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-Urteil[1]?
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

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:die 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.ldi.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 ***zusätzlicher Maßnahmen***[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 vertragstreuem 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 werden [10], im Übrigen aber auch die Verantwortung der Verantwortlichen betont. Ähnlich die für die Hochschulen in NRW zuständige LDI NRW[11]. 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.ldi.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. 5-9[13]) 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-Veröffentlichung[14], 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-datentransfer/
- 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