

Datenschutz in der medizinischen Forschung



"Rechtliche Aspekte im Forschungs-Daten-Management"
21.-25.03.2022

22.3.2022, Dr. T. Langbein
Datenschutzbeauftragter UMG

Datenschutz in der medizinischen Forschung

Agenda:

1. Worum geht's?
2. Wer hat's erfunden? Eine kurze Geschichte der Datenschutzgesetze
3. Gesetzliche Regelungen (allgemein)
4. Gesetzliche Regelungen in der Forschung
5. Digitalisierung und Forschung

Datenschutz? ...was geht mich das an??



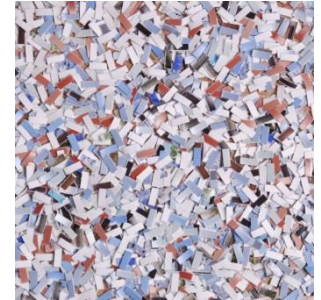
Datenschutz in der medizinischen Forschung

Datenschutz in der öffentlichen Wahrnehmung

11. Februar 2016, 16:19 Uhr

Untersuchungen zu Konfetti aus Patientenakten dauern an

Erfurt/Dermbach (dpa/th) - Nach dem Fund von Konfetti aus zerschredderten Patientenakten in Dermbach(Wartburgkreis) sind die genauen Umstände des Datenschutzverstoßes noch nicht bis ins letzte Detail geklärt.... Auf den nur grob zerkleinerten Papierschnipseln waren unter anderem Namen und Adressen erkennbar...



Patientendaten, Patente, Konstruktionspläne auf eBay-Festplatten gefunden

Verfasst von dub am 5. September 2014 - 14:06

[Datenpanne](#) [Sicherheit](#) [Datensicherheit](#) [Datenschutz](#) [Deutschland](#) [Österreich](#) [Patientendaten](#)



Bei der Überprüfung von gebrauchten Festplatten, welche die Marktplattform eBay in Österreich und Deutschland für das hauseigene Ersatzteillager angekauft hatte, fanden Spezialisten sensible Patientendaten aus der Praxis einer Kinderärztin sowie von einer Gemeinschaftspraxis für Interne Medizin.

Datenschutz in der medizinischen Forschung

Datenschutz in der öffentlichen Wahrnehmung

Der/die „gläserne Patient/in“...?



BILD erfuhr: Die Uni-Klinik Grenoble hat jetzt die Einsicht in die Patientenakte von Schumi gesperrt.

Bisher konnte jeder **der Krankenhaus-Mitarbeiter** (allein **1600** im medizinischen Bereich) per Computer einsehen, wie es dem verunglückten Schumi geht.

Jetzt wurde der Zugang gesperrt. Nur noch Chefarzte kommen mit persönlichen Codes an die Dokumente.

"Fall Lierhaus" alarmiert Datenschützer

3. Juni 2009 | 06:35 Uhr | Von Markus Lorenz

Datenschützer schlagen Alarm: Elektronische Krankenakten begünstigen den Missbrauch von Patientendaten. Beispiel: die Erkrankung von Monica Lierhaus.



[+ Vergrößern](#)

Monica Lierhaus: Die "Sportschau"-Moderatorin lag schwer erkrankt im Uniklinikum Eppendorf. Foto: dpa

Der Fall bewegte die Nation: Anfang des Jahres musste sich "Sportschau"-Moderatorin Monica Lierhaus im Hamburger Uniklinikum Eppendorf (UKE) einer Operation unterziehen. Angaben zum Krankheitsverlauf machte die Klinik nicht. Dennoch waren kurz danach Einzelheiten zum Gesundheitszustand der "Miss Sportschau" nachzulesen. Während Lierhaus das Krankenhaus laut "Bild"-

Zeitung inzwischen wieder verlassen hat, tobt nun der Streit darum, wie die intimen Details an die Öffentlichkeit geraten konnten.

Datenschutz in der medizinischen Forschung

Agenda:

1. Worum geht's?

2. **Wer hat's erfunden?** Eine kurze Geschichte der Datenschutzgesetze

3. Gesetzliche Regelungen (allgemein)

4. Gesetzliche Regelungen in der Forschung

5. Digitalisierung und Forschung

Datenschutz in der medizinischen Forschung

Geschichte der Datenschutzgesetze

Beginn des modernen Datenschutzes

Anfang der **1960er** Jahre in den USA („Privacy Act“ - Privatsphärengesetz)

Geschichte der Datenschutzgesetze

1970 Das Bundesland Hessen verabschiedet das erste allgemeine Datenschutzgesetz der Welt

1973 Parlamentsvorlage des ersten Entwurfs Bundesdatenschutzgesetzes (BDSG)

1978 Inkrafttreten des ersten BDSG; Erstes Niedersächsisches Datenschutzgesetz

1983 **Volkszählungsurteil des Bundesverfassungsgerichts:**

Das Recht auf informationelle Selbstbestimmung → Grundgesetz (GG), Artikel 2:

(1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

in Verbindung mit Artikel 1 (GG)

(1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt.

Datenschutz in der medizinischen Forschung

Geschichte der Datenschutzgesetze

- 1990/91** Zweite Fassung des BDSG
- 1993** Anpassung Niedersächsisches Datenschutzgesetz
- 1995** EG-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- 2001** Dritte Fassung des BDSG
- 2009** Novellierung der dritten Fassung
- 2016** **EU-Datenschutzgrundverordnung, Anwendung ab 25.5.2018**
- 2017** **BDSG-Neu, Anwendung ebenfalls ab 25.5.2018**

- 2018** **Neues Niedersächsisches Datenschutzgesetz**

Datenschutz in der medizinischen Forschung

Agenda:

1. Worum geht's?
2. Wer hat's erfunden? Eine kurze Geschichte der Datenschutzgesetze
3. Gesetzliche Regelungen (allgemein)
4. Gesetzliche Regelungen in der Forschung
5. Digitalisierung und Forschung

Datenschutz in der medizinischen Forschung

Rechtsgrundlagen

Zwei Grundrechte:

- 1. Recht auf informationelle Selbstbestimmung, abgeleitet aus Art 1 und 2 des GG**
- 2. Freiheit von Forschung und Lehre, Art 5(3) GG**



Personenbezogene Daten unterliegen nationalen Gesetzen UND – seit dem 25.5.2018 – auch europäischer Gesetzgebung

Datenschutz in der medizinischen Forschung

Rechtsgrundlagen

Relevante Gesetze:

- Bundesdatenschutzgesetz (BDSG)
- Landesdatenschutzgesetz (z.B. NDSG))
- Europäische Datenschutzgrundverordnung (EU-DSGVO)



Grundsatz: Die Verarbeitung von personenbezogenen Daten ist verboten! ... außer sie ist durch andere Gesetze, Verträge, Vereinbarungen erlaubt ODER durch die **Einwilligung der betroffenen Personen. („Verbot mit Erlaubnisvorbehalt“)**

Datenschutz in der medizinischen Forschung

Rechtsgrundlagen: EU-DSGVO – kurzgefasst (173 Erwägungsgründe und 99 Artikel in 11 Kapiteln)

Zielsetzung der DS-GVO ist ein **wirksamer Schutz personenbezogener Daten vor unbefugtem Zugriff**, wobei „der freie Verkehr personenbezogener Daten in der Europäischen Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden“ darf (Art. 1 Abs. 3 DS-GVO).

Definition: Was sind personenbezogene Daten?

DSGVO Art 4: Personenbezogene Daten sind **Einzelangaben** über persönliche oder sachliche Verhältnisse von bestimmten oder bestimmbaren natürlichen Personen*. **Einzelangaben** = Informationen über eine einzelne, natürliche Person;



* Für Daten ohne Personenbezug sind die Datenschutzgesetze nicht anwendbar!

Datenschutz in der medizinischen Forschung

Rechtsgrundlagen: Besondere Arten personenbezogener Daten (Art 9, DSGVO)

- rassische und ethnische Herkunft
- politische Meinungen
- religiöse und philosophische Überzeugung
- Gewerkschaftszugehörigkeit
- Gesundheit oder Sexualleben



**Verarbeitung erfordert Risikoanalyse –
Datenschutzfolgenabschätzung (Art. 35, DSGVO)!**

Datenschutz in der medizinischen Forschung

Rechtsgrundlagen: Schutzstufen*

- A frei zugängliche Daten
- B keine besondere Beeinträchtigung
- C Beeinträchtigung des Ansehens
- D Beeinträchtigung der Existenz
- E Gefährdung von Freiheit oder Leben

* Schutzstufenkonzept der Landesbeauftragten für den Datenschutz Niedersachsen

Datenschutz in der medizinischen Forschung

Schutzstufe	Personenbezogene Daten,	zum Beispiel	Schwere eines möglichen Schadens
A	die von den Betroffenen frei zugänglich gemacht wurden.	Telefonverzeichnis, Wahlvorschlagsverzeichnisse, eigene freizugänglich gemachte Webseite; frei zugängliche soziale Medien	geringfügig
B	deren unsachgemäße Handhabung zwar keine besondere Beeinträchtigung erwarten lässt, die aber von den Betroffenen nicht frei zugänglich gemacht wurden.	beschränkt zugängliche öffentliche Dateien, Verteiler für Unterlagen, Grundbucheinsicht; nicht frei zugängliche soziale Medien	
C	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen“).	Einkommen, Grundsteuer, Ordnungswidrigkeiten	überschaubar
D	deren unsachgemäße Handhabung den Betroffenen in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigen könnte („Existenz“).	Anstaltsunterbringung, Straffälligkeit, dienstliche Beurteilungen, Arbeitszeugnisse, Gesundheitsdaten, Schulden, Pfändungen, Sozialdaten, Daten besonderer Kategorien nach Art. 9 DS-GVO	substantiell
E	deren unsachgemäße Handhabung Gesundheit, Leben oder Freiheit des Betroffenen beeinträchtigen könnte.	Daten über Personen, die mögliche Opfer einer strafbaren Handlung sein können, Zeugenschutzprogramm	groß

Datenschutz in der medizinischen Forschung

Rechtsgrundlagen: Einwilligung

(Art. 7)

- Schriftform (seit 25.5.2018 nicht mehr zwingend!)
- Andere Form, wenn besondere Umstände vorliegen.
- Besonders hervorzuheben, wenn sie zusammen mit anderen Erklärungen erteilt wird.



Datenschutz in der medizinischen Forschung

Einwilligungen

UNIVERSITÄTSMEDIZIN
GÖTTINGEN UMG

Patientenidentität
oder Patienten-
nummer: _____
Name, Vorname: _____
Geburtsdatum: _____
Straße: _____
PLZ, Wohnort: _____

Falls Patient nicht mit Antragsteller identisch

Name, Vorname: _____
Geburtsdatum: _____
Straße: _____
PLZ, Wohnort: _____

Der aufzunehmende Patient ist

- ☐ meine Ehefrau / mein Ehemann
☐ mein Kind
☐ _____

Sehr geehrte Patientin,
sehr geehrter Patient,

die UMG ist aus Datenschutzgründen verpflichtet, folgende Einwilligungen, die im Zusammenhang mit Ihrer Behandlung von Bedeutung sein könnten, von Ihnen einzuholen.

Die von Ihnen erteilten Einwilligungen gelten sowohl für die ambulante, als auch für die stationäre Behandlung in allen Kliniken, Abteilungen und Instituten der UMG für einen Zeitraum von 90 Tagen. Bei möglichen weiteren Behandlungen nach Ablauf dieses Zeitraums werden wir Sie bitten, die Einwilligungen zu aktualisieren.

Davon abgesehen haben Sie jederzeit die Möglichkeit, Ihre Einwilligungen ohne Angabe von Gründen zu widerrufen. Die Widerrufserklärung richten Sie an den Krankenhausträger. Die entsprechenden Kontaktdaten finden Sie teilweise direkt im zugehörigen Passus oder auf unserer Homepage www.umg.eu.

Ihr Widerruf gilt allerdings erst ab dem Zeitpunkt, zu dem Sie diesen aussprechen. Er hat keine Rückwirkung. Die Verarbeitung Ihrer Daten und Restmaterialien bis zu diesem Zeitpunkt bleibt rechtmäßig.

Ihre Einwilligungen sind freiwillig.

Datenübermittlung zwischen dem Krankenhaus, Hausarzt und sonstigen Vor- / Weiterbehandlern

Einverständniserklärung gem. Art. 6 Abs. 1a, Art. 9 Abs. 2a, h, Abs. 3, Abs. 4 DS-GVO i. V. m. § 73 Abs. 1b SGB V - nur bzgl. gesetzlich krankenversicherter Patienten

Ich bin damit einverstanden, dass das Krankenhaus die mich betreffenden Behandlungsdaten und Befunde an meinen Vorbehandler und Weiterbehandler (ggf. sonstigen Behandler) zum Zwecke der Dokumentation und Weiterbehandlung übermittelt.

Des Weiteren bin ich damit einverstanden, dass das Krankenhaus die bei meinem Vorbehandler vorliegenden Behandlungsdaten und Befunde, soweit diese für meine Krankenhausbehandlung erforderlich sind, anfordern kann. Das Krankenhaus wird die Daten jeweils nur zu dem Zweck verarbeiten, zu dem sie übermittelt worden sind.

Fortsetzung auf der nächsten Seite

Universitätsmedizin Göttingen
Anschrift: Robert-Koch-Str. 40, 37075 Göttingen
Briefpost: 37099 Göttingen
Telefon: 0551/39-0; www.umg.eu

Stand: 10/2019

Art.-Nr.: XXXXXXXX

Seite 1 von 4

Einwilligungen

UNIVERSITÄTSMEDIZIN
GÖTTINGEN UMG

Jedes Forschungsvorhaben, welches diese Restmaterialien und Daten nutzen möchte, wird vorab von einer unabhängigen Ethikkommission bewertet. Außerdem wird sichergestellt, dass eine Weitergabe Ihrer Restmaterialien und Daten an Dritte nur so erfolgt, dass ein Rückschluss auf Ihre Person nicht möglich ist.

Sie können Ihre erteilte Einwilligung jederzeit ohne Angabe von Gründen gegenüber der UMG Biobank (Robert-Koch-Str. 40, 37075 Göttingen; biobank@med.uni-goettingen.de) widerrufen. In diesem Fall werden die in der UMG Biobank lagernden Restmaterialien vernichtet. Wird die Einwilligung widerrufen oder nicht erteilt, so hat dies keine Auswirkungen auf Ihre Behandlung in der UMG.

Ich willige ein, dass Restmaterialien und die dazugehörigen Daten in verschlüsselter Form für alle biomedizinischen Forschungszwecke genutzt werden dürfen. Restmaterialien und Daten dürfen an Dritte weitergegeben werden, sofern ein Rückschluss auf meine Person nicht möglich ist.

Ja ☐
Nein ☐

In die Nutzung von Patientendaten aus der Versorgung für medizinische Forschungszwecke und die Lehre in der Medizin

Im Zusammenhang mit Ihrer medizinischen Behandlung werden personenbezogene Daten erhoben. Hierbei handelt es sich um die Dokumentation von diagnostischen und therapeutischen Maßnahmen und Erkenntnissen.

Wir bitten Sie um Ihr Einverständnis, dass die vorgenannten Daten für alle Arten von Forschung und Lehre in der Medizin genutzt werden dürfen. Finanzielle oder sonstige Ansprüche erheben Sie in diesem Zusammenhang nicht.

Jedes Forschungsvorhaben wird vorab von einer unabhängigen Ethikkommission bewertet, wobei die Ethikkommission insbesondere auch die Belange der Patienten berücksichtigt. Ihre Daten werden ausschließlich nach einer positiven Bewertung der Ethikkommission zu Forschungszwecken genutzt.

Ihre erteilte Einwilligung können Sie jederzeit ohne Angabe von Gründen gegenüber der UMG (Robert-Koch-Str. 40, 37075 Göttingen) widerrufen. In diesem Fall würden Ihre Patientendaten ab Zugang des Widerrufs nicht weiter zu Forschungszwecken und zur Lehre in der Medizin verwandt. Wird die Einwilligung widerrufen oder nicht erteilt, so hat dies keine Auswirkungen auf Ihre Behandlung in der UMG.

Ich willige ein, dass krankheitsbezogene Daten aus der Versorgung für alle medizinischen Forschungszwecke und für die medizinische Lehre genutzt werden dürfen. Daten dürfen an externe Institutionen weitergegeben werden, sofern ein Rückschluss auf meine Person durch Dritte ausgeschlossen ist.

Ja ☐
Nein ☐

Medikamentenversorgung während der ambulanten Behandlung in der UMG

Für den Fall, dass während meiner ambulanten Behandlung in den Räumlichkeiten der UMG die Einnahme oder die Gabe von Medikamenten erforderlich ist, erkläre ich mit meiner Unterschrift, dass diese von der krankenhauseigenen Apotheke der UMG direkt zur Verfügung gestellt werden sollen.

Hinweis: dieses betrifft nur den unmittelbaren Arzneimittelbedarf während der Behandlung oder Untersuchung in unseren Krankenzimmern. Sämtliche Arzneimittel, die Ihnen zur persönlichen Einnahme zu Haus verordnet werden, erhalten Sie weiterhin in der niedergelassenen Apotheke Ihrer eigenen Wahl.

Befeierte Verordnungen rechnet die UMG selbst oder eine hiermit betraute Abrechnungsstelle zu den jeweils gesetzlich bestimmten Abrechnungspreisen gemäß geltender Arzneimittelpreisverordnung oder, im Falle mit Ihrer Versicherung vertraglich bestimmter Preise, zu den jeweils vereinbarten Beträgen ab. Versicherte der gesetzlichen Krankenkassen bitten wir zu beachten, dass Sie bei Abgabe verschriebener Medikamente durch Apotheken gem. § 61 SGB V zur Übernahme eines Eigenanteils verpflichtet sind. Falls Sie von dieser Zuzahlung befreit sind, ist es in diesem Zusammenhang von hoher Bedeutung, dass Sie uns dies vor der Behandlung anzeigen und im Rahmen der Aufnahme hierzu Ihren Befreiungsnachweis vorlegen. In allen anderen Fällen wird Ihnen die UMG selbst oder eine hiermit betraute Abrechnungsstelle die gesetzlich bestimmten Zuzahlungsbeträge in Rechnung stellen.

Fortsetzung auf der nächsten Seite

Universitätsmedizin Göttingen
Anschrift: Robert-Koch-Str. 40, 37075 Göttingen
Briefpost: 37099 Göttingen
Telefon: 0551/39-0; www.umg.eu

Stand: 10/2019

Art.-Nr.: XXXXXXXX

Seite 3 von 4

Datenschutz in der medizinischen Forschung

„Sieben goldene Regeln des Datenschutzes“

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit
5. Transparenz
6. Datensicherheit
7. Kontrolle



Jede Datenverarbeitung bedarf einer rechtlichen Grundlage in Form einer gesetzlichen Grundlage, eines Vertrages, einer betrieblichen Regelung oder der Einwilligung des Betroffenen.

Datenschutz in der medizinischen Forschung

„Sieben goldene Regeln des Datenschutzes“

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit
5. Transparenz
6. Datensicherheit
7. Kontrolle



Eine Einwilligung ist nur wirksam, wenn der Betroffene ausreichend informiert worden ist und seine Einwilligung freiwillig erteilt hat.

Datenschutz in der medizinischen Forschung

„Sieben goldene Regeln des Datenschutzes“

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit
5. Transparenz
6. Datensicherheit
7. Kontrolle



Personenbezogene Daten dürfen nur zu dem Zweck verwendet werden, zu dem sie erhoben worden sind.

Datenschutz in der medizinischen Forschung

„Sieben goldene Regeln des Datenschutzes“

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit
5. Transparenz
6. Datensicherheit
7. Kontrolle



Die Datenverarbeitung ist auf den für ihren Erhebungszweck notwendigen Umfang zu begrenzen.

Datenschutz in der medizinischen Forschung

„Sieben goldene Regeln des Datenschutzes“

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit
5. Transparenz
6. Datensicherheit
7. Kontrolle



Die Erhebung und Verarbeitung personenbezogener Daten muss gegenüber dem Betroffenen transparent sein.

Datenschutz in der medizinischen Forschung

„Sieben goldene Regeln des Datenschutzes“

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit
5. Transparenz
6. Datensicherheit
7. Kontrolle



Der Datenschutz ist nur gewährleistet, wenn die personenbezogenen Daten auch sicher verarbeitet werden. Ziele der IT-Sicherheit und damit auch der Datensicherheit sind die

- Vertraulichkeit
- Verfügbarkeit und
- Integrität

personenbezogener Daten.

Datenschutz in der medizinischen Forschung

„Sieben goldene Regeln des Datenschutzes“

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit
5. Transparenz
6. Datensicherheit
7. Kontrolle



Die Datenverarbeitung unterliegt einer internen und externen Kontrolle.

Datenschutz in der medizinischen Forschung

Agenda:

1. Worum geht's?
2. Wer hat's erfunden? Eine kurze Geschichte der Datenschutzgesetze
3. Gesetzliche Regelungen (allgemein)
4. Gesetzliche Regelungen in der Forschung
5. Digitalisierung und Forschung

Datenschutz in der medizinischen Forschung

Rechtsgrundlagen: Für Forschungsprojekte gibt es besondere Regelungen

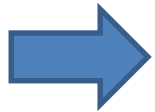
DSGVO: Artikel 89 Garantien und Ausnahmen in Bezug auf die Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

Niedersächsisches Datenschutzgesetz (NDSG): § 13 Verarbeitung personenbezogener Daten für Forschungsvorhaben

BDSG neu: § 27 – Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken

Datenschutz in der medizinischen Forschung

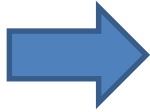
Rechtsgrundlage 1: Art. 89 DSGVO



- Verarbeitung erfordert geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen.
- Garantien heißt: technische und organisatorische Maßnahmen stellen die Einhaltung der Grundsätze des Datenschutzes sicher
 - Erforderlichkeit (Datenminimierung)
 - Vertraulichkeit
 - Integrität etc.
 - ...
- Eine Maßnahme kann Pseudonymisierung sein wenn Forschungszweck dies erlaubt.
- Bei Forschung zu Archivzwecken: Betroffenenrechte nach Art. 15, 16,18, 19,20,21 können eingeschränkt/ verweigert werden.

Datenschutz in der medizinischen Forschung

Rechtsgrundlage 2: § 13 NDSG



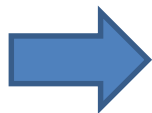
- Regelung der Verarbeitung durch **öffentliche niedersächsische Stellen**
- Forschung: = "ernsthafter, planmäßiger Versuch zur Ermittlung der Wahrheit" mit weiter Auslegung (vgl. EwG 159 DS-GVO).
- **Forschungsprivileg** gilt auch bei **Dissertations-** und **Habilitations-vorhaben** (nicht aber Seminararbeiten oder Untersuchungen zu Aufsichts-, Organisations- und Kontrollzwecken)
- **Notwendig:** Abwägung der schutzwürdigen Interessen der Betroffenen gegen das öffentliche Interesse; Überwiegen erstere->Einwilligung erforderlich! Dokumentation! Information des DSB!
Zulässig: Weiterverarbeitung von ursprünglich zu anderen Zwecken legitim erhobenen Daten für wissenschaftliche Forschungszwecke (sog. Eigenforschung).
- **Bei Forschung mit Gesundheitsdaten** unbedingt beachten: Regelungen zum Patientengeheimnis (ärztliche Schweigepflicht) beachten; siehe Berufsordnungen der Kammern, § 203 StGB; **regelmäßig Einwilligungen der Patient*innen erforderlich!**

Datenschutz in der medizinischen Forschung

Rechtsgrundlage 3: § 27 BDSG

- Regelungen gleichen Inhalts wie in §13, NDSG
- Explizit: Einwilligungen sind auch bei besonderen Kategorien personenbezogener Daten nicht erforderlich, wenn das öffentliche Interesse das persönliche der Betroffenen überwiegt.

Aber auch hier gelten bei Gesundheitsdaten weitere Regelungen wie Berufsordnung der Ärzte und die (strafrechtlich relevante!) Schweigepflicht

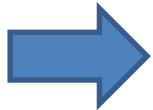


Einwilligungen meist erforderlich

Datenschutz in der medizinischen Forschung

Rechtsgrundlagen: Ethikantrag, Probandeninfo, Einwilligung

Forschungsprojekte am Menschen, insbesondere medizinische müssen aus ethischer Perspektive begutachtet werden!



Ethikkommission

Geschäftsstelle

Ethikkommission der Universitätsmedizin Göttingen
Von-Siebold-Str.3
37075 Göttingen

- Datenschutzrelevante Angaben
- Information für Studienteilnehmer*innen
- Einwilligungserklärung

Datenschutz in der medizinischen Forschung

Rechtsgrundlagen: Ethikantrag, Probandeninfo, Einwilligung

.....

3. Probandenrekrutierung

Die Studierenden werden im Rahmen eines elektronischen Seminars durch die Antragsteller auf die Möglichkeit zur Studienteilnahme aufmerksam gemacht. Neben den Studienzielen wird dabei auf die genutzten Datenquellen und insbesondere Aspekte des Datenschutzes eingegangen. Die Studierenden werden darüber informiert, dass Sie den Antragstellern durch Unterzeichnen der Einverständniserklärung die Genehmigung erteilen, ihre persönlichen Daten in anonymisierter Form auszuwerten. Es wird ausdrücklich auf die Freiwilligkeit der Teilnahme und die Möglichkeit zum Widerruf der Einwilligung ohne Angaben von Gründen hingewiesen. Parallel wird die diesem Antrag beigefügte Probandeninformation ausgegeben. In einem weiteren Termin findet die Datenerhebung statt; hier können die Studierenden durch Unterschrift auf dem beigefügten Formular auf freiwilliger Basis einer Nutzung ihrer Daten zustimmen.

Datenschutz in der medizinischen Forschung

Rechtsgrundlagen: Ethikantrag, Probandeninfo, Einwilligung

.....

4. Archivierung und Datenschutz

Die personenbezogenen Daten werden auf einem passwortgeschützten Rechner mit Standort im UBFT gespeichert, zu dem nur der Projektleiter Zugang hat. Im Rahmen des elektronischen Seminars melden die Studierenden sich sowohl bei der Simulation als auch bei EvaSys mit ihrer Matrikelnummer an. Auf diese Weise sind alle eingegebenen Daten zunächst mit personenbezogenen Daten verknüpft. Dies ist notwendig, um einen Abgleich mit den schriftlichen Einverständniserklärungen durchführen zu können.

Daten von Studierenden, die einer Nutzung der Daten zu wissenschaftlichen Zwecken nicht zugestimmt haben, werden gelöscht. Zur Auswertung werden die Logfiles und die Übergabe-Protokolle individueller Studierender zusammengeführt. Danach werden die Matrikelnummern gelöscht. Im geschlossenen Datensatz ist dann nicht mehr ersichtlich, welche Daten zu welchem individuellen Studierenden gehören. Die Studierenden werden im Informationsbogen und in der Projektvorstellung über dieses Vorgehen informiert.

Datenschutz in der medizinischen Forschung

Rechtsgrundlagen: Ethikantrag, Probandeninfo, Einwilligung

Probanden/innen-Information zur Studie

„Entwicklung von klinischem Denken bei Medizinstudierenden im Laufe des klinischen Studienabschnittes“ (Amendment)

Sehr geehrte Studierende,
im Wintersemester 2018/19 nehmen Sie am Modul 6.x teil. In diesem Rahmen absolvieren Sie Unterrichtseinheiten.....

Im Rahmen der hier vorgestellten Studie wollen wir folgende Studienfragen beantworten:.....

Datenerhebung und Datenschutz

.....

Datenschutz in der medizinischen Forschung

Rechtsgrundlagen: Ethikantrag, Probandeninfo, Einwilligung

Einverständniserklärung für Probanden/innen zur Studie

„Entwicklung von klinischem Denken bei Medizinstudierenden im Laufe des klinischen Studienabschnittes“ (Amendment)

Ich wurde vom Studienleiter vollständig über Wesen, Bedeutung und Tragweite der Studie

aufgeklärt. Ich hatte die Möglichkeit, Fragen zu stellen, habe falls erforderlich Antworten erhalten und diese verstanden.

Ich erkläre mich damit einverstanden, dass im Rahmen dieser Studie erhobene Daten, insbesondere mein Matrikelnummer und aufgezeichnet werden. Vor der Datenanalyse werden personenbezogene Daten gelöscht. Eine Rückverfolgung zu meiner Person ist anhand dieser Daten nicht möglich. Mir ist bekannt, dass ich meine Einwilligung in die Studienteilnahme jederzeit widerrufen kann.

JA

NEIN

Unterschrift

Datenschutz in der medizinischen Forschung

Informationen, Formulare

Information und Hilfe bietet das Studienzentrum der UMG!

[TMF-Arbeitsgruppen zum Datenschutz in Forschungsprojekten](http://www.tmf-ev.de/Arbeitsgruppen_Foren/AGDS.aspx)

http://www.tmf-ev.de/Arbeitsgruppen_Foren/AGDS.aspx

Datenschutz in der medizinischen Forschung

Informationen, Formulare

Vertraulichkeitserklärung

UNIVERSITÄTSMEDIZIN
GÖTTINGEN **UMG**
Verpflichtungserklärung zur Wahrung der Vertraulichkeit nach Artikel 5 DSGVO
in Verbindung mit Artikel 24, 29 und 32 DSGVO

Herrn/Frau

beschäftigt bei:

Ich verpflichte mich, personenbezogene Daten vertraulich zu behandeln, sofern ich Kenntnis von personenbezogenen Daten von Patientinnen und Patienten der Universitätsmedizin Göttingen während meiner Tätigkeit als

.....erlange.

Mir ist bekannt, dass es untersagt ist, geschützte personenbezogene Daten unbefugt zu einem anderen als zu dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekannt zugeben, zugänglich zu machen oder auf sonstige Weise zu nutzen. Diese Verpflichtung besteht auch nach Beendigung der Tätigkeit in der Universitätsmedizin Göttingen fort.

Ich bin darauf hingewiesen worden, dass andere in Gesetzen und Verordnungen enthaltene Geheimhaltungsverpflichtungen, wie z.B. die ärztliche Schweigepflicht (§ 203 StGB) zu beachten sind.

Mir ist weiterhin bekannt, dass Verstöße gegen die Verpflichtung zur Wahrung des Datengeheimnisses mit Geld- oder Freiheitsstrafe geahndet werden können.

Eine Ausfertigung dieser Verpflichtung wurde mir übergeben.

Göttingen, den
Datum, Unterschrift der/des Verpflichteten

Bestätigung durch die verpflichtende Abteilung/Organisationseinheit der UMG

Dem/der Verpflichteten wurde eine Durchschrift der Verpflichtung ausgehändigt.

Göttingen, den
Datum, Unterschrift der Mitarbeiterin/des Mitarbeiters der UMG

Datenschutz in der medizinischen Forschung

Informationen, Formulare Datenzugriffsvereinbarung

UNIVERSITÄTSMEDIZIN GÖTTINGEN UMG

Datenschutzbeauftragter der UMG
Tel.: 0551 39 27780
E-Mail: datenschutz@med.uni-goettingen.de

Datenzugriffsvereinbarung/2017

Bitte ausgefüllt (Seite 1-2) an den Datenschutzbeauftragten senden. Falls keine Rückfragen sind, erhält der Antragsteller Seite 1 zurück und kann damit im Zentralarchiv die benötigten Patientenakten anfordern bzw. bei elektronischem Zugriff einen ixserv-Account im G3-7 Informationstechnologie (Sachgebiet Klinische Systeme) beantragen.

An den
Datenschutzbeauftragten der Universitätsmedizin Göttingen
Telefax: 142

Per Fax: 39 - 12726 Als gescanntes Dokument (PDF) an: datenschutz@med.uni-goettingen.de

1. Persönliche Daten des/der Antragstellenden

Name	
Privatanschrift	
Telefon/E-Mail	
Abteilung/Klinik	

2. Thema des Forschungsvorhabens:

--

3. Zweck: ☐ Promotion ☐ Habilitation ☐ Sonstiges Forschungsvorhaben

4. Folgende Patientendaten werden benötigt (z.B. Patienten der Klinik...Zeitraum...Diagnose ...):

--

→ weiter mit Nr.5

Unterschrift des Datenschutzbeauftragten

Stand 02/2016

Unterschrift der Archivleitung bzw. der Leitung der speichernden Stelle

1

5. Der Antragsteller bestätigt die Kenntnisnahme der Hinweise des Datenschutzbeauftragten:
Datenschutzmaßnahmen bei Forschungsvorhaben und in klinischen Prüfungen¹

Datum, Unterschrift des/der Antragstellenden

6. Erklärung zur ärztlichen Schweigepflicht

☐ Ich habe bei meiner Immatrikulation eine „Erklärung über die ärztliche Schweigepflicht“ unterschrieben.

Datum, Unterschrift des/der Antragstellenden

Falls eine Erklärung nicht unterschrieben wurde, ist diese (Schweigepflicht für Studierende¹) dem Antrag beizufügen.

Datum, Unterschrift des Betreuenden

Stempel/Unterschrift der zustimmenden Abteilungsleitung

Stempel/Unterschrift der zustimmenden Abteilungsleitung
(Bei Antragstellern, die für das Projekt auch Daten aus einer anderen Abteilung benötigen.)

¹ <http://www.rostra.med.uni-goettingen.de> (freier Zugang Datenschutz) oder beim Datenschutzbeauftragten anfordern.
Stand 02/2016

2

Datenschutz in der medizinischen Forschung

„Schrems II“

Datenaustausch mit den USA: Mit dem EuGH-Urteil vom 16.7.2020 ist der EU-US-Privacy-Shield ungültig! Damit ist seit dem Datum ohne jede Übergangsfrist die Übermittlung personenbezogener Daten in die USA illegal und prinzipiell Bußgeldbewährt!

Weiterhin möglich ist der Transfer, wenn sogenannte Standardvertragsklauseln (SVK) in den Kooperations- oder Auftragsverarbeitungsverträgen abgeschlossen worden sind. Da diese aber nicht davon entbinden, sich von der Gleichwertigkeit des Datenschutzniveaus mit dem der EU zu überzeugen, bieten SVK wegen der US-Rechtslage (Patriot Act; Cloud Act) keine wirkliche Lösung.

Die EU-Kommission ist am Zug!

Juristische Bewertung siehe Anlage

Datenschutz in der medizinischen Forschung

Agenda:

1. Worum geht's?
2. Wer hat's erfunden? Eine kurze Geschichte der Datenschutzgesetze
3. Gesetzliche Regelungen (allgemein)
4. Gesetzliche Regelungen in der Forschung
5. Digitalisierung und Forschung

Datenschutz in der medizinischen Forschung

Digitalisierung und Forschung: Neue Strukturen



MII-Initiative: Nutzbarmachung von Versorgungsdaten für die Forschung; BMBF finanziert mit 300 Mio. € in 2018-2026



Teilnahme aller Uni-Klinika; 4 Konsortien (DIFUTURE, MIRACUM, SMITH, **HIGHMED**):

Datenschutz in der medizinischen Forschung

Digitalisierung und Forschung: Neue Strukturen

Aufgaben:

- Datenschutzkonzept, Nutzungskonzept,
- Broad Consent
- Aufbau von Datenintegrationszentren



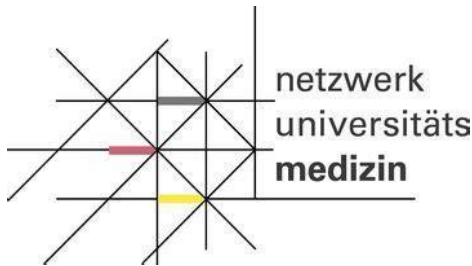
UMG-Medic, Use&Access Committee

Use Cases Highmed: Onkologie, Kardiologie, Infection Control

Konsortienübergreifende Projekte: CODEX, CORD-MI

Datenschutz in der medizinischen Forschung

Digitalisierung und Forschung: Neue Strukturen



Das Netzwerk Universitätsmedizin hat zum Ziel, Daten, Erkenntnisse, Maßnahmenpläne, Diagnostik- und Behandlungsstrategien aller deutschen Universitätskliniken und ggf. weiterer Akteure im Sinne einer Pandemic Preparedness zusammenzuführen und auszuwerten.

NUM Projekte:

- CODEX: Covid 19 Datenplattform
- NAPKON: Nat. Pandemie Kohorten Netz
- RACOON: Rad. Coop. Netzwerk zur Covid Pandemie
- AKTIN-EZV: Notfallversorgungsforschung
-

Datenschutz in der medizinischen Forschung

Digitalisierung und Forschung: Neue Strukturen

Elektronische Patientenakte (ePA)

Dokumente der elektronischen Patientenakte

Kategorien nach § 341 Abs. 2 SGB V:

- Nr. 1a: Daten zu Befunden, Diagnosen, durchgeführten und geplanten Therapiemaßnahmen, Früherkennungsuntersuchungen, Behandlungsberichten und sonstige untersuchungs- und behandlungsbezogene medizinische Informationen
- Nr. 1b: elektronischer Medikationsplan
- Nr. 1c: elektronische Notfalldaten
- Nr. 1d: elektronische Arztbriefe
- ...
- Nr. 5: elektronische Impfdokumentation
- Nr. 6: Gesundheitsdaten, die durch den Versicherten zur Verfügung gestellt werden
-

Freigabe zu Forschungszwecken

Ab 1.1.2023 können Versicherte ihre Daten nach § 363 SGB V zur Verfügung stellen!

Datenschutz in der medizinischen Forschung



Internet 4.0

Datenschutz in der medizinischen Forschung

Dr. Thomas Langbein, Andrea Abel

Büro: Waldweg 35, 37073 Göttingen

Anschrift: UMG, Robert-Koch-Str. 40, 37075 Göttingen

Briefpostadresse: 37099 Göttingen

Tel.: 39-62762

E-Mail: datenschutz@med.uni-goettingen.de

Das war's!
Vielen Dank für die Aufmerksamkeit!

Rechtliche Einschätzung: Einordnung des Schrems-II-Urteil (Privacy Shield) und Handlungsvorschläge

Projekt Rechtsinformationsstelle Digitale Hochschule NRW

Leitung Prof. Hoeren, Uni Münster

22. September 2020

Wissenschaftlicher Mitarbeiter Julian Albrecht

A. Fragestellung

- I. Welche Bedeutung hat das Schrems-II-Urteil¹?
- II. Auf welchen Rechtsgrundlagen können Datentransfers in Drittländer wie z.B. die USA noch gestützt werden?
- III. Welche praktischen Handlungsmöglichkeiten bestehen für die Hochschulen in NRW?

Inhalt

A.	Fragestellung	1
B.	Ergebnis	1
C.	Ausführliche Untersuchung	2
I.	Inhalt und Bedeutung des „Schrems-II-Urteils“	2
II.	Alternative Rechtsgrundlagen für den Datentransfer in Drittländer insb. die USA	5
III.	Praktische Handlungsvorschläge für Hochschulen in NRW	7
D.	Auswahl hilfreicher weiterführender Quellen	11

B. Ergebnis

Mit Urteil vom 16.07.2020 hat der EuGH eine wichtige Rechtsgrundlage zur Übertragung von Daten in die USA für ungültig erklärt. An eine weitere entsprechende Rechtsgrundlage werden neue Anforderungen gestellt.

Dies ist von großer Bedeutung für Hochschulen, weil viele von ihnen US-amerikanische Cloud-Dienste wie z.B. Microsoft Teams oder Zoom nutzen. Diese übertragen Daten in die USA.

Für Hochschulen ist daher Handlungsbedarf entstanden und dies in größerem Umfang und Dringlichkeit als es zunächst schien und in einer Kurzmitteilung der RiDHnrw am Tag des Urteils am 16.07.20 kommuniziert wurde. Dies liegt daran, dass eine wichtige Rechtsgrundlage zur Übertragung der Daten in Drittstaaten zwar ausdrücklich als weiterhin für zulässig befunden wurde. Dies aber nur unter dem

¹ Rechtssache C-311/18, abrufbar unter <http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1>.

Vorbehalt einer Prüfung im Einzelfall, welche im Ergebnis – v.a. bei Übertragungen in die USA – regelmäßig den Bedarf der Einführung zusätzlicher Maßnahmen verlangen wird.

Zwar drohen den Hochschulen als öffentliche Stellen anders als privaten Unternehmen keine Geldbußen bei Verstößen gegen die DSGVO. Selbstverständlich sind sie jedoch dazu angehalten, geltendes Recht zu beachten. Bei Passivität droht eine Untersagung der Nutzung bestimmter Dienste durch die Aufsichtsbehörde.

Zusammengefasst schlagen wir folgendes Vorgehen vor (genauer unter C.III.):

1. Erstellung einer Übersicht von allen Drittstaatentransfers inklusive genutzter Rechtsgrundlage, Kategorie und Risiko der übertragenen Daten
2. Sofortiges Umstellen aller Verträge auf Standardvertragsklauseln
3. Schriftlich dokumentierte Begründung einer Unzumutbarkeit von Alternativen ohne Drittstaaten-Problematik in bestimmten Fällen
4. Anschreiben der Unternehmen unter Verwendung einer Vorlage
5. Einordnung der Antworten; ggfs. Einschalten der Aufsichtsbehörde (in NRW für die Hochschulen: Landesbeauftragte für Datenschutz und Informationsfreiheit NRW (LDI NRW))
6. Abwarten der allgemeinen Handlungsempfehlungen der LDI NRW und insb. des Europäischen Datenschutzausschusses
7. Weitere Schritte einleiten (Nachverhandlungen, teilweise Kündigung von Verträgen, organisatorische Maßnahmen)
8. Bei zukünftigen Anschaffungsentscheidungen ist auf bestimmte Faktoren verstärkt Acht zu geben

C. Ausführliche Untersuchung

I. Inhalt und Bedeutung des „Schrems-II-Urteils“

Der Transfer personenbezogener Daten in andere Staaten als die EU-Mitgliedsstaaten muss nach der europäischen Datenschutzgrundverordnung (DSGVO) aufgrund gesonderter Rechtsgrundlagen durchgeführt werden. Denn mit dem Transfer gehen besondere Gefahren einher. Die Rechtsgrundlagen sollen eine hinreichende Gewähr dafür bieten, dass auch bei einer Verarbeitung in dem Drittland ein dem europäischen Datenschutzrecht vergleichbares Schutzniveau besteht – oder in eng begrenzten Ausnahmefällen der Betroffene in Kenntnis des geringeren Schutzniveaus dennoch dem Transfer zustimmt. Eine der möglichen Rechtsgrundlagen sind sog. Angemessenheitsbeschlüsse gem. Art. 45 DSGVO. Mit einem solchen kann die europäische Kommission das Schutzniveau jeweils für ein Land als gleichwertig im Vergleich zur EU erklären.

Gegenstand des Urteils des Europäischen Gerichtshofs (EuGH) war nun der Angemessenheitsbeschluss der Kommission, der die USA betraf – der Beschluss trägt den Namen EU-Privacy-Shield. Dieser wurde

in dem hier besprochenen, viel beachteten Urteil vom 16. Juli 2020 für ungültig befunden.² Das Urteil wird in Fachkreisen als „Schrems-II-Urteil“ bezeichnet. Max Schrems heißt der Beschwerdeführer in dem Verfahren. Er hatte bereits 2015 erfolgreich ein Verfahren zum EuGH geführt, in dem der damalige Angemessenheitsbeschluss („Safe Harbour“) für ungültig befunden wurde – daher Schrems II. Die Begründung liegt in den Zugriffsrechten für amerikanische Geheimdienste wie die NSA, die der amerikanische Rechtsrahmen vorsieht (Rn. 150 ff.). Diese seien sehr weit gefasst und vor allem ohne Rechtsschutzmöglichkeit des betroffenen europäischen Bürgers ausgestaltet. An keiner Stelle würden ihm subjektive Rechte eingeräumt, die er vor amerikanischen Gerichten einklagen könnte. Auch der im Privacy-Shield vorgesehene Ombudsmechanismus biete insoweit keinen Ersatz, denn der Ombudsmann sei dem Außenministerium unterstellt, daher nicht hinreichend unabhängig, und könne den Geheimdiensten im Übrigen keine verbindlichen Anweisungen erteilen und so einem Rechtsverstoß sicher abhelfen.

Das Urteil bedeutet zunächst, dass Datentransfers in die USA nun nicht mehr auf dieser einen Rechtsgrundlage (Privacy Shield) geschehen dürfen. Entsprechende Hinweise auf das Privacy Shield sind aus den Datenschutzerklärungen von Verantwortlichen zu entfernen. Hinweise auf das Privacy Shield in Werbetexten amerikanischer Cloud-Diensteanbieter können als gegenstandslos betrachtet werden.

Das Urteil legt indes auch die Messlatte für alternative Rechtsgrundlagen für den Transfer deutlich höher. In der Praxis wurden auch vor dem Urteil häufig zusätzliche alternative Rechtsgrundlagen für den Transfer genutzt, meist durch die Vereinbarung sogenannter Standardvertragsklauseln gem. Art. 46 DSGVO. Standardvertragsklauseln (abgekürzt SVK; im Gesetz „Standarddatenschutzklauseln“, in Englisch: „Standard Contractual Clauses“ oder abgekürzt „SCC“) ist ein von der Kommission ausgearbeiteter Vertragstext („Klauseln“), der angemessene Schutzgarantien für die Übermittlung von Daten in Drittländer bieten soll und ist als alternative Rechtsgrundlage des Datentransfers im Grundsatz anerkannt. Beispielsweise Microsoft und Zoom haben bisher neben dem Privacy Shield auch SVK als Rechtsgrundlage für den Transfer vorgesehen, indem sie standardmäßig die entsprechenden Klauseln unterzeichnet haben.

Der EuGH betont in dem Urteil nun, was aus seiner Sicht schon vorher galt: **Die Vereinbarung von den SVK entbindet die Verantwortlichen nicht von ihrer Verantwortung, im Einzelfall zu prüfen, ob die Garantien der SVK alleine ein hinreichendes Schutzniveau garantieren können (Rn. 142).** Falls dies negativ zu beantworten ist, müsse der Verantwortliche „zusätzliche Maßnahmen“ ergreifen, um ein angemessenes Schutzniveau zu erreichen (Rn. 133 ff.).

Aus den Feststellungen zu den Zugriffsrechten von Geheimdiensten kann gefolgert werden, dass im Falle der Übertragung in die USA die SVK allein jedenfalls nicht ausreichen. **In der Praxis muss es daher zu einer rechtlichen Neubewertung aller Datenübertragungen kommen. Kaum ein Verantwortlicher, der Daten in die USA überträgt, dürfte die Anforderungen der DSGVO, wie sie auf diese Weise von**

² Rechtssache C-311/18, Randnummer (Rn.) 199, abrufbar unter <http://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=DE&mode=req&dir=&occ=first&part=1>.

dem Urteil konkretisiert werden, daher erfüllen, weil sie bisher noch keine hinreichenden „zusätzlichen Maßnahmen“ getroffen haben. Und da amerikanische Software- und Cloud-Diensteanbieter in Europa eine so wichtige Rolle spielen (Microsoft, Apple, Google, Amazon, Zoom, Slack u.a.), kommt dem Urteil eine erhebliche Bedeutung zu. Die Betriebsabläufe ganzer Unternehmen und auch öffentlicher Einrichtungen sind gefährdet, wenn die genannten Dienste nicht weiter genutzt werden können.

Ist ein Datentransfer noch möglich? Was bedeutet „deutlich höhere Messlatte“ und „zusätzliche Maßnahmen“? Einig ist sich die Mehrheit der Datenschutzrechtler (auch aus der Praxis) darüber, dass ein bloßes „Weiter so“ ohne Anpassungen nicht möglich ist. Viel Ungewissheit und Unklarheit besteht aber darüber, wie genau und wie erheblich die Anpassungen aussehen müssen. Somit ist auch unklar, wie realistisch es ist, hinreichende Anpassungen in absehbarer Zeit mit den großen amerikanischen Softwareherstellern zu verhandeln. Das Urteil hat insofern Rechtsunsicherheit gebracht. Knackpunkt ist, dass es die wichtigste alternative Rechtsgrundlage für den Transfer, die Standardvertragsklauseln, zwar für weiterhin zulässig erachtet, allerdings nur unter dem Vorbehalt, dass Verantwortlicher und Datenempfänger gemeinsam prüfen müssen, „ob im betreffenden Drittland das unionsrechtlich geforderte Schutzniveau eingehalten wird“ (Rn. 142) und falls dies die SVK alleine nicht gewährleisten können, zusätzliche Maßnahmen vorzusehen. Konkretisierungen oder Beispiele für zusätzlichen Maßnahmen werden nicht gegeben. Auch die Aufsichtsbehörden werden bisher größtenteils nicht konkreter. Der Europäische Datenschutzausschuss kündigt an, dass er daran arbeite „further guidance“ bereitzustellen hinsichtlich der Frage, welche „zusätzliche Maßnahmen“ in Betracht kommen.³

Ähnlich hat sich die für die Hochschulen in NRW zuständige Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI NRW) geäußert: „Die deutschen und die europäischen Aufsichtsbehörden arbeiten zusammen, um das Urteil des EuGH einheitlich zu verstehen und umzusetzen. Sie arbeiten auch an Empfehlungen für die Rechtsanwender.“⁴ Eine Ausnahme stellt der LfDI BaWü dar, der eine hilfreiche Orientierungshilfe veröffentlicht hat und darin auch konkrete Vorschläge zu „zusätzlichen Maßnahmen“ macht.⁵

Im nächsten Abschnitt C.II. haben wir zusammengetragen, (1) welche alternativen Rechtsgrundlagen für den Datentransfer in Drittländer neben dem Privacy-Shield in Betracht kommen, (2) welche „zusätzlichen Maßnahmen“ im Rahmen der prominentesten Alternative (Standardvertragsklauseln) in der Praxis und Literatur als Vorschläge diskutiert werden, und (3) wie man Drittlandtransfers in Zukunft ganz vermeiden könnte, sodass keine gesonderte Rechtsgrundlage nötig ist.

Im abschließenden Abschnitt C.III. machen wir konkrete Vorschläge, wie sich Hochschulen in NRW in der aktuellen Situation verhalten könnten.

³ S. 5 einer Stellungnahme, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/frequently-asked-questions-judgment-court-justice-european-union_en.

⁴ <https://www.lidi.nrw.de/mainmenu/Aktuelles/Inhalt/Schrems-II/Schrems-II.html>.

⁵ Abrufbar unter <https://www.baden-wuerttemberg.datenschutz.de/orientierungshilfe-des-lfdi-bw-was-jetzt-in-sachen-internationaler-datentransfer/>.

Zur Quellenlage: Auch zwei Monate nach dem Urteil ist angesichts seiner Relevanz erstaunlich wenig Fachliteratur zu dem Thema erschienen. Das ist ein Indikator dafür, wie unklar die Rechtslage aktuell ist. Die folgenden Tabellen und anschließenden Empfehlungen basieren auf den vier bisher erschienenen Fachartikeln (*Botta*, CR 2020, 505-513; *Voigt*, CR 2020, 513-522; *Lejeune*, CR 2020, 522-529; EuGH m. Anm. *Hoeren*, MMR 2020, 597, 608 f.; *Grasmück/Kollmar*, IPRB 2020, 212-216), einigen Blogbeiträgen und im Übrigen auf eigener Auswertung des Urteils, allgemeiner Literatur sowie fachlichem Austausch mit Kolleginnen und Kollegen.

II. Alternative Rechtsgrundlagen für den Datentransfer in Drittländer insb. die USA

Alternative Rechtsgrundlagen			
Norm	Beschreibung	Hinweise	Bewertung aus Hochschulsicht
Art. 45 DSGVO	Neuer Angemessenheitsbeschluss der EU-Kommission für den Datentransfer in die USA	Eine Liste mit erlassenen und gültigen Angemessenheitsbeschlüssen (Japan, Schweiz u.a.) finden Sie hier ⁶	Zeitaufwändiger, politischer Prozess – damit ist in den nächsten Monaten nicht zu rechnen.
Art. 46 Abs. 2 lit. c DSGVO	Einbeziehung der sog. Standardvertragsklauseln (in Art. 46 Abs. 2 lit. c DSGVO genannt), „Standarddatenschutzklauseln“ + Prüfung des Schutzniveaus im Einzelfall + Vereinbarung <u>zusätzlicher Maßnahmen</u> ⁷	Welche zusätzlichen Maßnahmen in Betracht kommen, ist unklar; siehe zum Diskussionsstand die nächste Tabelle	Aufwändig und von ungewissem Erfolg, aber unseres Erachtens die beste Option.
Art. 49 Abs. 1 UAbs. 1 lit. a DSGVO	Einwilligung zum Transfer in Kenntnis des nicht gleichwertigen Schutzniveaus	Richtigerweise bezieht sich die Beschränkung aus Erwägungsgrund 111 („gelegentlich“, „nicht wiederholt“) nicht auf die Möglichkeit zur Einwilligung. Vielfach wird dennoch der Ausnahmecharakter der Norm betont. ⁸ Davon diesen Erlaubnistatbestand zur Grundlage planmäßiger, wiederholter Datenübertragungen zu machen, ist bereits aus diesem Grund abzuraten. Jedenfalls ist dieser Erlaubnistatbestand nach Art. 49 Abs. 3 DSGVO aber auch für „Tätigkeiten, die Behörden in Ausübung ihrer hoheitlichen Befugnisse durchführen“ gesperrt. Damit entfallen große Handlungsfelder von Hochschulen und somit auch von Einsatzmöglichkeiten von Software.	Wegen der Einschränkung aus Abs. 3 für weite Tätigkeitsbereiche von Hochschulen nicht einsetzbar.

⁶ https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de

⁷ Näher in der nächsten Tabelle.

⁸ Leitlinien 2/2018 des Europäischen Datenschutzausschuss, S. 5, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_de; a.A. BeckOK DatenschutzR/Lange/Filip, 33. Ed. 1.8.2020, DS-GVO Art. 49 Rn. 11.

		In dann verbleibenden Anwendungsfällen sind die hohen Anforderungen an eine wirksame Einwilligung nach Art. 49 Abs. 1 UAbs. 1 lit. a DSGVO hervorzuheben. Wie bei der normalen Einwilligung muss echte Freiwilligkeit vorliegen. An die Informiertheit bestehen mit Blick auf die besonderen Risiken des Transfers aber besonders hohe Aufklärungsanforderungen ⁹ , konkret müsste etwa über die Zugriffsrechte amerikanischer Geheimdienste und über fehlende Rechtsschutzmöglichkeiten aufgeklärt werden.	
Art. 49 Abs. 1 UAbs. 1 lit. b-g, UAbs. 2	Andere Ausnahmetatbestände für den Transfer für bestimmte Fälle	Absolute Ausnahmebestimmungen; nicht vorgesehen für den wiederholten, systematischen Transfer aller Daten, sondern nur für nicht wiederholte Transfers, die nur begrenzte Anzahl an Personen betreffen (Erwägungsgrund 111 DSGVO).	Passt nicht auf Situation des wiederholten, allgemeinen Transfers wie z.B. bei der Nutzung von Videokonferenzdiensten.

Tabelle 1: Alternative Rechtsgrundlagen für Drittlandtransfers

Vorschläge „zusätzlicher Maßnahmen“ für den Transfer auf Grundlage von Standardvertragsklauseln (siehe Tabelle oben, vierte Zeile)			
Art der Maßnahmen	Vorschläge aus der Praxis und Literatur	Bewertung der Erfolgsaussichten, den Anforderungen von Schrems-II gerecht zu werden	Probleme der Umsetzung
Technischer Art	➤ Ende-zu-Ende-Verschlüsselung aller Daten (auch Metadaten), bei der nur der Datenexporteur (DE) den Schlüssel hat und die auch von US-Diensten nicht gebrochen werden kann ➤ Echte Anonymisierung von Daten	Sehr gut	Technisch aufwändig; liegt nicht allein in der Hand der Verantwortlichen – er wird regelmäßig wesentlich auf den Auftragsverarbeiter angewiesen sein
Vertraglicher Art = Vereinbarung zusätzlicher Rechte und Pflichten	➤ Pflicht des Datenimporteurs (DI), betroffene Person bei jeder Datenübertragung zu informieren ➤ Pflicht des DI, nicht nur den DE, sondern auch die betroffene Person, bei rechtlich bindender Aufforderung einer Vollstreckungsbehörde zur Weitergabe personenbezogener Daten, unverzüglich zu informieren ➤ Pflicht des DI, sich gerichtlich gegen Weitergabe personenbezogener Daten an Behörden zu wehren bis zur letztinstanzlich rechtskräftigen Verurteilung ➤ Eröffnung des Gerichtsweges in dem Mitgliedsstaat des DE für den Fall, dass Betroffener Rechte ggü. dem DI direkt geltend macht ➤ Entschädigungsklausel, d.h. Ausgleich im Innenverhältnis DE und DI, sodass letztlich der Schadensverursacher die Kosten trägt.	Ungewiss, da amerikanisches Recht vertrags-treuem Verhalten entgegensteht	Vermutlich werden sich große Softwarehersteller auf entsprechende Vereinbarungen nicht einlassen – mehr Verhandlungsmacht kann durch den Zusammenschluss mehrerer Hochschulen zu Einkaufsgemeinschaften o.Ä. erreicht werden.

⁹ Leitlinien 2/2018 des Europäischen Datenschutzausschuss, S. 9, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_de.

	➤ Vertragsstrafe für den Fall, dass Klauseln verletzt werden.		
Organisatorischer Art	➤ Pseudonymisierung, bei der nur der Datenexporteur die Zuordnung vornehmen kann ➤ Zusätzliche Verwendung von EU-Software/-Diensten für besonders sensible Daten	Gut	Hoher Aufwand

Tabelle 2: Zusätzliche Maßnahmen

III. Praktische Handlungsvorschläge für Hochschulen in NRW

Zwar ergibt sich das klare Bild, dass regelmäßig zusätzliche Maßnahmen zur Umsetzung des Schrems-II-Urteils ergriffen werden müssen. Dies betrifft auch Hochschulen in NRW, die vielfach in ganz unterschiedlichen Kontexten Verantwortliche im Sinne der DSGVO sind und dabei auf amerikanische Cloud-Dienste als Auftragsverarbeiter setzen, z.B. beim Einsatz von Videokonferenzdiensten von Microsoft oder Zoom. Ebenfalls zutreffend ist, dass im Urteil keine Übergangsfrist vorgesehen ist.

Zugleich konnten auch die Aufsichtsbehörden und ihre gemeinsamen Organisationen nicht ad-hoc benennen, welche konkreten Maßnahmen vorzunehmen sind. Der Europäische Datenschutzausschuss hat in einer Stellungnahme mitgeteilt, dass praktische Handreichungen erst noch entwickelt und dann veröffentlicht werden¹⁰, im Übrigen aber auch die Verantwortung der Verantwortlichen betont. Ähnlich die für die Hochschulen in NRW zuständige LDI NRW¹¹. Einzig der LfDI BaWü hat bisher konkretisiert, wann er bei einem Datentransfer in die USA via Standardvertragsklauseln diese durch zusätzliche Maßnahmen als hinreichend abgesichert ansieht (nach unserer Lesart einzig bei einer Ende-zu-Ende-Verschlüsselung, Anonymisierung oder Pseudonymisierung mit Zuordnungsmöglichkeit jeweils nur beim Datenexporteur in Verbindung mit umfassenden zusätzlichen vertraglichen Vereinbarungen).¹²

Zugleich steht am Ende des Dokuments (S. 9 f.) des LfDI BaWü folgender Hinweis:

¹⁰ S. 5 einer Stellungnahme, abrufbar unter https://edpb.europa.eu/our-work-tools/our-documents/ovrigt/frequently-asked-questions-judgment-court-justice-european-union_en.

¹¹ <https://www.lidi.nrw.de/mainmenu/Aktuelles/Inhalt/Schrems-II/Schrems-II.html>.

¹² Abrufbar unter <https://www.baden-wuerttemberg.datenschutz.de/orientierungshilfe-des-lfdi-bw-was-jetzt-in-sachen-internationaler-datentransfer/>.

Im Zentrum des weiteren Vorgehens des LfDI Baden-Württemberg wird die Frage stehen, ob es neben dem von Ihnen gewählten Dienstleister/Vertragspartner nicht auch zumutbare Alternativangebote ohne Transferproblematik gibt. Wenn Sie uns nicht davon überzeugen können, dass der von Ihnen genutzte Dienstleister/Vertragspartner mit Transferproblematik kurz- und mittelfristig unersetzlich ist durch einen zumutbaren Dienstleister/Vertragspartner ohne Transferproblematik, dann wird der Datentransfer vom LfDI Baden-Württemberg untersagt werden.

Uns ist bewusst, dass mit dem Urteil des EuGH u.U. extreme Belastungen für einzelne Unternehmen einhergehen können. Der LfDI wird sein weiteres Vorgehen

am Grundsatz der Verhältnismäßigkeit ausrichten. Wir werden die Entwicklung weiter beobachten und unsere Positionen dementsprechend laufend überprüfen und fortentwickeln.

Zu unterscheiden ist also zumindest nach dieser Position zwischen der Rechtslage und der Durchsetzung der Rechtslage durch die Aufsichtsbehörden. Nach unserer Auffassung ist es wegen der umfassenden Herausforderungen im Datenschutz auf allen Seiten – besonders im Zusammenhang mit der Corona-Krise – wahrscheinlich, dass auch andere Aufsichtsbehörden – wie etwa die LDI NRW – eine ähnliche Haltung einnehmen werden. Dafür spricht auch die Komplexität des Themas internationaler Datenverkehr, welche dadurch deutlich wird, dass bereits zwei Beschlüsse der gut ausgestatteten Europäischen Kommission (Safe Harbour, Privacy Shield) vom EuGH gekippt wurden. Zusätzlich ist zu berücksichtigen, dass Verantwortliche im öffentlichen Bereich - wie Hochschulen - wichtige Aufgaben im öffentlichen Interesse wahrnehmen und zur Aufgabenerfüllung auf manche Cloud-Services angewiesen sind. Schließlich hat die zuständige Aufsichtsbehörde (LDI NRW) selbst noch keine Konkretisierung veröffentlicht. **Aus diesen Gründen ist aus unserer Sicht nicht damit zu rechnen, dass innerhalb kurzer Frist pauschal alle Datentransfers in die USA untersagt werden.** Mit Bußgeldern müssen öffentliche Stellen in Deutschland nicht rechnen. Solche können nur gegen private Unternehmen verhängt werden.

Dies vorausgeschickt, raten wir Hochschulen in NRW dennoch nicht zur Passivität. Selbst wenn es mit verhältnismäßigem Aufwand den Hochschulen nicht möglich ist, schon jetzt eine eindeutig rechtssichere Grundlage von Datentransfers in die USA zu schaffen, ist es aus unserer Sicht angezeigt, sich darum zumindest zu bemühen. Dieses Bemühen und der Aktivitätsnachweis wird auch in etwaigen Gesprächen bzw. Prüfverfahren (mit) der Aufsichtsbehörde helfen.

Folgendes Vorgehen schlagen wir vor:

1. Alle Datentransfers dem nach Art. 30 DSGVO zu führendem Verzeichnis entnehmen.

2. Datentransfers, die ausschließlich auf das Privacy Shield gestützt wurden, sofort einstellen. Den Auftragsverarbeiter kontaktieren, auf das Urteil und dessen Bedeutung hinweisen und die Vereinbarung von Standardvertragsklauseln mit wesentlichen Ergänzungen (der Tabelle 2 zu entnehmen) vorschlagen.
3. Bei Datentransfers, die lediglich *auch* auf das Privacy Shield gestützt wurden, den Hinweis auf dieses in den entsprechenden Datenschutzerklärungen löschen.
4. Das „Zumutbarkeitsargument“ des LfDI BaWü für sich aufbauen. Auch dies verlangt indes ein Tätigwerden: Es muss für jeden Cloud-Dienst mit Transferproblematik reflektiert werden, ob es eine **zumutbare Alternative ohne Transferproblematik** gibt. Diese Reflexion sollte schriftlich festgehalten werden. Bestenfalls lässt sich hierzu die schriftlich dokumentierte Abwägungsentscheidung zur Anschaffung der Software (vgl. *Albrecht/Fischer/McGrath/John/Wellmann*, Datenschutzrechtlicher Leitfaden: Zoom-Angebot durch Hochschulen, S. 5-9¹³) als Basis heranziehen.

Am Beispiel eines Videokonferenzdienstes wie Zoom muss analysiert werden:

- a) Welche Funktionen und Kapazitäten werden für die Aufgabenerfüllung benötigt? Welche Ressourcen können eingesetzt werden?
Hier erscheint auch eine Evaluation nach den ersten Monaten Praxiserfahrung im Online-Semester angezeigt (Ist eine Videokonferenz bei 200 Teilnehmer:innen sinnvoll? Reichen auch Kapazitäten bis 50 Teilnehmer:innen? Und ähnlich).
 - b) Welche Funktionen und Kapazitäten bietet Zoom, welche Ressourcen erfordert es?
 - c) Welche Funktionen und Kapazitäten bieten andere Dienste, die keine Transferproblematik haben, welche Ressourcen erfordern sie? (vgl. hierzu z.B. *Fischer/Albrecht*, Übersicht: Videodienste und Datenschutz, RiDHnrw-Veröffentlichung¹⁴, z.B. zu BigBlueButton)
5. Dienste, bei denen keine zumutbaren Alternativen bestehen, können in der Dringlichkeit eines „datenschutzrechtlichen Updates“ zunächst zurückgestellt, wenn auch nicht vergessen werden. Auch für diese Dienste sollten mittelfristig folgende Schritte durchgeführt werden. Bei Diensten mit zumutbarer Alternative sollten diese sofort eingeleitet werden. Führen sie nicht zu einem befriedigenden, verbesserten Ergebnis, sollte ein Wechsel des Dienstes auch vor Auslaufen der Verträge ernstlich erwogen werden.
- Bei knappen Ressourcen kann eine weitere Priorisierung nach einem risikobasiertem Ansatz vorgenommen werden: Dabei wird in der Übersicht der Datenübertragungen in Drittstaaten die jeweils übertragenen Kategorien an Daten vermerkt. In Einklang mit den Wertungen der

¹³ Zuletzt abgerufen am 9.9.20 unter https://www.itm.nrw/wp-content/uploads/RiDHnrw_18.05.20_Datenschutzrechtlicher-Leitfaden-Zoom-Angebot-durch-Hochschulen-NRW.pdf.

¹⁴ Abrufbar unter https://www.itm.nrw/wp-content/uploads/RiDHnrw_02.07.20_Uebersicht_Videodienste_Datenschutz.pdf.

DSGVO (z.B. besonderer Schutz von Gesundheitsdaten, biometrische Daten u.Ä.) sollten – sofern eine Priorisierung nötig ist – die Transfers von besonders sensiblen Daten zuerst analysiert und den neuen Vorgaben angepasst werden.

6. Wenn dann die Transfers geordnet und die Prioritäten klar sind, schlagen wir als ersten Aktivitätsnachweis folgende Schritte vor:
 - a) Die entsprechend identifizierten (Schritte 1-5) Auftragsverarbeiter anschreiben, auf das Urteil hinweisen und sich die Einhaltung der vereinbarten Standardvertragsklauseln (im Folgenden SVK), insbesondere Artikel 5, bestätigen lassen – und zwar in detaillierter Form nach Art einer Checkliste.
 - b) Für den Fall der negativen Auskunft fragen, welche „zusätzlichen Maßnahmen“ aus Sicht des Unternehmens ergriffen werden können, die dann hinreichend zur Umsetzung des Urteils sind.
 - c) Fragen, ob und unter welchen Voraussetzungen ein „Umzug“ der Cloud-Dienstleistung inklusive der Metadatenverarbeitung auf europäische Server möglich ist.

Zu einer entsprechenden Anfrage an die Unternehmen bietet die Non Profit Organisation NOYB des Beschwerdeführers Max Schrems eine englischsprachige Vorlage im .doc/.odt-Format, die unter <https://noyb.eu/de/naechste-schritte-fuer-eu-unternehmen-faqs> heruntergeladen werden kann. Auszug:

Request to a US importer, when using SCCs (case by case analysis)

Given the judgment of the Court of Justice of the European Union in C-311/18, especially paragraphs 138 to 145, Clause II of the Annex of Decision 2004/915/EC, and/or Clause 5(b) of the Annex to Decision 2010/87, we urgently seek clarification on the following questions:

Direct Application of 50 U.S.C. § 1881a (= FISA 702)

- (1) Do you or any other relevant US entity (controller or processor) that processes or has access to personal data that is transferred to you fall under one of the following definitions in 50 U.S.C. § 1881(b)(4), that could render you or the other entit(ies) directly subject to 50 U.S.C. § 1881a (= FISA 702)?

☐ Yes ☐ No ☐ We are under a legal obligation not to answer this question

- (2) Especially,

7. Bei Unsicherheiten über den Umgang mit Antworten auf die Anfrage aus Schritt 6 kann eine Anfrage an die LDI NRW als zuständige Aufsichtsbehörde gestellt werden.
8. Abwarten der (konkreteren) Handlungsempfehlungen des Europäischen Datenschutzausschusses und insb. der LDI NRW.

9. Je nach Handlungsempfehlungen nach 7. und 8. Einleiten weiterer Schritte, z.B.
 - a) Nachverhandlung der Standardvertragsklauseln
 - b) Verlangen des „Umzugs“ auf europäische Server, um Datentransfer zu beenden
 - c) Einstellen der Nutzung des Dienstes, Kündigung der Verträge

Für die Zukunft gilt aus unserer Sicht bei Anschaffungsentscheidungen und Vertragsverhandlungen zur Neulizenzierung schon jetzt in jedem Fall:

1. Europäische Alternativen oder US-amerikanische Alternativen mit EU-Servern (eingeschränkt, wegen des CLOUD Acts) sind sorgfältig in die Auswahl mit einzubeziehen und *unter Datenschutzaspekten* grundsätzlich vorzuziehen, um Datentransfers ganz zu vermeiden. (Hier können einzelne Hochschulen mehr Verhandlungsmacht gegenüber großen Softwarekonzernen gewinnen, wenn sie sich zu Einkaufsgemeinschaften zusammenschließen und zentral verhandeln, siehe z.B. <https://www.kopit.de/> - Gleiches gilt auch für das Nachverhandeln von Standardvertragsklauseln u.Ä.).
2. Falls US-Anbieter ohne EU-Server lizenziert werden sollen, gilt, dass sie nun mehr nur in Betracht kommen bei guter Verschlüsselungsstruktur (Ende-zu-Ende) oder Pseudonymisierung mit Zuordnungsmöglichkeit nur beim Verantwortlichen *und in beiden Fällen* unter Vereinbarung wesentlicher Ergänzungen zu den SVK. Abweichungen hiervon sind allenfalls bei Anwendungen denkbar, bei denen nachweisbar keine zumutbare Alternative ohne Datentransferproblematik besteht.

D. Auswahl hilfreicher weiterführender Quellen

- Grasmück/Kollmar, Drittstaatenübermittlung nach Schrems II - Wie geht es weiter mit US-amerikanischen Clouddiensten?, IPRB 2020, 212-216
- <https://noyb.eu/de/naechste-schritte-fuer-eu-unternehmen-faqs> insb. zu (englischsprachige) Musterversionen für Anfragen Frage 6.
- Orientierungshilfe des LfDI BaWü, abrufbar unter <https://www.baden-wuerttemberg.datenschutz.de/orientierungshilfe-des-lfdi-bw-was-jetzt-in-sachen-internationaler-daten-transfer/>
- <https://datenschutz-generator.de/dsgvo-usa-muster-checkliste-scc/>
- Link-Sammlung der Gesellschaft für Datenschutz und Datensicherheit (Stellungnahme aller Aufsichtsbehörden soweit verfügbar, Fachbeiträge, eigene Hinweise), <https://www.gdd.de/eu-us-privacy-shield-schrems-ii-urteil>