4/2020
73 – 96

Judikatur
Digitaler Türspion
Haidinger/Löffler

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

EuGH *Schrems II* – internationaler Datenverkehr ade?

Prüfschema internationaler Datenverkehr
Andreas Zavadil

Schrems II: Uncle Sam am Boden?
Maximilian Kröpfl und Andreas Rohner

Datenübermittlung in die USA: Auswege aus dem digitalen Lock-down?
Claudia Gabauer und Alexander Höller

Daten können Leben retten
Interview mit Peter Lehner, 1. Vorsitzender Konferenz SV-Träger

Information & Transparenz (Teil 2)
Ursula Illibauer

Sind vollautomatisierte Entscheidungen unter Art 22 DSGVO zu subsumieren?
Stefanie Chiba

BGH hat zu Cookies entschieden – Relevanz in Österreich?!
Juliane Messner und Max W. Mosing

ISSN 2313-5409

dako.manz.at

MANZ

Österreichische Post AG PZ 18Z041356 P Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

Andreas Zavadil (Prüfschema)/Rainer Knyrim
Referent DSB/Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte

Prüfschema internationaler Datenverkehr nach EuGH *Schrems II*

Datentransfer in Drittstaat; Datentransferinstrument. Mit der Entscheidung vom 16. 7. 2020, C-311/18, *Schrems II*, hat der EuGH das Privacy Shield-Abkommen für ungültig erklärt. Ein Transfer von Daten in einen Drittstaat ist daher neu zu beurteilen. Dieses Prüfschema hilft dabei.

Dieses Prüfschema zur Vorgehensweise bei der Prüfung der Auswirkungen wurde der Dako von Herr Mag. *Andreas Zavadil* von der Datenschutzbehörde zur Verfügung gestellt. Es handelt sich hierbei ausschließlich um die persönliche Meinung von Herrn Mag. *Zavadil,* welche die Datenschutzbehörde in einem Verfahren nicht bindet.

Das Prüfschema ist in Einklang mit den Dokumenten des EDSA zu lesen, insb den Leitlinien 2/2018 zu den Ausnahmen nach Art 49 DSGVO und der EDSA-Stellungnahme vom 17. 7. 2020 zur Entscheidung *Schrems II*.

Das Prüfschema ist von unten nach oben zu lesen:

- In der ersten Stufe ist das Vorliegen der Grundsätze für die Datenverarbeitung nach Art 5 ff DSGVO zu prüfen.
- Sind die Grundsätze erfüllt und die Verarbeitung und Übermittlung der Daten damit an sich zulässig, muss in der zweiten Stufe geprüft werden, ob der geplante Datentransfer in einen EWR-Staat oder in einen Drittstaat stattfinden soll. Für den Transfer in einen EWR-Staat sind aufgrund des einheitlichen Schutzniveaus, das die DSGVO geschaffen hat, keine weiteren Voraussetzungen erforderlich.
- Für einen Transfer in einen Drittstaat sind hingegen zusätzliche Voraussetzungen notwendig, die in der dritten Stufe zu prüfen sind:
  - Entweder es liegt ein Datentransferinstrument der Art 45 bis 47 DSGVO vor, wobei auf diese nun die vom EuGH in der Entscheidung *Schrems II* aufgestellten Grundsätze anzuwenden sind;[1]
  - oder, wenn kein solches Datentransferinstrument vorliegt, muss geprüft werden, ob eine der – restriktiv auszulegenden – Ausnahmen des Art 49 DSGVO vorliegt.
- Die Ausnahmen können in einer Ausnahme des Art 49 Abs 1 UAbs 1 DSGVO bestehen (insb Einwilligung, Vertragserfüllung, wichtige Gründe öffentlichen Rechts oder die Erforderlichkeit zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen), oder wenn keiner dieser Tatbestände zutrifft und kein Instrument gem Art 45 bis 47 DSGVO in Betracht

[1] Siehe *Kröpfl/Rohner, Schrems II:* Uncle Sam am Boden? Dako 2020/44 (in diesem Heft Seite 78).

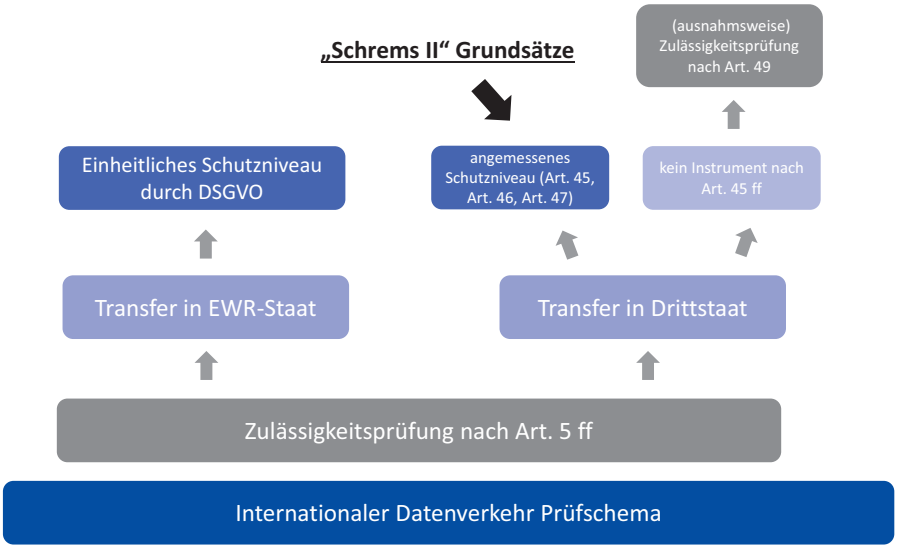

Abb 1: Prüfschema internationaler Datenverkehr nach *Schrems II*

kommt, nach Abs 1 UAbs 2 in einer besonderen Ausnahme für die Wahrnehmung eines zwingenden berechtigten Interesses, wobei diesfalls die Übermittlung nicht wiederholt erfolgen darf und nur eine begrenzte Anzahl Betroffener umfassen darf, wobei eine Gesamtbeurteilung der Umstände der Datenübermittlung vorgenommen werden muss, angemessene Garantien vorgesehen werden müssen und die Datenschutzbehörde darüber in Kenntnis und die Betroffenen darüber unterrichtet werden müssen.[2]

Rainer Knyrim

Dako 2020/43

[2] Siehe *Gabauer/Höller*, Datenübermittlung in die USA: Auswege aus dem digitalen Lock-down? Dako 2020/45 (in diesem Heft Seite 80).

Über die Autoren

Prüfschema: Mag. Andreas Zavadil ist seit 2017 Referent bei der Datenschutzbehörde. Der Beitrag gibt ausschließlich seine persönliche Meinung wieder und bindet die Datenschutzbehörde in keinem allfälligen Verfahren.
E-Mail: Andreas.Zavadil1@dsb.gv.at
Dr. Rainer Knyrim ist Rechtsanwalt und Partner bei Knyrim Trieb Rechtsanwälte, Wien.
E-Mail: ky@kt.at

Zur Entscheidung *Schrems II* siehe auch:

- *Kröpfl/Rohner*, *Schrems II:* Uncle Sam am Boden? Dako 2020/44 (in diesem Heft Seite 78);
- *Gabauer/Höller*, Datenübermittlung in die USA: Auswege aus dem digitalen Lock-down? Dako 2020/45 (in diesem Heft Seite 80).

Nicht aufgehoben wurden hingegen SDK, deren grundsätzliche Zulässigkeit als Instrument zur Gewährleistung eines angemessenen Schutzniveaus bei der Übermittlung von personenbezogenen Daten in Drittländer vom EuGH bestätigt wird.

Gleichzeitig betont der Gerichtshof aber die hohen Anforderungen an ihre Nutzung: Der Datenexporteur hat **in jedem Einzelfall** – gegebenenfalls in Zusammenarbeit mit dem Datenimporteur – zu prüfen, *„ob das Recht des Bestimmungsdrittlands nach Maßgabe des Unionsrechts einen angemessenen Schutz der auf der Grundlage von Standarddatenschutzklauseln übermittelten personenbezogenen Daten gewährleistet"*.[13] Ist dieser Schutz nicht gegeben, so hat der Datenexporteur zusätzliche Maßnahmen zu ergreifen, um die Einhaltung des angemessenen Schutzniveaus zu gewährleisten.[14] Ist das nicht möglich, so ist **die Übermittlung** bis zur Sicherstellung des angemessenen Schutzniveaus **auszusetzen oder zu beenden**.[15] Der zuständigen Aufsichtsbehörde kommt dieselbe Pflicht zu. Will der Datenexporteur Daten in die USA übermitteln, nachdem ein Empfänger den Mangel von notwendigen Garantien mitgeteilt hat, so hat er der Datenschutzbehörde die Mitteilung des Empfängers weiterzuleiten.[16]

Warum sich Standardvertragsklauseln weiterhin anwenden lassen

Anders als beim Angemessenheitsbeschluss zu den USA, hat der EuGH hinsichtlich der SDK bloß festgestellt, dass die Prüfung anhand der Art 7, 8 und 47 GRC nichts ergeben hat, was deren Gültigkeit berühren könnte.[17] SDK sind somit weiterhin ein zulässiges Instrument zur Gewährleistung eines adäquaten Schutzniveaus bei einem Empfänger in einem Drittland.[18]

Denn anders als beim Angemessenheitsbeschluss, der darauf abzielt, verbindlich festzustellen, dass in einem bestimmten Drittland ein angemessenes Schutzniveau besteht,[19] liegt die Zielsetzung bei SDK darin, dass es Sache des Verantwortlichen bzw Auftragsverarbeiters ist, insb geeignete Garantien als Ausgleich für den im Drittland bestehenden Mangel an Datenschutz vorzusehen und dadurch sicherzustellen, dass der europäische Datenschutz und die Rechte der betroffenen Personen auf angemessene Art und Weise beachtet werden.[20] Und (alleine) hierfür ist die Vereinbarung und Umsetzung der Bestimmungen der SDK ein geeignetes Instrument. Dennoch hält der EuGH klar fest, dass SDK naturgemäß keine Garantien bieten können, die über die vertragliche Verpflichtung hinausgehen. Es kann daher erforderlich sein, dass der Verantwortliche zusätzliche Maßnahmen ergreift, um ein angemessenes Schutzniveau zu gewährleisten, wenn dies nach durchgeführter Einzelfallanalyse notwendig ist.[21]

Es stellt sich die Frage, wann das Recht des Bestimmungsdrittlands dem Unionsrecht adäquat ist. Der EuGH verlangt einen Art 47 GRC nachgebildeten[22] Rechtsschutz.[23] Darüber hinaus müssen Eingriffe in Privatsphäre und Datenschutz[24] für die Zweckerreichung notwendig[25] und auf ein verhältnismäßiges Maß beschränkt sein.[26] Hilfsweise herangezogen werden kann das Prüfschema der Art. 29-Datenschutzgruppe,[27] wonach bei Behördenzugriffen jedenfalls folgende **vier „Europäische Garantien"**[28] vorliegen sollen:

- 1. Die Verarbeitung geschieht auf Grundlage einer klaren, präzisen und öffentlich zugänglichen Vorschrift.
- 2. Die Notwendigkeit und Verhältnismäßigkeit sind in Hinblick auf das verfolgte (legitime) Ziel nachgewiesen.
- 3. Es existiert ein unabhängiger Überwachungsmechanismus.
- 4. Für betroffene Personen bestehen effektive Rechtsschutzinstrumente.

Warum das für die Vereinigten Staaten nicht gilt

Legt man die vier „Europäischen Garantien" auf SDK für die Übermittlung in die USA um, so hat der Datenexporteur zu gewährleisten, dass diese bei einem behördlichen Zugriff eingehalten werden. Der Datenexporteur wird hierbei mit Blick in die USA jedoch auf **dieselben Probleme** stoßen, die der EuGH auch in seiner **Beurteilung des Privacy Shield** aufgezeigt hat.

Um SDK für eine Übermittlung in die USA verwenden zu können, muss der Datenexporteur zunächst prüfen, ob der US-amerikanische Empfänger in den Anwendungsbereich der Überwachungsprogramme fällt. Das trifft im Wesentlichen auf alle *„Anbieter elektronischer Kommunikationsdienste"*[29] zu. Relevant sind aber auch andere Empfänger, die ihrerseits einen solchen Anbieter (bspw für Hosting) nutzen. Zusätzlich ist zu überprüfen, ob die Übermittlung der personenbezogenen Daten an den Empfänger ausreichend vor Zugriff im Transit geschützt ist. Hier könnte die Antwort in der Verschlüsselung liegen.

Kann der Empfänger Ziel eines Überwachungsprogramms werden, so hat der Datenexporteur zusätzliche Maßnahmen zu treffen, um ein angemessenes Schutzniveau herzustellen, also die **Beeinträchtigungen durch die amerikanischen Überwachungsprogramme und die damit verbundenen Rechtsschutzdefizite auszugleichen**.[30] Praktisch ist das nur schwer möglich, da rein vertragliche Zusatzvereinbarungen es nicht vermögen, gesetzliche Vorschriften des Empfängerlandes außer Kraft zu setzen. Auf faktischer Ebene könnten die SDK für diese Empfänger in den USA aber etwa dann anwendbar bleiben, wenn die übermittelten personenbezogenen Daten sowohl beim Transit als auch für den Datenimporteur in den USA durch Verschlüsselung nicht lesbar sind. Dies wäre jedoch mit Ausnahme weniger Dienste (bspw das „reine" Hosten) vermutlich kaum sinnvoll.

Die Übermittlung personenbezogener Daten in die USA auf reiner Basis der SDK wird daher mit heutigem Stand in aller Regel nicht zulässig sein.[31]

Vor Zugriffen im Transit kann Verschlüsselung schützen.

Was jetzt zu tun ist

In ersten Reaktionen auf das Urteil versichern große US-Anbieter,[32] dass der Daten-

[13] *Schrems II* Rn 134. [14] *Schrems II* Rn 133. [15] *Schrems II* Rn 135, 146. [16] *Schrems II* Rn 145. [17] *Schrems II* 4. Spruchpunkt. [18] Wenngleich sich der EuGH nur mit den C2P-SDK auseinandergesetzt hat, sind keine Gründe ersichtlich, die vom EuGH getätigten Aussagen nicht auch auf SDK zwischen Verantwortlichen vollumfänglich anzuwenden. [19] *Schrems II* Rn 129. [20] *Schrems II* Rn 131. [21] *Schrems II* Rn 133. [22] Eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu seinen personenbezogenen Daten zu erlangen, ihre Berichtigung oder Löschung zu erwirken, widerspricht dem Wesensgehalt des Art 47 GRC auf wirksamen gerichtlichen Rechtsschutz; vgl *Schrems I* Rn 95. [23] *Schrems II* Rn 168. [24] *Schrems II* Rn 176. [25] So steht für den EuGH fest, dass eine Regelung, die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen vermögen, nicht auf das Notwendige beschränkt ist; vgl *Schrems I* Rn 93. [26] Siehe *Schrems I* Rn 73. [27] *Art. 29-Datenschutzgruppe,* Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) 13. 4. 2016, WP 237. [28] *Art. 29-Datenschutzgruppe,* 01/2016, WP 237, 6. [29] 50 U.S. Code § 1881. [30] *Schrems II* Rn 133. [31] *Datenschutzkonferenz,* Urteil des Europäischen Gerichtshofs zur Übermittlung personenbezogener Daten in Drittländer („Schrems II") stärkt den Datenschutz für EU-Bürgerinnen und Bürger (28. 7. 2020). [32] *Weiß,* Google setzt auf Standarddatenschutzklauseln nach gekipptem Privacy Shield; www.heise.de/news/Google-setzt-auf-Standarddatenschutzklauseln-nach-gekipptem-Privacy-Shield-4862466.html. *Mailchimp,* Ensuring Compliance with EU Data Protection Laws, https://mailchimp.com/eu-us-data-transfer-statement/ (Stand 10. 8. 2020).

fluss in die USA weiterhin auf SDK gestützt werde. Doch ohne weitere Schritte und Garantien ist die Verwendung von SDK für die Übermittlung personenbezogener Daten in die USA ein „totes Pferd". Und bekanntlich reiten nur verzweifelte Indianer ein totes Pferd.[33]

Ein einfaches Umsatteln vom Privacy Shield auf SDK wird aufgrund der Probleme nicht möglich sein.

In der Praxis empfiehlt sich für einen EU-Datenexporteur, die Datenflüsse in die USA zu identifizieren und unter Mithilfe des Empfängers zu definieren, ob dieser dem FBI, der NSA oder sonstigen staatlichen Stellen Zugriff auf die bei ihm verarbeiteten europäischen Daten geben muss.[34] Bejahendenfalls ist zu prüfen, ob unter Anwendung der vier „Europäischen Garantien" ein angemessenes Schutzniveau (potentiell auch mit zusätzlichen Maßnahmen) erreicht werden kann. Je nach Ergebnis: Datenübermittlung aussetzen, stoppen oder weiterführen. *Gabauer/Höller* stellen Alternativen in Form von anderen Garantien und besonderen Ausnahmen für den internationalen Datentransfer vor.[35]

Zwar nicht Verfahrensgegenstand, aber dennoch naheliegend sind Fragen, wie mit bestehenden Angemessenheitsbeschlüssen (bspw Israel) umzugehen ist und ob nach Ende der **Brexit-Übergangsphase** ein freier Datenverkehr zwischen der EU und dem Vereinigten Königreich möglich sein wird. Unternehmen mit engen Verbindungen in andere Drittländer mit Angemessenheitsbeschluss sollten auch hier hinterfragen, ob man nicht einem unkalkulierbaren Risiko ausgesetzt ist. Es liegt an der Kommission diese Beschlüsse zu überprüfen, bevor sie wie der Privacy Shield vom EuGH aufgehoben werden. Prioritärer für die Kommission dürfte nun aber der Nachfolger zum Privacy Shield – oder, zynisch gesagt, der Grund für Schrems III – sein.[36]

Dako 2020/44

[33] In Anlehnung an *Matthias Strolz*, Sten Prot 31. 1. 2017 160. Sitzung 25. GP 178. [34] Section 702 FISA, EO 12.333. [35] Vgl *Gabauer/Höller*, Datenübermittlung in die USA: Auswege aus dem digitalen Lock-down? Dako 2020/45. [36] *Kom*, Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross; https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836 (11. 8. 2020).

Zum Thema

Über die Autoren

Mag. Maximilian Kröpfl ist Rechtsanwaltsanwärter bei Knyrim Trieb Rechtsanwälte. E-Mail: mk@kt.at. Mag. Andreas Rohner ist Rechtsanwaltsanwärter bei Knyrim Trieb Rechtsanwälte. E-Mail: ar@kt.at.

Zur Entscheidung *Schrems II* siehe auch:

- ***Gabauer/Höller*, Datenübermittlung in die USA: Auswege aus dem digitalen Lock-down? Dako 2020/45 (in diesem Heft Seite 80);**
- ***Zavadil*, Prüfschema internationaler Datenverkehr nach EuGH Schrems II, Dako 2020/43 (in diesem Heft Seite 77).**

Claudia Gabauer/Alexander Höller
Rechtsanwaltsanwärterin/Rechtsanwalt bei Knyrim Trieb Rechtsanwälte

Datenübermittlung in die USA: Auswege aus dem digitalen Lock-down?

Konsequenzen aus der EuGH-Entscheidung *Schrems II*. Die DSGVO bietet eine Vielzahl geeigneter Garantien zur Übermittlung personenbezogener Daten in Drittländer. Die Gründe für die Aufhebung des EU-US Privacy Shields durch den EuGH schlagen jedoch auf die meisten dieser Garantien durch, sodass diese kaum geeignet sind, eine Übermittlung in die USA zu legitimieren. Auswege bieten die Ausnahmen nach Art 49 DSGVO sowie bereits bestehende Genehmigungen nach dem DSG 2000.

Einleitung

Der EuGH hat den **EU-US Privacy Shield** mit sofortiger Wirkung für ungültig erklärt.[1] Datenübermittlungen in die USA können daher nicht mehr auf diesen gestützt werden. Auch wenn der EuGH die Gültigkeit der Standardvertragsklauseln[2] (nach der Diktion der DSGVO nunmehr **„Standarddatenschutzklauseln"** – SDK) bestätigt hat, schlagen die im Urteil ins Treffen geführten Einwände in Bezug auf das in den USA gewährleistete Schutzniveau, insb die geheim- und sicherheitsbehördlichen Befugnisse, auch auf die SDK durch, sofern nicht zusätzliche Maßnahmen ergriffen werden, die über eine bloße vertragliche Verpflichtung hinausgehen.[3]

In der Folge wird skizziert, ob und wenn ja, unter welchen Voraussetzungen personenbezogene Daten dennoch datenschutzkonform in die USA übermittelt werden können.

(Alternative) Geeignete Garantien

Neben SDK sieht Art 46 DSGVO weitere geeignete Garantien vor, die bei Fehlen eines Angemessenheitsbeschlusses eine Übermittlung in ein Drittland legitimieren können. Der Europäische Datenschutzaus-

[1] EuGH 16. 7. 2020, C-311/18, *Data Protection Commissioner/Facebook Ireland Ltd, Maximilian Schrems*. [2] Beschluss 2010/87/EU der EK vom 5. 2. 2010 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländer nach der RL 95/46/EG. [3] Vgl im Detail zu den Entscheidungsgründen *Kröpfl/Rohner*, *Schrems II:* Uncle Sam am Boden? Dako 2020/44, in diesem Heft Seite 78.