VISCHER

Schrems II.

International Data Transfer Update

David Rosenthal
June 28, 2021

Schrems II

- **European Court of Justice** (ECJ) on July 16, 2020, publishes its decision C-311/18 ("Schrems II")
  - Approval of Privacy Shield lifted → PS no longer relevant
  - Use of standard contractual clauses (SCC) confirmed, but additional measures are required
- **European Data Protection Board** (EDPB)
  - Adopted an opinion on additional measures on November 10, 2020, then release 2.0 on June 18, 2021
  - Initially, the EDPB took a "no risk" approach
  - Now, risk based transfers are possible, but a detailed transfer impact assessment (TIA) is necessary
- **European Commission** released new SCC on June 4, 2021

Key EDPB Requirement | 1

Alternatively, you may decide to proceed with the transfer without being required to implement supplementary measures, if you consider that you have no reason to believe that relevant and problematic legislation will be applied, in practice, to your transferred data and/or importer. You will need to have demonstrated and documented through your assessment, where appropriate in collaboration with the importer, that the law is not interpreted and/or applied in practice so as to cover your transferred data and importer, also taking into account the experience of other actors operating within the same sector and/or related to similar transferred personal data and the additional sources of information described further below.[53]

Therefore, you will need to have demonstrated and documented with a detailed report[54] that problematic legislation will not be applied in practice to your transferred data and/or importer, and, consequently, that it will not prevent the importer from fulfilling its obligations under the Article 46 GDPR transfer tool.[55]

EDPB Recommendation 01/2020, Para. 43.3

Key EDPB Requirement | 2

Problematic legislation is understood as legislation that

1) imposes on the recipient of personal data from the European Union obligations and/or affect the data transferred in a manner that may impinge on the transfer tools' contractual guarantee of an essentially equivalent level of protection and
2) does not respect the essence of the fundamental rights and freedoms recognised by the EU Charter of Fundamental Rights or exceeds what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in Union or EU Member States' law, such as those listed in Article 23 (1) GDPR.

Foreign Lawful Access

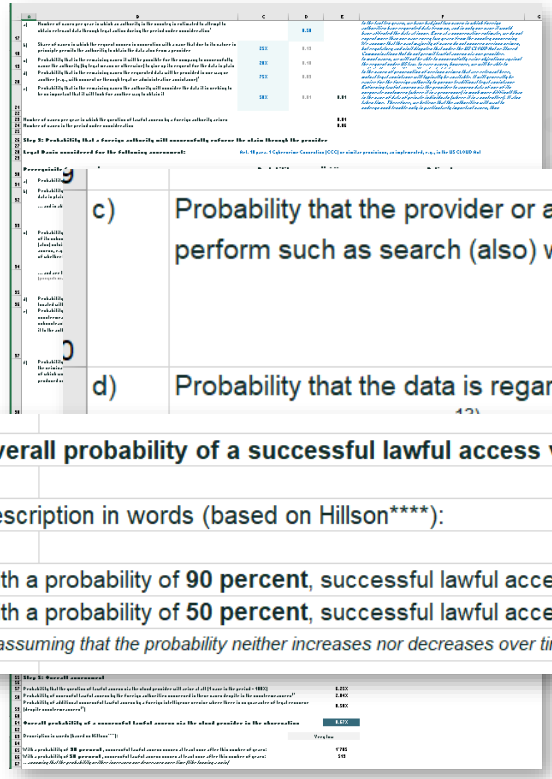
Without the possibility to appeal before an independent court of justice

=

Sec. 702 FISA
+ EO 12.333

EDPB Recommendation 01/2020, Footnote 50

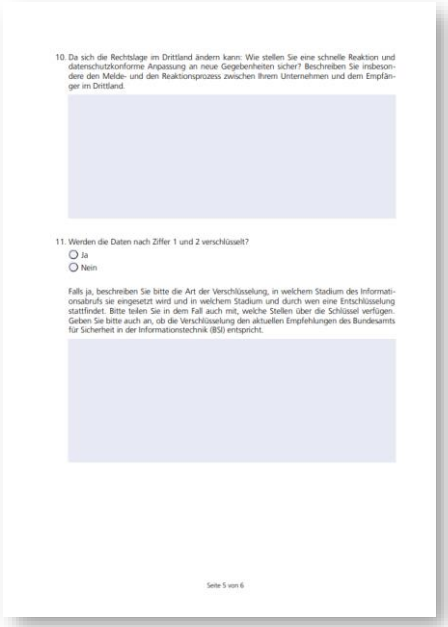
Covers foreign lawful access with/without legal recourse



c)	Probability that the provider or a subcontractor in the country above may be legally required to perform such as search (also) with the company's data[12)]	30%
d)	Probability that the data is regarded as content that it is typically the subject of intelligence	

61	**Overall probability of a successful lawful access via the cloud provider in the observation period:*** **	0.67%
62		
63	Description in words (based on Hillson****):	Very low
64		
65	With a probability of **90 percent**, successful lawful access occurs at least once after this number of years:	1'705
66	With a probability of **50 percent**, successful lawful access occurs at least once after this number of years:	513
67	*… assuming that the probability neither increases nor decreases over time (like tossing a coin)*	

https://www.rosenthal.ch/downloads/Rosenthal_Cloud_Lawful_Access_Risk_Assessment.xlsx



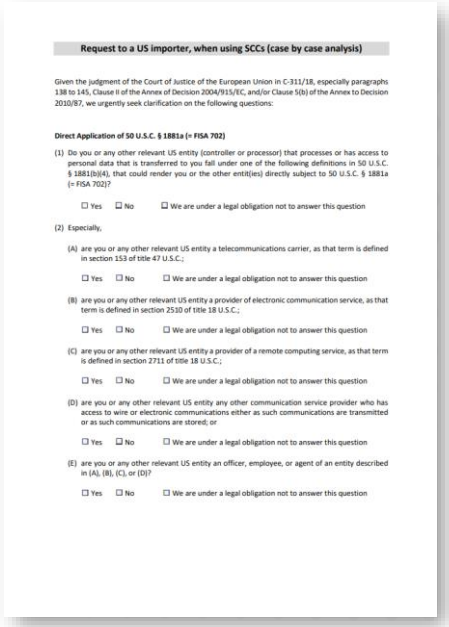
10. Da sich die Rechtslage im Drittland ändern kann: Wie stellen Sie eine schnelle Reaktion und datenschutzkonforme Anpassung an neue Gegebenheiten sicher? Beschreiben Sie insbesondere den Melde- und den Reaktionsprozess zwischen Ihrem Unternehmen und dem Empfänger im Drittland.

11. Werden die Daten nach Ziffer 1 und 2 verschlüsselt?

◯ Ja
◯ Nein

Falls ja, beschreiben Sie bitte die Art der Verschlüsselung, in welchem Stadium des Informationsabrufs sie eingesetzt wird und in welchem Stadium und durch wen eine Entschlüsselung stattfindet. Bitte teilen Sie in dem Fall auch mit, welche Stellen über die Schlüssel verfügen. Geben Sie bitte auch an, ob die Verschlüsselung den aktuellen Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) entspricht.

Seite 5 von 6



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,

(A) are you or any other relevant US entity a telecommunications carrier, as that term is defined in section 153 of title 47 U.S.C.;

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

(B) are you or any other relevant US entity a provider of electronic communication service, as that term is defined in section 2510 of title 18 U.S.C.;

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

(C) are you or any other relevant US entity a provider of a remote computing service, as that term is defined in section 2711 of title 18 U.S.C.;

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

(D) are you or any other relevant US entity any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; or

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

(E) are you or any other relevant US entity an officer, employee, or agent of an entity described in (A), (B), (C), or (D)?

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

Main advice of data protection authorities is to keep personal data in Europe or otherwise fully encrypt it before exposing it

https://www.lda.bayern.de/de/thema_schrems2_pruefung.html
https://noyb.eu/files/CJEU/EU-US_form_v3_nc.pdf

EU Standard Contractual Clauses | 1

UK exports not covered!

- Two versions: International transfers + data processing
- New SCC have to be customized (cannot be signed as such)
  - Select the transfer scenario and certain options
  - Complete description of transfer, of technical and organisational measures of data security and of subprocessors
  - Agree on further terms
- Beware: SCC cannot be changed or overruled
  - Unlimited liability among parties, third party rights for individuals
  - Any onward transfer of data is prohibited, unless, *inter alia*, "it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings"

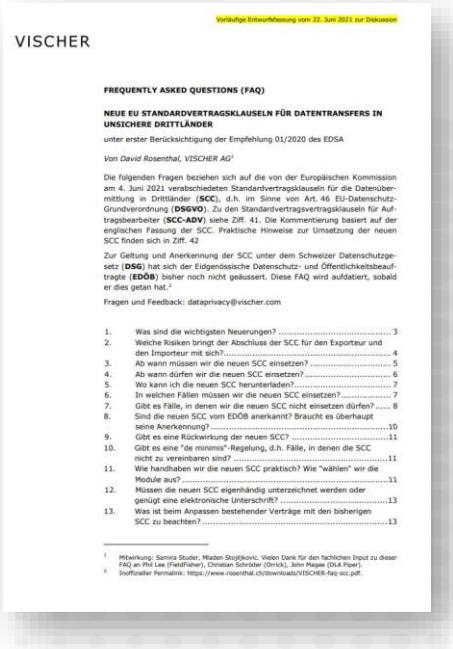
EU Standard Contractual Clauses | 2

- Last date to enter into existing SCC is September 27, 2021
- Any existing SCC will have to be replaced
  - If processing at issue changes following September 27, 2021
  - If personal data is no longer protected sufficiently abroad (in particular from foreign lawful access without guarantee of legal recourse)
  - At the latest by December 27, 2022
- What to do?
  - Determine where SCC are in use today (e.g., with US counsel for eDiscovery, IGDTAs, service providers)
  - Perform a TIA (also required as per the SCC)
  - Enter into the new SCC

VISCHER

Thank you!

FAQ


Vorläufige Entwurfsfassung vom 22. Juni 2021 zur Diskussion

VISCHER

FREQUENTLY ASKED QUESTIONS (FAQ)

NEUE EU STANDARDVERTRAGSKLAUSELN FÜR DATENTRANSFERS IN UNSICHERE DRITTLÄNDER

unter erster Berücksichtigung der Empfehlung 01/2020 des EDSA

Von David Rosenthal, VISCHER AG[1]

Die folgenden Fragen beziehen sich auf die von der Europäischen Kommission am 4. Juni 2021 verabschiedeten Standardvertragsklauseln für die Datenübermittlung in Drittländer (**SCC**), d.h. im Sinne von Art. 46 EU-Datenschutz-Grundverordnung (**DSGVO**). Zu den Standardvertragsvertragsklauseln für Auftragsbearbeiter (**SCC-ADV**) siehe Ziff. 41. Die Kommentierung basiert auf der englischen Fassung der SCC. Praktische Hinweise zur Umsetzung der neuen SCC finden sich in Ziff. 42

Zur Geltung und Anerkennung der SCC unter dem Schweizer Datenschutzgesetz (**DSG**) hat sich der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (**EDÖB**) bisher noch nicht geäussert. Diese FAQ wird aufdatiert, sobald er dies getan hat.[2]

Fragen und Feedback: dataprivacy@vischer.com

[1] Mitwirkung: Samira Studer, Mladen Stojiljkovic. Vielen Dank für den fachlichen Input zu dieser FAQ an Phil Lee (FieldFisher), Christian Schröder (Orrick), John Magee (DLA Piper).
[2] Inoffizieller Permalink: https://www.rosenthal.ch/downloads/VISCHER-faq-scc.pdf.

https://bit.ly/3xTJ2YC (German)
https://bit.ly/3dhwaDB (English)

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