VISCHER

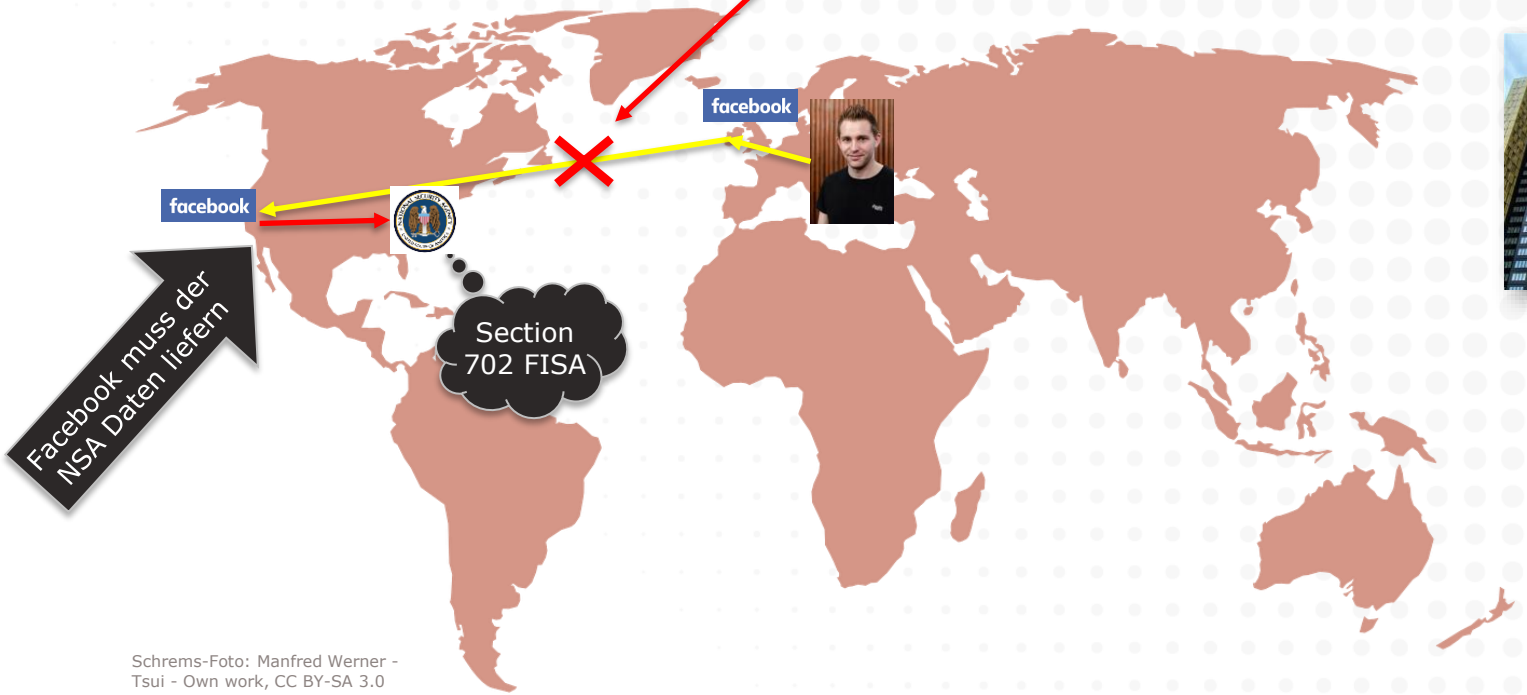
Internationaler Datentransfer.

Herausforderungen und Lösungen aus der Praxis

David Rosenthal, Partner, VISCHER AG
17. Oktober 2022

Ausgangslage

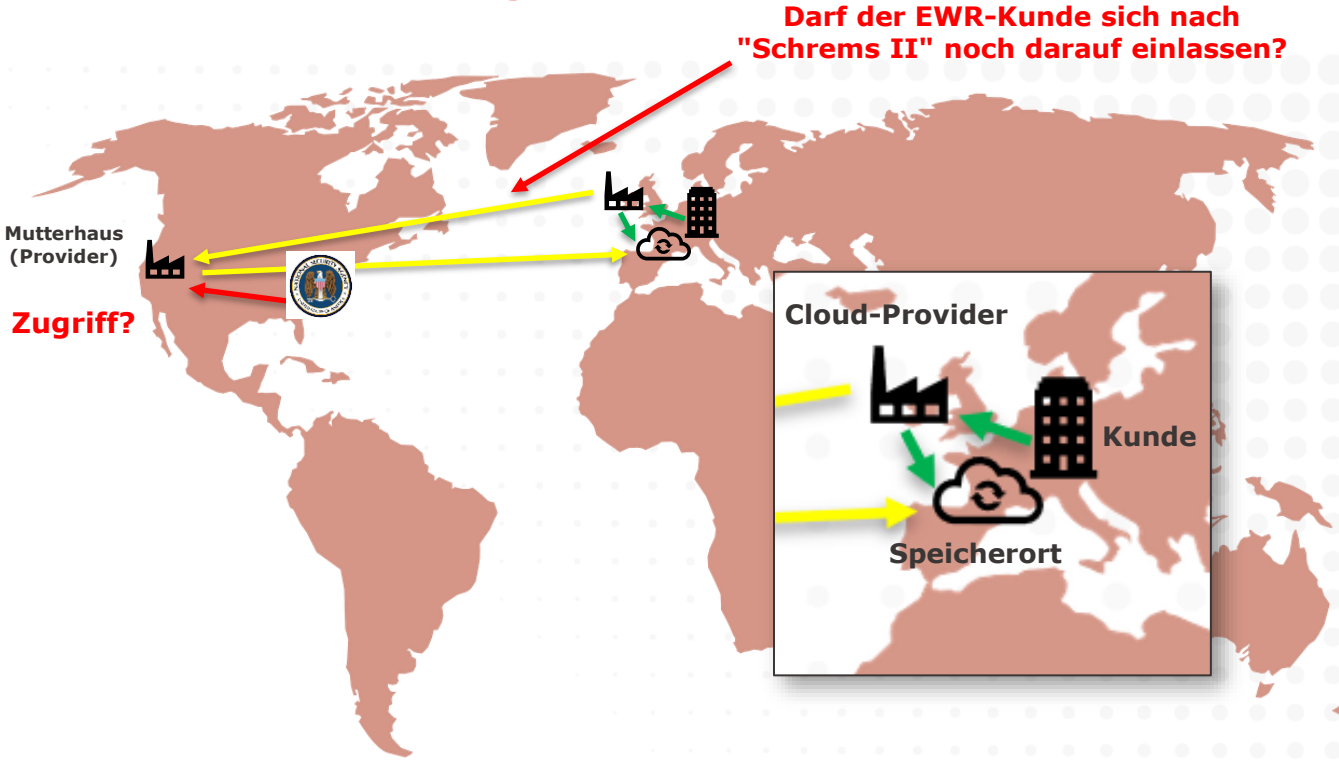
Datentransfer ist unzulässig, weil von einem Zugriff durch die NSA nach Section 702 FISA / EO 12333 auszugehen ist



EuGH vom 16. Juli 2020 (C-311/18, "Schrems II")

Schrems-Foto: Manfred Werner - Tsui - Own work, CC BY-SA 3.0

Herausforderung Nr. 1



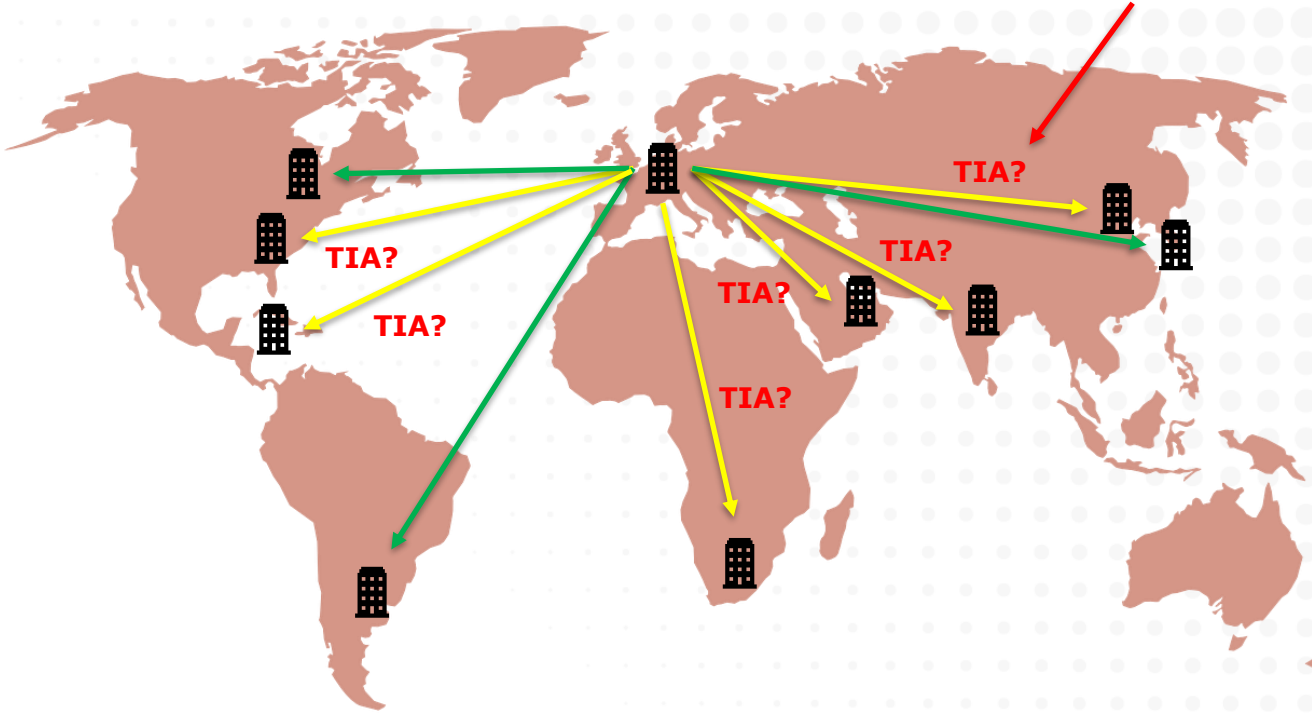
Besteht ein Risiko eines Datenzugriffs durch die NSA beim Einsatz eines Cloud-Providers mit US-Mutter, auch wenn eine Cloud in Europa verwendet wird?

Spoiler: Bei den meisten Cloud-Anbietern können Zugriffe vom Mutterhaus in den USA vorkommen

Herausforderung Nr. 2

Transfer Impact Assessment = Prüfung, ob im konkreten Fall Grund zur Annahme besteht, dass es zu einem problematischen Behördenzugriff kommen wird

Artikel 14 EU SCC

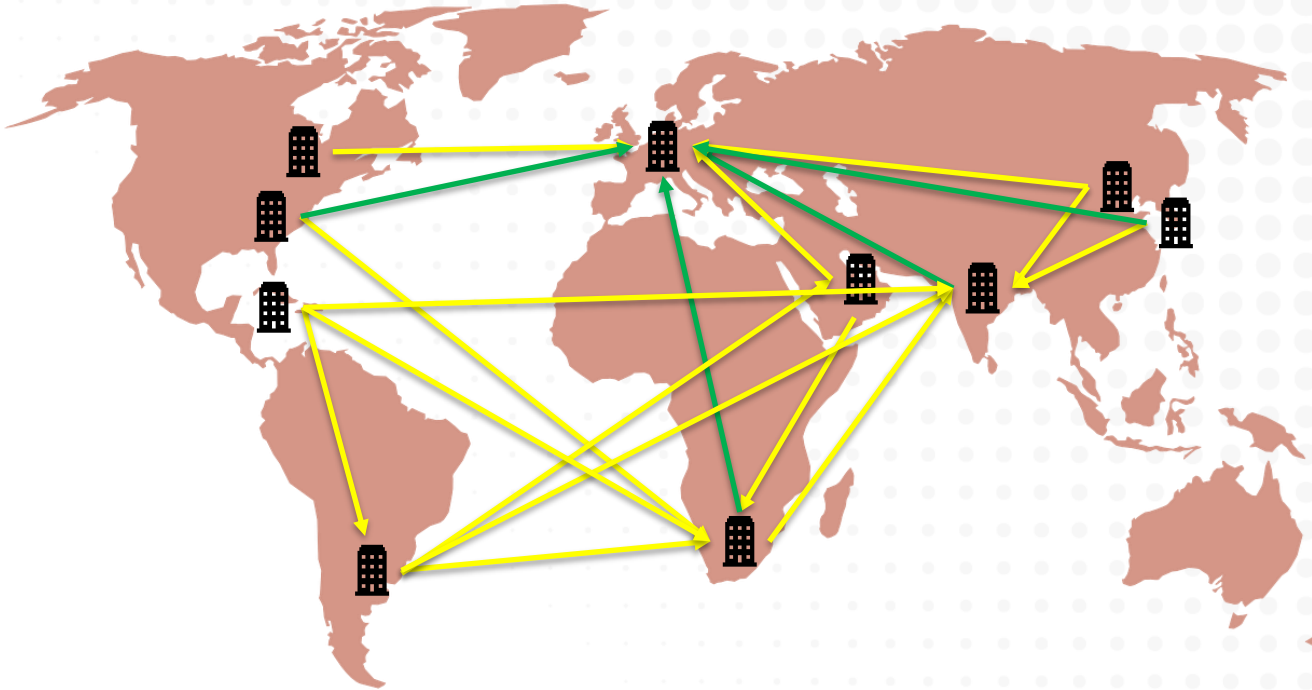


Die "Schrems II"-Herausforderung betrifft nicht nur Übermittlungen an Provider in den USA, sondern in alle Länder ohne angemessenen Datenschutz …

Spoiler: In manchen Staaten in die Lage viel schlimmer als in den USA

Herausforderung Nr. 3

Welche vertraglichen und sonstigen Regeln gelten für Übermittlungen aus diesen anderen Ländern?

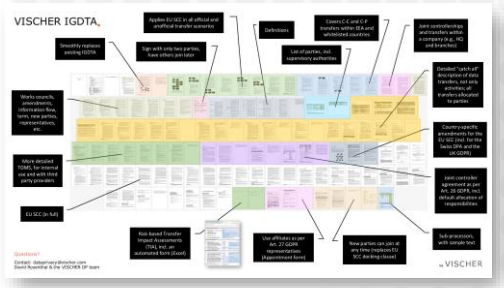


Wir verwenden für alle Übermittlungen aus Europa heraus die EU SCC. Aber was ist mit den Übermittlungen aus anderen Ländern?

Spoiler: Immer mehr haben ihre eigenen, teils auch stark abweichenden Vorgaben an SCC und Übermittlungen …

Lösung zu Nr. 3

Checkliste für IGDTAs:
https://bit.ly/3g23geR



- Ein **Intra-Group-Data-Transfer-Agreement** (IGDTA)
  - Mehrparteien-Vertrag unter allen Konzerngesellschaften
  - Bringt EU SCC wo nötig zum Einsatz (Kapitel V DSGVO)
  - Controller-Processor-Verträge (Art. 28 DSGVO)
  - Joint-Controller-Verträge (Art. 26 DSGVO)
  - Controller-Controller-Transfers, auch *branches*
  - Länderspezifische Anhänge, welche all diese Dinge auch aus Sicht des lokalen Rechts regeln
- In den meisten Ländern können die **EU SCC in modifizierter Form** für Übermittlungen aus diese Ländern benutzt werden
- Hohe Komplexität, hoher Aufwand, aber nur eine Fleissarbeit

Lösung zu Nr. 1

Was macht die NSA wirklich? Antworten: https://bit.ly/3wGjRup

- **Ausgangslage**: Cloud-Service eines US-Providers, mit dessen EU-Tochtergesellschaft wir einen Vertrag schliessen
  - Microsoft, AWS, Google, Salesforce.com, Hubspot etc.
  - Zugriffe aus den USA etc. vertraglich fast immer vorbehalten
  - Übermittlung in die USA ist zwar primär Sache der Tochter, aber als Controller bleiben wir in der Verantwortung …
- **Ziel:** Kein Grund zur Annahme, dass im konkreten Fall ein aus EU-Sicht problematischer US-Behördenzugriff erfolgen wird
  - Section 702 FISA, EO 12333: In jedem Fall problematisch
  - US CLOUD Act: Bei Berufs- und Amtsgeheimnis problematisch
  - Erreichen wir mit technischen und organisatorischen Mitteln, beurteilen wir mit einem "Transfer Impact Assessment" (TIA)

Schweizer Banken kannten das Problem wegen des Bankgeheimnisses schon vor "Schrems II" …

EDSA: "no reason to believe that relevant and problematic legislation will be applied in practice"

Welche Massnahmen wir treffen

Bis in zwei Jahren wird es die Angebote der grossen Hyperscaler aus (fast) rein europäischer Hand geben

- Wir **verschlüsseln Daten "in-transit"**
  - Folge: Upstream-Zugriffsrisiko durch NSA fällt ± weg
    - Upstream = Kabelaufklärung (Mithören auf Backbones etc.)
- Wir wählen einen **Vertragspartner in Europa**
  - Folge: Downstream-Zugriffsrisiko durch NSA ist reduziert
    - Downstream = Zugriff "at-rest"-Daten von gesuchten Konten
- Wir wählen als **Speicherstandort Europa**
  - Folge: Klingt gut, nutzt aber nur in wenigen Fällen

Falls er einer Gesellschaft in Europa gehört

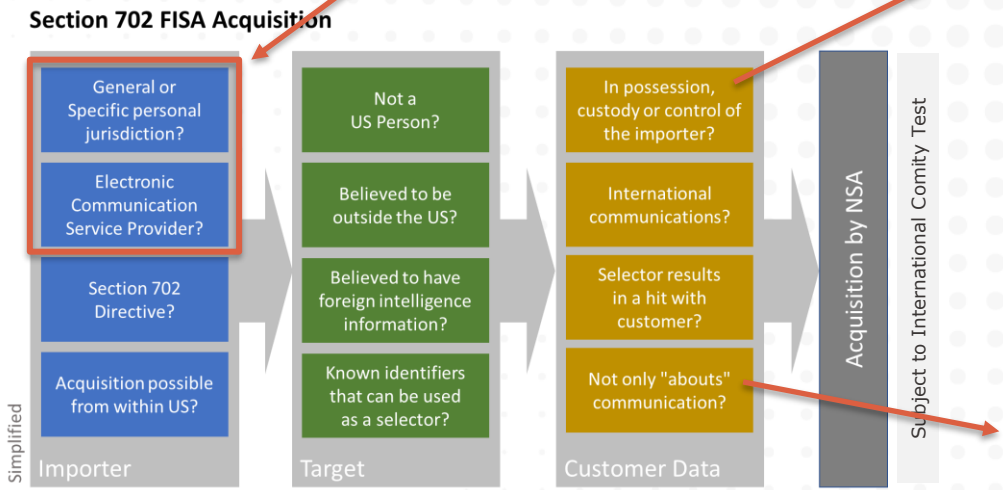
Falls in einem Land mit Sonderschutz (z.B. CH)

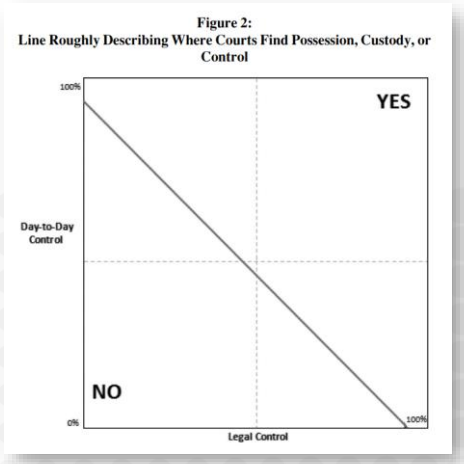
- Wir verhindern **im Tagesgeschäft Zugriffe aus den USA**
  - Folge: Downstream-Zugriffsrisiko durch NSA ist reduziert

Art. 271 StGB hat sich als sehr wirksam erwiesen

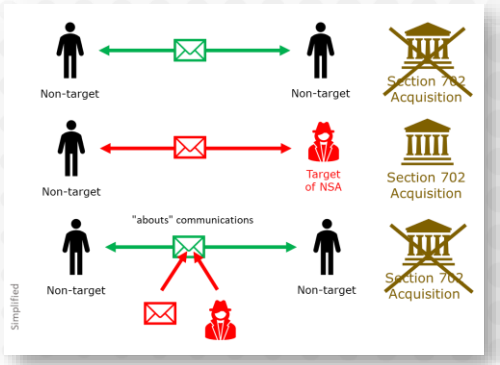
Warum sie wirken

Die EU-Datenschützer kennen/interessieren i.d.R. nur diese beiden Kriterien





Quelle: Justin Hemmings, Sreenidhi Srinivasan, Peter Swire, Defining the Scope of "Possession, Custody, or Control" for Privacy Issues and the CLOUD Act, in: Journal of National Security Law & Policy, Vol. 10 No. 3 vom 23. Januar 2020 (https://bit.ly/3i2xfC9)



Detaillierte Ausführungen in Q29 meiner FAQ: https://bit.ly/3wGjRup

VISCHER

Wie wir sie beurteilen

Excel: https://bit.ly/3EZO38T
FAQ: https://bit.ly/3wGjRup

Step 4: Assess the risk of prohibited lawful access in the target jurisdiction[9]

Country-specific! The following factors have been drafted for ***US law*** *; amend as necessary for other jurisdictions.*

		Probability†	Probability of possibility of a (successful)	Reasoning
a)	Assess the probability that during the assessment period, the following *legal arguments* will prevent the local authorities in the target jurisdiction from successfully forcing the data importer/recipient to disclose personal data at issue under the ...			
	The data importer/recipient is no "Electronic Communications Service Provider"[11] with regard to the processing of personal data at issue and, thus, out of scope of the relevant laws	40%	60.00%	*The parent company may ... as a ECSP for its US custom... in terms of the services provided to its European subsidiary, it is only providing support services, and will in our view not qualify as an ECSP with regard to such activities. Hence, it would in our view not be subject to the relevant laws with regard to the European data to which it has access. We understand that this argument may not be shared by others, which is why we rate it very conservatively to be on the safe side*
	The data importer/recipient has no possession, custody or control over the personal data at issue in clear text and can, thus, not be (successfully) ordered to provide or search it in clear text under the relevant laws[12]	60%	40.00%	*The parent company has no possession or custody of the customer data, as it is stored in the data centers of its European subsidiary. We also believe that it has no legal or day-to-day control over the customer data, as it is granted access only on a case-by-case-basis in selected support cases and only if the customer approves ("lockbox"). The data is encrypted with access permitted in principle only by the customer's own users, not the provider. Under its contract with its European subsidiary, too, the parent is legally not permitted to access unencrypted customer data without prior ...*
	The transfer of the personal data at issue ... personal data will be considered communi... person located in the United States or a US... be "intentionally targeted" by the US autho... relevant laws, but such targeting would occ... and, thus, prevent such a request[13]			
	Performing a prohibited lawful access wou... exporter's or other applicable foreign law i... permitted under the US law doctrine of inte... thus, prevents such a request[14]			
	There are other legal grounds under US law... prohibited lawful access to occur in the pre...			
b)	Is the data importer/recipient contractually ... personal data at issue against lawful access attempts?[16]	Yes	100.00%	*the parent company.*

Wir schätzen, wie überzeugend ein Argument ist, mit welchem der Provider einen Behördenzugriff mit Erfolg zurückweisen können wird oder es gar nicht dazu kommt (z.B. Chance 40:60)

Probability that legal arguments fail to prevent foreign lawful access: †††	19.20%
Overall probability of a lawful access prohibited under applicable data protection laws:	0.38%
In view of the TIA parameters, the residual risk of prohibited lawful access is:	**acceptable**
Number of years it takes for a lawful access to occur at least once with a *90 percent* probability:	2'992
Number of years it takes for a lawful access to occur at least once with a *50 percent* probability:	901
... assuming that the probability neither increases nor decreases over time (like tossing a coin)	

during the assessment period

Die Wirksamkeit der rein rechtlichen Argumente (= Rechte-basierter Ansatz)

Die Wahrscheinlichkeit, dass *alle* Voraussetzungen, die es für einen erfolgreichen Behördenzugriff braucht, im konkreten Fall zusammen erfüllt sind (= risikobasierter Ansatz)

Ist die Methode anerkannt?

- Gutachten der Schweizer Bundeskanzlei: **"Gute Praxis"**
- Regierungsrat Kanton Zürich: Zum Kantons-"Standard" erklärt
- Schweizer Strafverfolgungsbehörde: "geeignetes Kriterium"
- In der Schweiz etabliert, international ebenfalls im Einsatz
  - Schweizer Banken und andere Berufsgeheimnisträger
  - Provider (z.B. Zoom)
  - Öffentliche Institutionen (z.B. holländische Regierung)
  - Allerdings ist ihr Einsatz nicht ganz trivial …
- **Kritisch:** Eidgenössischer Datenschutz- und Öffentlichkeits-Beauftragter (EDÖB), einzelne kantonale Datenschützer in der Schweiz (z.B. Zürich: Auch "bei 0,0001 Prozent" geht es nicht)

Und wo liegt nun das Problem?

- Gemäss der (aktuellen) Haltung der EU-Datenschutzbehörden muss die **Zugriffswahrscheinlichkeit Null** sein
  - Es bleibt unklar, was genau sie damit meinen …
  - 2021 hatten sie den risiko-basierten Ansatz noch akzeptiert, einigten sich aber im Zuge der Task-Force zur Behandlung der 101 NOYB-Beschwerden (Google Analytics) auf den neuen Kurs
- **Begründung:** "Schrems II" verlange dies; der Wortlaut von Kapitel V DSGVO sehe keinen risiko-basierten Ansatz vor
  - Lehre sieht es anders; schon der Begriff des Personendatums ist risikobasiert – und ohne Personendatum keine Übermittlung
  - Da es kein Null-Risiko gibt, wären Datenexporte meist verboten
- **Kaum Enforcement** – die **Gerichte** werden es lösen müssen

… oder der EO 14086 tut es

Diverse Fragen bleiben offen – was wird der EuGH zum EO sagen?

- Dekret des US-Präsidenten vom 7. Oktober 2022
  - Soll in "Schrems II" identifizierte **Defizite** im Rahmen der "signals intelligence" der US-Nachrichtendienste **beheben**
  - Führt u.A. unabhängige Beschwerdestelle für betroffene Personen aus "qualifying states" (z.B. EU) ein
  - Gilt nur, wenn Übermittlungen in die USA erlaubt werden
- USA lanciert **"Privacy Shield"-Nachfolger**, auf dessen Basis Übermittlungen in die USA wieder möglich sein sollen
  - Angemessenheitsbeschluss vermutlich im Frühjahr 2023
- Tangiert Übermittlungen auf Basis der EU SCC nur indirekt
  - Entscheidend wird die Haltung der Datenschutzbehörden sein, da der Exporteur weiterhin in der Pflicht bleibt

Der Druck, dies als gesichtswahrenden Ausweg aus der Sackgasse zu nutzen ist IMHO hoch …


Presidential Documents

Executive Order 14086 of October 7, 2022

Enhancing Safeguards for United States Signals Intelligence Activities

The President

Wirkung auf EU SCC Transfers bis "Schrems III"?


Presidential Documents

EO 14086

EU Datenschutzbehörden

"Wirksam"
IMHO 70% Chance*

- Nur noch ein pro-forma TIA nötig, sobald die EU ein "qualifying state" und der EO implementiert ist (1 Jahr)
- Exporteur bleibt formal im Risiko, weil ein Beschluss der Kommission betr. Angemessenheit nur Transfers an unter den EU-U.S. DPFP zertifizierte Betriebe erfasst

"Teilwirksam"
IMHO 25% Chance*

- Bestimmte Massnahmen bleiben für die USA nötig (z.B. "in-transit"-Verschlüsselung), weil der Sache nicht voll vertraut wird bzw. Teilaspekte wie z.B. die "bulk collections" ihnen nach wie vor zu weit gehen
- Weiterhin ein reduziertes TIA erforderlich

"Unwirksam"
IMHO 5% Chance*

- Weiterhin ein normales TIA erforderlich, selbst im Falle eines Angemessenheits-beschlusses
- Würden sie es durchsetzen?

Für Berufs- und Amtsgeheimnisse ändert sich jeweils nichts → TIA nötig

* Persönliche Einschätzung, bezogen auf die Haltung der EU-Datenschutzbehörden (sie ist für das Risiko bei Verwendung der EU SCC relevant, weil eine solche Verwendung formal von einem DPFP-Angemessenheitsbeschluss nicht erfasst wäre); ich gehe davon aus (und hoffe), dass sich die Behörden taktisch verhalten werden.

Lösung für Nr. 2

Vereinfachtes TIA: https://bit.ly/3EZO38T

- Prinzip von "Schrems II" gilt auch **für alle anderen Staaten**
  - Oft grössere Defizite als USA; Prüfbogen: https://bit.ly/3EZO38T
  - Falls Defizite bestehen: Grund zur Annahme eines Zugriffs?
- **Realität:** Risikobasierte Compliance
  - Hohe Kosten für international tätige Firmengruppen; mehrheitlich Pseudo-TIAs bzw. vereinfachte TIAs für harmlose Fälle im Einsatz
  - Daran denken: Ausnahmen nach Art. 49 DSGVO
    - Ausdrückliche Einwilligung (eher schwierig, aber möglich)
    - Vertragsabwicklung (z.B. Arbeitsvertrag bei HR-Daten)
    - Geltendmachung und Ausübung von Rechtsansprüchen
  - Datenschutzbehörden fokussieren derzeit auf **Big-Tech und USA**

Schlussbemerkungen


DIGITALWIRTSCHAFT IN DER EU

So war die DSGVO nicht gemeint

VON STEFAN BRINK, HAN OETJEN, ROLF SCHWARTMANN UND AXEL VOSS

AKTUALISIERT AM 18.07.2022 - 14:14

Quelle: FAZ (https://bit.ly/3EKEfzo)

- Wir würden das viele Geld besser in **mehr Cybersecurity** investieren als Phantome zu jagen
  - 46% der deutschen Unternehmen wurden binnen zwölf Monaten Opfer eines Cyberangriffs (Quelle: Statista, Mai 2022, https://bit.ly/3EJx0aU)
- Wir haben im Datenschutz das **Ziel aus den Augen verloren**
  - Extremismus der EU-Behörden schadet der Sache und Europa
  - EU-U.S. DPF als ihr Rettungsanker in einem politischen Spiel
- Wirtschaft kommt ohne **risikobasierte Compliance** nicht aus
  - Daten-Regionalisierung wird zunehmen
  - Immer mehr nicht-europäische Datenschutzgesetze müssen adressiert werden (vgl. SCC und TIA-Erfordernisse aus China)

VISCHER

Danke für Ihre Aufmerksamkeit!

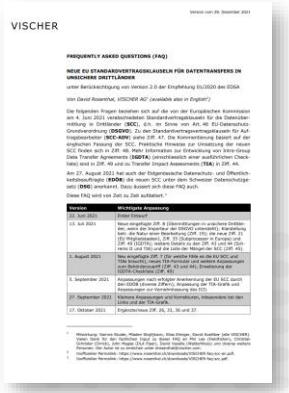
Fragen: drosenthal@vischer.com

Zürich
Schützengasse 1
Postfach
8021 Zürich, Schweiz
T +41 58 211 34 00

Basel
Aeschenvorstadt 4
Postfach
4010 Basel, Schweiz
T +41 58 211 33 00

Genf
Rue du Cloître 2-4
Postfach
1211 Genf 3, Schweiz
T +41 58 211 35 00

www.vischer.com

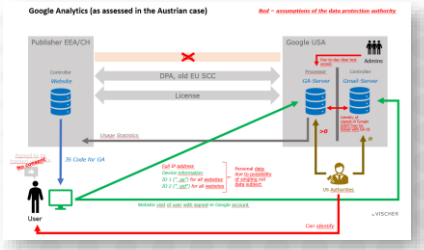

VISCHER

FREQUENTLY ASKED QUESTIONS (FAQ)

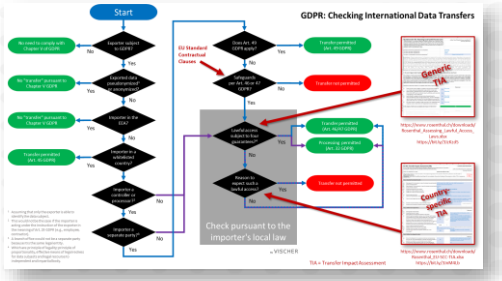
NEUE EU STANDARDVERTRAGSKLAUSELN FÜR DATENTRANSFERS IN UNSICHERE DRITTLÄNDER

Umfangreiche FAQ zu EU SCC:
https://bit.ly/3T62NH9

Noch mehr kostenloses Material auf www.rosenthal.ch



Google Analytics legal einsetzen:
https://bit.ly/3yK8vX7



TIA Toolbox mit vielen Hilfsmitteln:
https://bit.ly/3EZO38T