AZ C-311/18

– Zur Erinnerung:
  - 2013 beschwerte sich ein junger Jurastudent (Max Schrems) bei der irischen Datenschutzaufsicht über die Datentransfers von Facebook
  - Irische Aufsicht legte EuGH Fragen vor
  - 2015 entschied EuGH, „Safe Harbour“ sei und war nie mit EU-Recht vereinbar
  - Irische Aufsicht teilte 2015 Max Schrems mit, Facebook habe Datentransfer nie auf Safe Harbour, sondern auf Standardvertragsklauseln gestützt
  - Daraufhin passte (inzwischen selbst Anwalt) Herr Schrems seine Beschwerde diesen neuen Tatsachen an und forderte die irische Aufsicht zur Untersagung des Facebook-Datentransfers auf
  - 2018 stellte der irische High Cour eine gezielte und massenhafte Überwachung durch die Regierungsbehörden der USA festgestellt und dem EuGH eine Reihe von Fragen vorgelegt
  - 19. Dez. 2019 hielt EU Generalanwalt seinen Schlussantrag
  - EuGH folgt sehr oft diesem Schlussantrag

Standardvertragsklauseln: Hinweis zu „Schrems II“

Rechtssache „Facebook Ireland und Schrems“, AZ C-311/18: Schlussantrag

- Schlussantrag in 19 EU-Sprachen (aber nicht auf Deutsch) auf EUR-Lex verfügbar (curia.europa.eu/juris/celex.jsf?celex=62018CC0311&lang1=de&type=TXT&ancre=)
- Im Schlussantrag findet sich
  - Gültigkeit des Kommissions-Beschlusses 2010/87 bzgl. Vertragsklauseln durch Prüfung der vorgelegten Fragen nicht beeinträchtigt
  - Die vom Exporteur (d.h. **vom Verantwortlichen**) u. a. durch vertragliche Mittel **getroffenen Schutzmaßnahmen müssen** selbst ein dem EU-Recht genügendes **Schutzniveau gewährleisten**
  - Standardvertragsklauseln dürfen **nicht angewendet** oder **müssen ausgesetzt werden**, wenn die Klauseln aufgrund eines **Konflikts zwischen** den **Verpflichtungen**, die sich aus den Standardklauseln ergeben, und den Verpflichtungen, die sich aus dem **Recht des Bestimmungsdrittlands** ergeben, **nicht eingehalten werden können**.

Standardvertragsklauseln: Zukunftsaussicht basierend auf „Schrems II“

Rechtssache „Facebook Ireland und Schrems“, AZ C-311/18: Was ist zu erwarten?

Wenn der EuGH dem Schlussantrag folgt:

- Standardvertragsklauseln bleiben bestehen, Privacy Shield wird nicht betrachtet
- Verantwortliche müssen **bei Vertragsabschluss prüfen**, ob **Recht des Bestimmungsdrittlands** eine **Anwendung** der Standardvertragsklauseln **erlauben**
- Verantwortliche müssen **während Vertragslaufzeit prüfen**, ob **Recht des Bestimmungsdrittlands** eine **Anwendung** der Standardvertragsklauseln **erlauben**, d.h. Änderung des Rechts des Bestimmungsdrittlandes verfolgen
- Wenn SCC nicht eingehalten werden können, **muss Drittlandtransfer ausgesetzt werden**
- Bei Beschwerden von betroffenen Personen muss die Aufsichtsbehörde prüfen, ob Recht des Bestimmungsdrittlands eine Anwendung der Standardvertragsklauseln erlauben oder eine Verarbeitung im Drittland beendet werden muss

➔ Wenn es so kommt: bei Übertragung des Rechts auf Vertragsabschluss entsprechende Pflichten in Verträge mit Auftragsverarbeitern aufnehmen und Haftungsfrage klären

Interne Datenschutzvorschriften - Binding Corporate Rules

Binding Corporate Rules (BCR*)

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) und Auftragsverarbeitung

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) und Auftragsverarbeitung

BCR kann Auftragsverarbeitern die Verarbeitung im Drittstaat erlauben

- Daher zu unterscheiden
  - a) BCR für Verantwortliche:

    Regeln Datentransfers durch Verantwortliche an gruppenangehörige Verantwortliche oder Auftragsverarbeiter in einem Drittland
  - b) BCR für Auftragsverarbeiter:

    Regeln Datenflüsse innerhalb von Unternehmensgruppen, deren Gruppenmitglieder als Auftragsverarbeiter für konzernfremde Auftraggeber agieren.
- Für beide BCR-Arten existieren Leitlinien der Art.-29-Datenschutzgruppe bzw. des EU Datenschutzausschusses

Binding Corporate Rules (BCR)

Vorgaben Aufsichtsbehörde: Artikel-29-Datenschutzgruppe

- Einige WP der Art-29-Datenschutzgruppe vom Datenschutz-Ausschuss anerkannt*
  - Working Document Setting Forth a Co-Operation Procedure for the approval of “Binding Corporate Rules” for controllers and processors under the GDPR, WP 263 rev.01
  - Recommendation on the Standard Application for Approval of Controller Binding Corporate Rules for the Transfer of Personal Data, WP 264
  - Recommendation on the Standard Application form for Approval of Processor Binding Corporate Rules for the Transfer of Personal Data, WP 265
  - Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, WP 256 rev.01
  - Working Document setting up a table with the elements and principles to be found in Processor Binding Corporate Rules, WP 257 rev.01
- Ältere WP können weiterhin hilfreich sein, da Aufsichtsbehörden auf diese verweisen

* siehe EDSA: Endorsement of GDPR WP29 Documents, https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de

Binding Corporate Rules (BCR)

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
    a) Unternehmensgruppe oder
    b) Gruppe von Unternehmen
  - Alle Beteiligten müssen die BCR anerkennen, damit BCR die erforderliche Wirkung entfalten
- Liste bei der EU-Kommission (allerdings nur bis 25. Mai 2018)
  - List of companies for which the EU BCR cooperation procedure is closed https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=613841

Ausnahmeregelungen

Verarbeitung personenbezogener Daten in einem Drittstaat

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
  - **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 **Durchführung 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
  - Übermittlung ist zum Abschluss oder zur Erfüllung eines **im Interesse der betroffenen Person** von dem Verantwortlichen mit einer anderen Person geschlossenen Vertrags erforderlich (insbesondere bei Vertrag zu Gunsten Dritter nach § 328 BGB anwendbar)

Verarbeitung personenbezogener Daten in einem Drittstaat

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 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
  - 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

Verarbeitung personenbezogener Daten in einem Drittstaat

Ausnahmen für bestimmte Fälle existieren (Art. 49)

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

Verarbeitung personenbezogener Daten in einem Drittstaat : Sicht der europäischen Aufsichtsbehörden*

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

Praxisteil:
Controller – Processor Standardvertragsklauseln

Beispiel: Fernwartung von IT-Systemen

Auftragsverarbeiter in der EU, Unterauftragsverarbeiter in Drittland

- IT-System gekauft und betrieben von Krankenhaus
- Wartung & Co durch bei Hersteller mit Sitz in Deutschland im Rahmen einer Auftragsverarbeitung
- Teil der Wartung wird durch einem Unternehmensteil in einem Drittland durchgeführt
- BCR existieren nicht

➔ Abschluss von Standardvertragsklauseln zwischen Krankenhaus und Unternehmen im Drittland erforderlich

➔ D.h. Controller-Processor-Klauseln, Kommissionentscheid 2010/87/EU (https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087)

Beispiel: Fernwartung von IT-Systemen

Standardvertragsklauseln : Controller-Processor

- Klausel 1: Begriffsbestimmungen
  - lit. a orientiert sich an die DSRL, natürlich wird dies von Art. 4 DS-GVO überlagert
  - Art. 94 Abs. 2 DS-GVO: „Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung.“
  - Aber:
    - Definition nach Art. 9 Abs. 1 DS-GVO ist weitergehend als der Begriff „besondere Kategorien personenbezogener Daten/sensible Daten“, z.B. enthält DS-GVO genetische Daten und biometrische Daten
    - Da Klauseln nicht geändert werden kann, kann hier bei Bedarf eine Ergänzungsvereinbarung zu den SCC getroffen werden, welche die Nutzung der Definitionen der DS-GVO vereinbart

Beispiel: Fernwartung von IT-Systemen

Standardvertragsklauseln : Controller-Processor

- Klausel 2: Einzelheiten der Übermittlung (Verweis auf Anhang 1)
- Klausel 3: Drittbegünstigtenklausel
  - Im Rahmen des Vertrages gelten betroffene Personen als „Drittbegünstigte“
  - Ihnen werde Rechte eingeräumt, auch wenn sie keine Vertragsparteien sind
  - Betroffene Personen können somit Klauseln gegenüber Datenexporteur, Datenimporteur oder gegenüber Unterauftragsverarbeiter ausüben

Drittbegünstigtenklausel

(1) Die betroffenen Personen können diese Klausel sowie Klausel 4 Buchstaben b bis i, Klausel 5 Buchstaben a bis e und g bis j, Klausel 6 Absätze 1 und 2, Klausel 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenexporteur als Drittbegünstigte geltend machen.

(2) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Datenimporteur geltend machen, wenn das Unternehmen des Datenexporteurs faktisch oder rechtlich nicht mehr besteht, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen.

(3) Die betroffene Person kann diese Klausel, Klausel 5 Buchstaben a bis e und g, die Klauseln 6 und 7, Klausel 8 Absatz 2 sowie die Klauseln 9 bis 12 gegenüber dem Unterauftragsverarbeiter geltend machen, wenn sowohl das Unternehmen des Datenexporteurs als auch das des Datenimporteurs faktisch oder rechtlich nicht mehr bestehen oder zahlungsunfähig sind, es sei denn, ein Rechtsnachfolger hat durch einen Vertrag oder kraft Gesetzes sämtliche rechtlichen Pflichten des Datenexporteurs übernommen; in letzterem Fall kann die betroffene Person die Klauseln gegenüber dem Rechtsnachfolger als Träger sämtlicher Rechte und Pflichten des Datenexporteurs geltend machen. Eine solche Haftpflicht des Unterauftragsverarbeiters ist auf dessen Verarbeitungstätigkeiten nach den Klauseln beschränkt.

(4) Die Parteien haben keine Einwände dagegen, dass die betroffene Person, sofern sie dies ausdrücklich wünscht und das nationale Recht dies zulässt, durch eine Vereinigung oder sonstige Einrichtung vertreten wird.

Beispiel: Fernwartung von IT-Systemen

Standardvertragsklauseln : Controller-Processor

– Klausel 4: Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

a) ...

d) die Sicherheitsmaßnahmen unter Berücksichtigung der Anforderungen des anwendbaren Datenschutzrechts, des Standes der Technik, der bei ihrer Durchführung entstehenden Kosten, der von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten hinreichend gewährleisten, dass personenbezogene Daten vor der zufälligen oder unrechtmäßigen Zerstörung, dem zufälligem Verlust, der Änderung, der unberechtigten Weitergabe oder dem unberechtigten Zugang, insbesondere wenn die Verarbeitung die Übermittlung der Daten über ein Netzwerk umfasst, und vor jeder anderen Form der unrechtmäßigen Verarbeitung geschützt sind;

e) **er für die Einhaltung dieser Sicherheitsmaßnahmen sorgt**;

Beispiel: Fernwartung von IT-Systemen

Standardvertragsklauseln : Controller-Processor

– Klausel 4: Pflichten des Datenexporteurs

Der Datenexporteur erklärt sich bereit und garantiert, dass:

f) die **betroffene Person** bei der **Übermittlung besonderer Datenkategorien vor oder sobald wie möglich nach der Übermittlung** davon **in Kenntnis gesetzt** worden ist oder gesetzt wird, **dass ihre Daten in ein Drittland übermittelt werden** könnten, das kein angemessenes Schutzniveau im Sinne der Richtlinie 95/46/EG bietet;

g) ...

h) er den **betroffenen Personen auf Anfrage eine Kopie der Klauseln** mit Ausnahme von Anhang 2 sowie eine allgemeine Beschreibung der Sicherheitsmaßnahmen zur Verfügung stellt; außerdem stellt er ihnen gegebenenfalls **die Kopie des Vertrags über Datenverarbeitungsdienste** zur Verfügung, der gemäß den Klauseln an einen Unterauftragsverarbeiter vergeben wurde, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden;

j) er für die Einhaltung der Klausel 4 Buchstaben a bis i sorgt.

Beispiel: Fernwartung von IT-Systemen

Standardvertragsklauseln : Controller-Processor

– Klausel 5: Pflichten des Datenimporteurs

Der Datenimporteur erklärt sich bereit und garantiert, dass:

a) er die personenbezogenen Daten **nur im Auftrag des Datenexporteurs** und in **Übereinstimmung mit dessen Anweisungen** und den vorliegenden Klauseln **verarbeitet**; dass er sich, falls er **dies aus irgendwelchen Gründen nicht einhalten kann,** bereit erklärt, den **Datenexporteur unverzüglich davon in Kenntnis zu setzen**, der unter diesen Umständen berechtigt ist, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

b) er **seines Wissens keinen Gesetzen unterliegt**, die ihm die Befolgung der **Anweisungen des Datenexporteurs** und die **Einhaltung seiner vertraglichen Pflichten unmöglich machen**, und eine **Gesetzesänderung**, die sich voraussichtlich sehr **nachteilig auf die Garantien und Pflichten auswirkt**, die die Klauseln bieten sollen, **dem Datenexporteur mitteilen** wird, sobald er von einer solchen Änderung Kenntnis erhält; unter diesen Umständen ist der Datenexporteur berechtigt, die Datenübermittlung auszusetzen und/oder vom Vertrag zurückzutreten;

Beispiel: Fernwartung von IT-Systemen

Standardvertragsklauseln : Controller-Processor

– Klausel 5: Pflichten des Datenimporteurs

Der Datenimporteur erklärt sich bereit und garantiert, dass:

c) ...

d) er den Datenexporteur unverzüglich informiert über

i. **alle rechtlich bindenden Aufforderungen einer Vollstreckungsbehörde zur Weitergabe der personenbezogenen Daten**, **es sei denn, dies wäre anderweitig untersagt**, beispielsweise durch ein strafrechtliches Verbot zur Wahrung des Untersuchungsgeheimnisses bei strafrechtlichen Ermittlungen;

ii. **jeden zufälligen oder unberechtigten Zugang** und

iii. alle Anfragen, die direkt von den betroffenen Personen an ihn gerichtet werden, ohne diese zu beantworten, es sei denn, er wäre anderweitig dazu berechtigt;

Beispiel: Fernwartung von IT-Systemen

Standardvertragsklauseln : Controller-Processor

– Klausel 5: Pflichten des Datenimporteurs

Der Datenimporteur erklärt sich bereit und garantiert, dass:

e) er alle Anfragen des Datenexporteurs im Zusammenhang mit der Verarbeitung der übermittelten personenbezogenen Daten durch den Datenexporteur unverzüglich und ordnungsgemäß bearbeitet und **die Ratschläge der Kontrollstelle im Hinblick auf die Verarbeitung der übermittelten Daten befolgt**;

f) er den betroffenen Personen auf Anfrage eine Kopie der Klauseln und gegebenenfalls einen bestehenden Vertrag über die Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter zur Verfügung stellt, es sei denn, die Klauseln oder der Vertrag enthalten Geschäftsinformationen; in diesem Fall können solche Geschäftsinformationen herausgenommen werden; Anhang 2 wird durch eine allgemeine Beschreibung der Sicherheitsmaßnahmen ersetzt, wenn die betroffene Person vom Datenexporteur keine solche Kopie erhalten kann;

Beispiel: Fernwartung von IT-Systemen

Standardvertragsklauseln : Controller-Processor

– Klausel 5: Pflichten des Datenimporteurs

Der Datenimporteur erklärt sich bereit und garantiert, dass:

h) er bei der **Vergabe eines Verarbeitungsauftrags an einen Unterauftragsverarbeiter den Datenexporteur vorher benachrichtigt** und seine **vorherige schriftliche Einwilligung** eingeholt hat;

i) der Unterauftragsverarbeiter die Datenverarbeitungsdienste in Übereinstimmung mit Klausel 11 erbringt;

j) er dem **Datenexporteur unverzüglich eine Kopie des Unterauftrags über die Datenverarbeitung zuschickt,** den er nach den Klauseln geschlossen hat.

Beispiel: Fernwartung von IT-Systemen

Standardvertragsklauseln : Controller-Processor

- Klausel 6: Haftung
- Klausel 7: Schlichtungsverfahren und Gerichtsstand
- Klausel 8: Zusammenarbeit mit Kontrollstellen
- Klausel 9: Anwendbares Recht
- Klausel 10: Änderung des Vertrag
- Klausel 11: Vergabe eines Unterauftrags
- Klausel 12: Pflichten nach Beendigung der Datenverarbeitungsdienste

Beispiel: Mitbehandlung durch weisungsfreie Personen

Standardvertragsklauseln : Controller-Processor

Anhang 1 (weitergehende Angaben)

- Datenexporteur
  - Angabe zum Datenexporteur, insbesondere Angabe der Tätigkeiten, die für die Übermittlung von Belang
- Datenimporteur
  - Angabe zum Datenimporteur, insbesondere Angabe der Tätigkeiten, die für die Übermittlung von Belang
- Betroffene Personen
  - Ggf. Kategorien von Personen
- Kategorien übermittelter Daten
- Besondere Datenkategorien (falls zutreffend)

Beispiel: Mitbehandlung durch weisungsfreie Personen

Standardvertragsklauseln : Controller-Processor

Anhang 1 (weitergehende Angaben)

- ...
- Verarbeitung
  (Angaben, die erforderlich sind um Art. 28 DS-GVO zu genügen)
  - Gegenstand
  - Dauer
  - Umfang, Art und Zweck
  - Unteraufträge
  - Weisungsbefugnisse
  - Unterstützungspflichten
  - Rückgabe überlassener Datenträger und die Löschung von Daten

Beispiel: Mitbehandlung durch weisungsfreie Personen

Standardvertragsklauseln : Controller-Processor

Anhang 2

– Beschreibung der technischen oder organisatorischen Sicherheitsmaßnahmen, die der Datenimporteur gemäß Klausel 4 Buchstabe d und Klausel 5 Buchstabe c eingeführt hat

Beispiel: Mitbehandlung durch weisungsfreie Personen

Bewertung des Rechts des Drittstaates: Beispiel USA

- Schutz von Gesundheitsdaten
  - 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 Ärzte & Co werden auch Unternehmen in die Pflicht genommen
    - Gleichzeitig leichtere Nutzung von Daten zu Forschungszwecken ermöglicht
  - 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

Beispiel: Mitbehandlung durch weisungsfreie Personen

Bewertung des Rechts des Drittstaates: Beispiel USA

- Schutz von Gesundheitsdaten
  - Landesrecht
    - Die meisten US Bundesstaaten erließen ergänzende Regelungen
    - Schutzniveau variiert daher erheblich von Bundesland zu Bundesland
  - 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
  - Fazit:
    - Andere Zielrichtung der Gesetzgebung
    - Um ein der DS-GVO angemessenes Schutzniveau zu erzielen, müssen ergänzende vertragliche Vereinbarungen getroffen werden

Beispiel: Mitbehandlung durch weisungsfreie Personen

Bewertung des Rechts des Drittstaates: Beispiel USA

- Zugriff durch Behörden
  - 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 eine Vorladung (subponea) oder einen Gerichtsbeschluss (court order) beruht
      - ✓ Keine Informationspflicht, wenn content-Herausgabe auf einen Durchsuchungsbeschluss (warrant) beruht
      - ✓ Grundsätzlich keine Informationspflicht bei Herausgabe von records
  - Fazit:
    - ➢ Auch mit vertraglichen Regelungen wird man ein dem EU-Recht entsprechendes Schutzniveau nicht erzielen können

Beispiel: Mitbehandlung durch weisungsfreie Personen

Bewertung des Rechts des Drittstaates: Beispiel USA

– Zugriff durch Behörden

Hinweis: Stark vereinfachte Darstellung

1) Natürlich müssen mehr Gesetze betrachtet werden und es
2) muss ein *angemessenes* Schutzniveau erzielt werden, kein *gleichwertiges*

nicht erzielen können

Praxisteil:
Controller – Controller Standardvertragsklauseln

Beispiel: Mitbehandlung durch weisungsfreie Personen

Merke: Weisungsfreiheit schließt weisungsgebundene Arbeit aus – keine AV

- Mitbehandlung durch weisungsfreie Personen, i.d.R. Ärzte, oder gemeinsame Forschung
- Z.B. Krankenhaus in einem Drittland, welches eine Diagnostik anbietet, die für die Behandlung in Deutschland benötigt wird (z.B. 3-D-Rekonstruktion für eine OP)
- Zusammenarbeit findet regelmäßig statt, da diese Kooperation bei jedem dieser Eingriffe erforderlich ist
- Keine Auftragsverarbeitung möglich, da Auftragsverarbeitung weisungsgebundene Verarbeitung voraussetzt
- Daher Controller-Controller-SCC, gewählt wird Set II (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0915)

Beispiel: Mitbehandlung durch weisungsfreie Personen

Standardvertragsklauseln Set II: Controller-Controller

- Angabe Vertragspartner
- Begriffsbestimmungen
  - lit. a orientiert sich an die DSRL, natürlich wird dies von Art. 4 DS-GVO überlagert
  - Art. 94 Abs. 2 DS-GVO: „Verweise auf die aufgehobene Richtlinie gelten als Verweise auf die vorliegende Verordnung."
  - Aber:
    - Definition nach Art. 9 Abs. 1 DS-GVO ist weitergehend als der Begriff „besondere Kategorien personenbezogener Daten/sensible Daten", z.B. enthält DS-GVO genetische Daten und biometrische Daten
    - Da Klauseln nicht geändert werden kann, kann hier bei Bedarf eine Ergänzungsvereinbarung zu den SCC getroffen werden, welche die Nutzung der Definitionen der DS-GVO vereinbart

Beispiel: Mitbehandlung durch weisungsfreie Personen

Standardvertragsklauseln Set II: Controller-Controller

I. Pflichten des Datenexporteurs

Der Datenexporteur gibt folgende Zusicherungen:

a) Die personenbezogenen Daten wurden nach den für den Datenexporteur geltenden Gesetzen gesammelt, verarbeitet und übermittelt.

b) Er hat sich im Rahmen des Zumutbaren davon **überzeugt**, dass der **Datenimporteur seine Rechtspflichten aus diesen Klauseln zu erfüllen in der Lage ist**.

c) Er stellt dem Datenimporteur auf Antrag Exemplare der einschlägigen Datenschutzgesetze oder entsprechende Fundstellennachweise seines Sitzlandes zur Verfügung, erteilt aber keine Rechtsberatung.

Beispiel: Mitbehandlung durch weisungsfreie Personen

Standardvertragsklauseln Set II: Controller-Controller

I. Pflichten des Datenexporteurs

Der Datenexporteur gibt folgende Zusicherungen:

d) Er beantwortet Anfragen der betroffenen Personen und der Kontrollstelle bezüglich der Verarbeitung der personenbezogenen Daten durch den Datenimporteur,

es sei denn, die Parteien haben vereinbart, dass der Datenimporteur die Beantwortung übernimmt;

der **Datenexporteur übernimmt die Beantwortung** im Rahmen der Zumutbarkeit und aufgrund der ihm zugänglichen Informationen auch dann, **wenn der Datenimporteur nicht antworten will oder kann**.

Sie erfolgt innerhalb einer angemessenen Frist.

Beispiel: Mitbehandlung durch weisungsfreie Personen

Standardvertragsklauseln Set II: Controller-Controller

I. Pflichten des Datenexporteurs

Der Datenexporteur gibt folgende Zusicherungen:

e) Er stellt **betroffenen Personen**, die Drittbegünstigte im Sinne von Klausel III sind, **auf Verlangen ein Exemplar der Klauseln zur Verfügung**, es sei denn, die Klauseln enthalten vertrauliche Angaben; in diesem Fall hat er das Recht, diese Angaben zu entfernen.

Werden Angaben entfernt, teilt der Datenexporteur den betroffenen Personen schriftlich die Gründe für die Entfernung mit und belehrt sie über ihr Recht, die Kontrollstelle auf die Entfernung aufmerksam zu machen.

Der Datenexporteur leistet indessen der Entscheidung der Kontrollstelle Folge, den betroffenen Personen Zugang zum Volltext der Klauseln zu gewähren, wenn diese sich zur Geheimhaltung der entfernten vertraulichen Informationen verpflichten.

Der Datenexporteur stellt ferner auch der Kontrollstelle auf Antrag ein Exemplar der Klauseln zur Verfügung.

Beispiel: Mitbehandlung durch weisungsfreie Personen

Standardvertragsklauseln Set II: Controller-Controller

II. Pflichten des Datenimporteurs

Der Datenimporteur gibt folgende Zusicherungen:

a) Er verfügt über die technischen und organisatorischen Voraussetzungen zum Schutz der personenbezogenen Daten gegen die unbeabsichtigte oder rechtswidrige Zerstörung oder gegen den unbeabsichtigten Verlust oder die unbeabsichtigte Änderung, die unberechtigte Offenlegung oder den unberechtigten Zugriff; damit ist ein Sicherheitsniveau gewährleistet, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden Daten gerecht wird.

Beispiel: Mitbehandlung durch weisungsfreie Personen

Standardvertragsklauseln Set II: Controller-Controller

II. Pflichten des Datenimporteurs

Der Datenimporteur gibt folgende Zusicherungen:

b) Seine Verfahrensregeln gewährleisten, dass von ihm zum Zugriff auf die personenbezogenen Daten befugte Dritte, einschließlich des Auftragsverarbeiters, die Geheimhaltung und Sicherheit der personenbezogenen Daten beachten und wahren. Die unter der Verantwortung des Datenimporteurs tätigen Personen, darunter auch Auftragsverarbeiter, dürfen die personenbezogenen Daten nur auf seine Anweisung verarbeiten. Diese Bestimmung gilt nicht für Personen, die von Rechts wegen zum Zugriff auf die personenbezogenen Daten befugt oder verpflichtet sind.

c) Zum **Zeitpunkt des Vertragsabschlusses** bestehen seines Wissens in **seinem Land keine entgegenstehenden Rechtsvorschriften**, die **die Garantien aus diesen Klauseln in gravierender Weise beeinträchtigen**; er benachrichtigt den Datenexporteur (der die Benachrichtigung erforderlichenfalls an die Kontrollstelle weiterleitet), wenn er Kenntnis von derartigen Rechtsvorschriften erlangt.

Beispiel: Mitbehandlung durch weisungsfreie Personen

Standardvertragsklauseln Set II: Controller-Controller

II. Pflichten des Datenimporteurs

Der Datenimporteur gibt folgende Zusicherungen:

d) Er verarbeitet die personenbezogenen Daten zu den in Anhang B dargelegten Zwecken und ist ermächtigt, die Zusicherungen zu geben und die Verpflichtungen zu erfüllen, die sich aus diesem Vertrag ergeben.

e) Er **nennt dem Datenexporteur eine Anlaufstelle innerhalb seiner Organisation**, die befugt ist, **Anfragen bezüglich der Verarbeitung der personenbezogenen Daten zu behandeln**, und arbeitet redlich mit dem Datenexporteur, der betroffenen Person und der Kontrollstelle zusammen, damit derartige Anfragen innerhalb einer angemessenen Frist beantwortet werden. Wenn der Datenexporteur nicht mehr besteht oder wenn die Parteien Entsprechendes vereinbaren, verpflichtet sich der Datenimporteur zur Einhaltung der Bestimmungen von Klausel I Buchstabe e).

f) ...

Beispiel: Mitbehandlung durch weisungsfreie Personen

Standardvertragsklauseln Set II: Controller-Controller

III. Haftung und Rechte Dritter
IV. Anwendbares Recht
V. Beilegung von Streitigkeiten mit betroffenen Personen oder der Kontrollstelle
VI. Beendigung des Vertrags
VII. Änderung der Klauseln
VIII. Beschreibung der Übermittlung

Beispiel: Mitbehandlung durch weisungsfreie Personen

Standardvertragsklauseln Set II: Controller-Controller

Anhang A: Grundsätze für die Datenverarbeitung

1. Zweckbindung
2. Datenqualität und Verhältnismäßigkeit
3. Transparenz
4. Sicherheit und Geheimhaltung
5. ...

ANHANG A

GRUNDSÄTZE FÜR DIE DATENVERARBEITUNG

1. Zweckbindung: Personenbezogene Daten dürfen nur für die in Anhang B festgelegten oder anschließend von der betroffenen Person genehmigten Zwecke verarbeite danach verwendet oder weiter übermittelt werden.
2. Datenqualität und Verhältnismäßigkeit: Personenbezogene Daten müssen sachlich richtig sein und nötigenfalls auf dem neuesten Stand gehalten werden. Sie müsse Übermittlungs- und Verarbeitungszwecken angemessen und dafür erheblich sein und dürfen nicht über das erforderliche Maß hinausgehen.
3. Transparenz: Die betroffenen Personen müssen Informationen erhalten, die eine Verarbeitung nach Treu und Glauben gewährleisten (beispielsweise Angaben Verarbeitungszweck und zur Übermittlung), sofern diese Informationen nicht bereits vom Datenexporteur erteilt wurden.
4. Sicherheit und Geheimhaltung: Der für die Verarbeitung Verantwortliche muss geeignete technische und organisatorische Sicherheitsvorkehrungen gegen die Risike Verarbeitung treffen, beispielsweise gegen die unbeabsichtigte oder rechtswidrige Zerstörung oder gegen den unbeabsichtigten Verlust oder die unbeabsichtigte Ände die unberechtigte Offenlegung oder den unberechtigten Zugriff. Alle unter der Verantwortung des für die Verarbeitung Verantwortlichen tätigen Personen, darunter Auftragsverarbeiter, dürfen die Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.
5. Recht auf Auskunft, Berichtigung, Löschung und Widerspruch: Nach Artikel 12 der Richtlinie 95/46/EG hat die betroffene Person das Recht, entweder direkt oder Dritte, Auskunft über alle ihre personenbezogenen Daten zu erhalten, die von einer Organisation vorgehalten werden; dies gilt nicht für Auskunftsersuchen, die aufg ihrer unzumutbaren Periodizität oder ihrer Zahl, Wiederholung oder Systematik offensichtlich übertrieben sind, oder für Daten, über die nach dem für den Datenexpo geltenden Recht keine Auskunft erteilt werden muss. Vorbehaltlich der vorherigen Genehmigung durch die Kontrollstelle muss auch dann keine Auskunft erteilt we wenn die Interessen des Datenimporteurs oder anderer Organisationen, die mit dem Datenimporteur in Geschäftsverkehr stehen, dadurch ernsthaft geschädigt würde die Grundrechte und Grundfreiheiten der betroffenen Personen hierdurch nicht beeinträchtigt werden. Die Quellen der personenbezogenen Daten müssen nicht angeg werden, wenn dazu unzumutbare Anstrengungen erforderlich wären oder die Rechte Dritter dadurch verletzt würden. Die betroffene Person muss das Recht haben, personenbezogenen Daten berichtigen, ändern oder löschen zu lassen, wenn diese unzutreffend sind oder entgegen den vorliegenden Grundsätzen verarbeitet wurden begründeten Zweifeln an der Rechtmäßigkeit des Ersuchens kann die Organisation weitere Belege verlangen, bevor die Berichtigung, Änderung oder Löschung er Dritte, gegenüber denen die Daten offen gelegt wurden, müssen von der Berichtigung, Änderung oder Löschung nicht in Kenntnis gesetzt werden, wenn dies mit e unverhältnismäßigen Aufwand verbunden wäre. Die betroffene Person muss auch aus zwingenden legitimen Gründen, die mit ihrer persönlichen Situ zusammenhängen, Widerspruch gegen die Verarbeitung ihrer personenbezogenen Daten einlegen können. Die Beweislast liegt im Fall einer Ablehnung Datenimporteur; die betroffene Person kann eine Ablehnung jederzeit vor der Kontrollstelle anfechten.
6. Sensible Daten: Der Datenimporteur trifft die zusätzliche Vorkehrungen (beispielsweise sicherheitsbezogener Art), die entsprechend seinen Verpflichtungen nach Kl II zum Schutz sensibler Daten erforderlich sind.
7. Direktmarketing: Werden Daten zum Zwecke des Direktmarketings verarbeitet, sind wirksame Verfahren vorzusehen, damit die betroffene Person sich jederzeit gege Verwendung ihrer Daten für derartige Zwecke entscheiden kann (‚Opt-out').
8. Automatisierte Entscheidungen: ‚Automatisierte Entscheidungen' im Sinne dieser Klauseln sind mit Rechtsfolgen behaftete Entscheidungen des Datenexporteurs ode Datenimporteurs bezüglich einer betroffenen Person, die allein auf der automatisierten Verarbeitung personenbezogener Daten zum Zwecke der Bewertung einz Aspekte ihrer Person beruhen, beispielsweise ihrer beruflichen Leistungsfähigkeit, ihrer Kreditwürdigkeit, ihrer Zuverlässigkeit oder ihres Verhaltens. Der Datenimpo darf keine automatisierten Entscheidungen über eine betroffene Person fällen, es sei denn:

Beispiel: Mitbehandlung durch weisungsfreie Personen

Standardvertragsklauseln Set II: Controller-Controller

Anhang B: Beschreibung der Übermittlung

- Betroffene Personen
- Übermittlungszwecke
- Kategorien übermittelter Daten
- Empfänger
- Sensible Daten (falls zutreffend)
- Datenschutzmelderegister-Angaben des Exporteurs (falls zutreffend)
- Sonstige nützliche Informationen (Aufbewahrungszeitraum und sonstige einschlägige Angaben)
- Anlaufstelle für Datenschutzauskünfte
  a) Datenimporteur
  b) Datenexporteur

Praxisteil: Standardvertragsklauseln - Fazit

Standardvertragsklauseln

Fazit

- Nutzung von Standardvertragsklauseln bei Drittlandverarbeitung letztlich unumgänglich
- Klauseln bedürfen der Aufmerksamkeit sowohl des Datenimporteurs als auch des Datenexporteurs
  - Insbesondere in Anbetracht des zu erwartenden Urteils Schrems/Facebook II
- An mehreren Stellen ist Verweis auf zu treffende Regelungen oder es besteht zur Schaffung von Rechtssicherheit Ergänzungsbedarf, z.B.
  - Beantwortung von Betroffenenanfragen oder
  - Haftungsfragen
- Daher vertragliche Ergänzung zu den Standardvertragsklauseln dringend zu empfehlen
- Hinweise zu Ergänzungen findet man in der Rechtsliteratur*

* z:B.: Moos F. (Hrsg.) Datenschutz- und Datennutzungsverträge. ottoschmidt Verlag, 2. Auflage 2018. ISBN: 978-3-504-56100-0

Diskussion / Fragen

Kontakt: Bernd.Schuetze@T-Systems.com