VISCHER

Cross-Border Data Transfers.

Challenges for companies (and how to deal with them in practice)

David Rosenthal, Partner, VISCHER Ltd.
March 11, 2024

Agenda

- Data Privacy Framework (DPF)
- Other countries
- Solutions for intra-group transfers
- Solutions for provider transfers
- Special cases

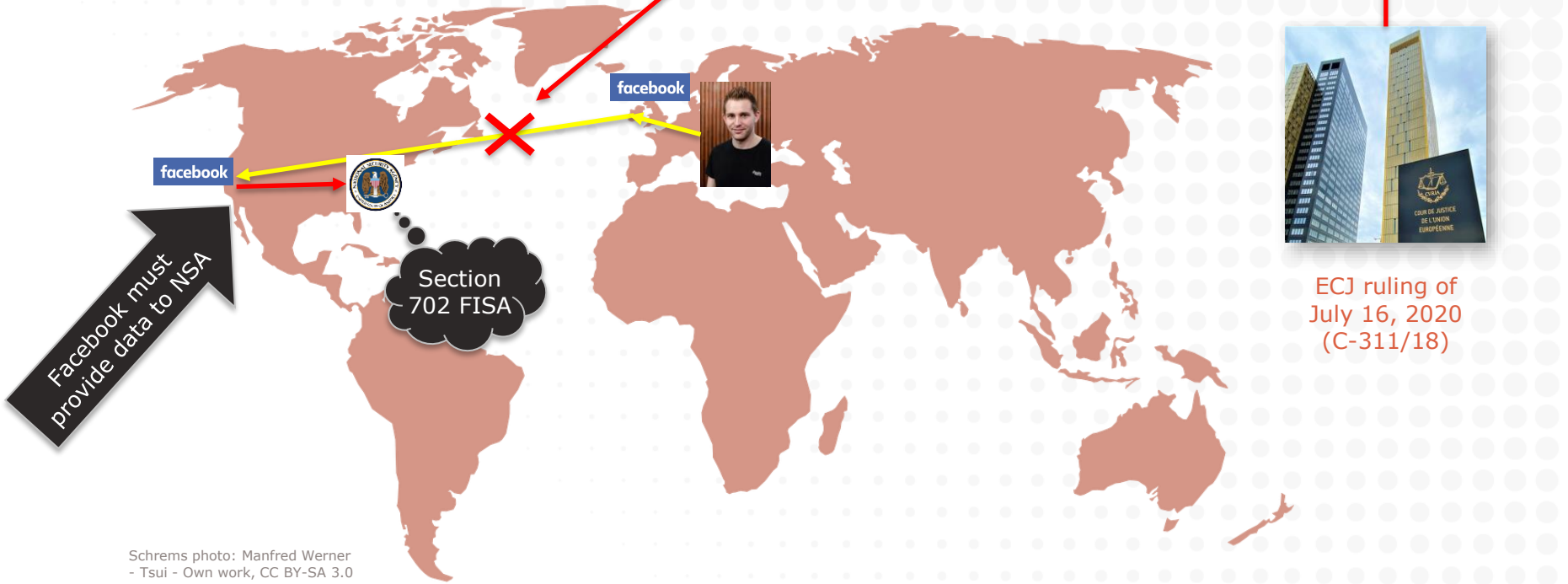
Basics

- **Why are international transfers regulated?**
  - Need to ensure an adequate level of data protection when personal data leaves the "protected zone" of the EEA/UK/CH
- **How do we ensure this?**
  - Some countries are recognized as providing an adequate level of data protection (by the Federal Council and EC) → no problem
  - For all other countries:
    - EU Standard Contractual Clauses (of 2021) → most common
    - Binding Corporate Rules (Processor, Controller) → rare
    - Explicit consent → online (warning, voluntariness, revocation)
    - Performance of contract with/for data subject (e.g., employees)
    - Foreign legal proceeding (civil, criminal, administrative)

CH: Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, ~~Japan~~, Jersey, New Zealand, ~~Republic of Korea~~, the United Kingdom and Uruguay, ~~Data Privacy Framework~~

"Schrems II"

Data transfer is inadmissible because access by the NSA is to be assumed under a piece of law that does not guarantee the necessary protection of data subjects (and cannot be prevented)



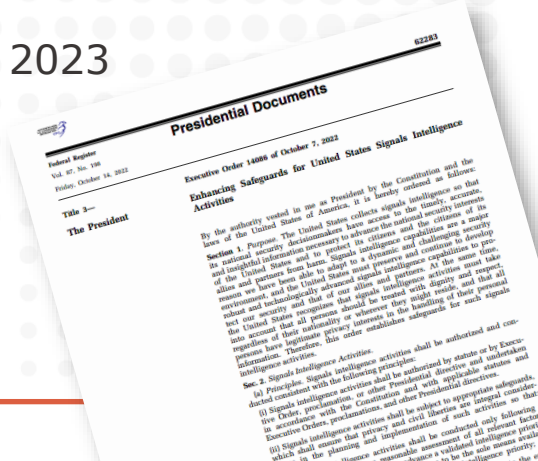
ECJ ruling of July 16, 2020 (C-311/18)

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

The (political) solution for the US

Various questions remain open - what will the ECJ say about the EO and the Adequacy Decision?

- **Executive Order** of the US President of October 7, 2022
  - Intended to address the legal **deficiencies** identified in "Schrems II" with regard to "signals intelligence" undertaken by the U.S.
  - Establishes independent redress mechanism for data subjects ("DP Review Court") from "qualifying states" (e.g., EEA, UK)
  - Says that signals intelligence will be done only "proportionate"
- **Adequacy Decision** of European Commission on July 10, 2023
  - Transfer of personal data to US recipient is permitted if recipient is self-certified under "Data Privacy Framework"
  - The EU-US DPF provides for a set of privacy rules that company can publicly promise to comply with; if they breach them, they can be sued


Federal Register / Vol. 87, No. 198 / Friday, October 14, 2022 / Presidential Documents

62283

Title 3—

The President

Executive Order 14086 of October 7, 2022

Enhancing Safeguards for United States Signals Intelligence Activities

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose. The United States collects signals intelligence so that its national security decisionmakers have access to the timely, accurate, and insightful information necessary to advance the interests of the United States and to protect its citizens and the citizens of its allies and partners from harm. Signals intelligence capabilities are a major reason we have been able to adapt to a dynamic and challenging security environment, and the United States must preserve and continue to develop robust and technologically advanced signals intelligence capabilities to protect our security and that of our allies and partners. At the same time, the United States recognizes that signals intelligence activities must take into account that all persons have legitimate privacy interests in the handling of their personal information. Therefore, this order establishes safeguards for such signals intelligence activities.

Sec. 2. Signals Intelligence Activities.

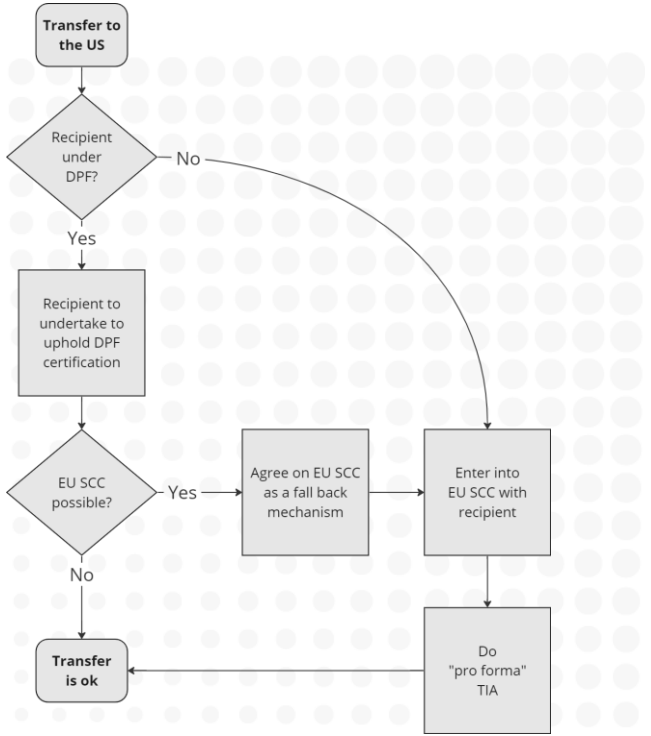
(a) Principles. Signals intelligence activities shall be authorized and conducted consistent with the following principles:

(i) Signals intelligence activities shall be authorized by statute or by Executive Order, proclamation, or other Presidential directive and undertaken in accordance with the Constitution and with applicable statutes and Executive Orders, proclamations, and other Presidential directives.

(ii) Signals intelligence activities shall be subject to appropriate safeguards, which shall ensure that privacy and civil liberties are integral considerations in the planning and implementation of such activities so that

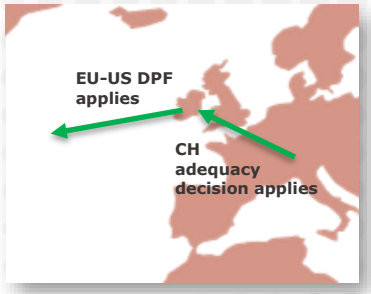
The (political) solution for the US

- **Two mechanisms** for transfer personal data
  - EC adequacy decision for EU-US DPF *or*
  - EU SCC + "pro forma" TIA
- The **TIA** for the US can be based on same considerations as the EC adequacy decision
  - https://www.rosenthal.ch/downloads/VISCHER-TIA-USA-EO14086.docx
- EO 14086 applies to **all** transfers from EEA to US
  - CJEU will likely scrutinize level of protection granted by EO 14086 → "Schrems III"
  - We recommend always also entering into the EU SCC as a backup (and because of its clauses)

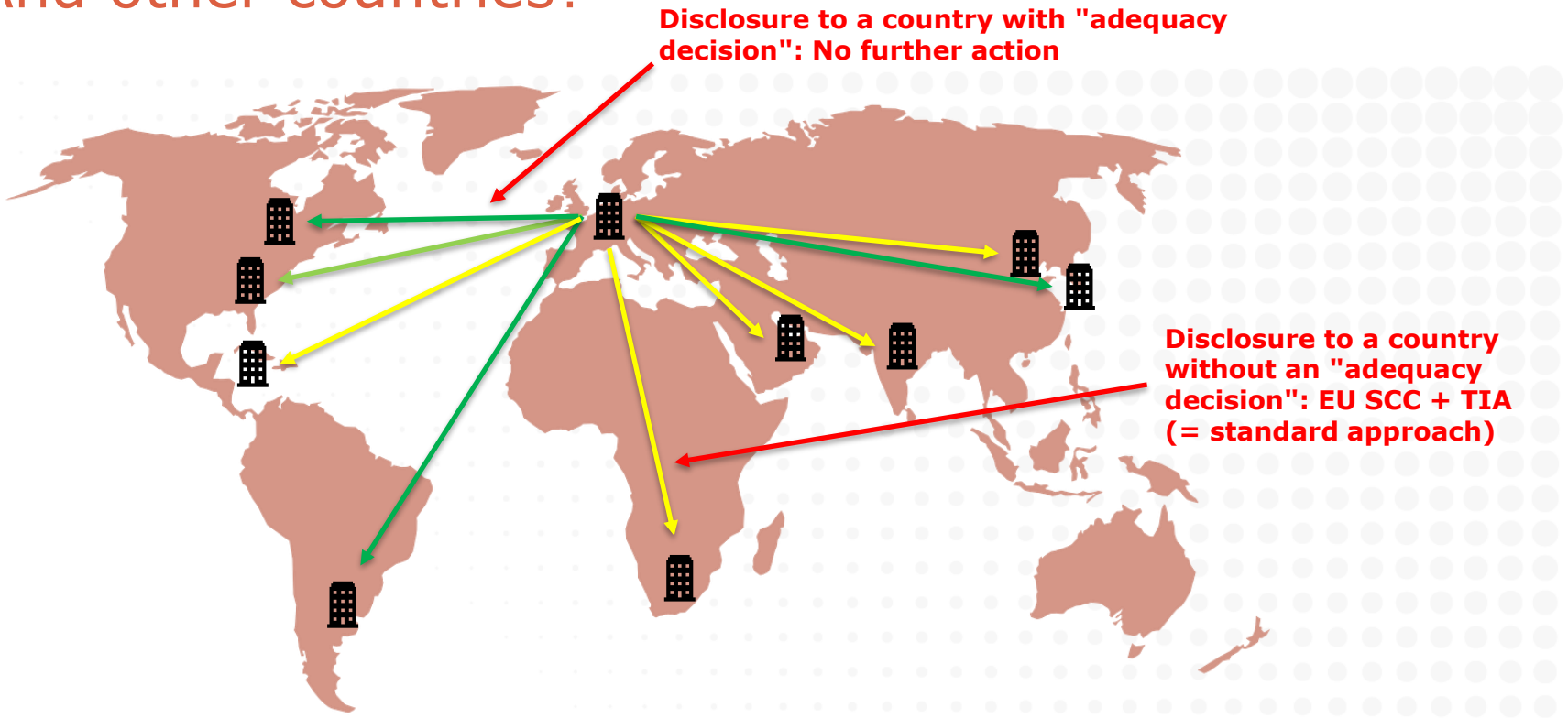


And what about Switzerland?

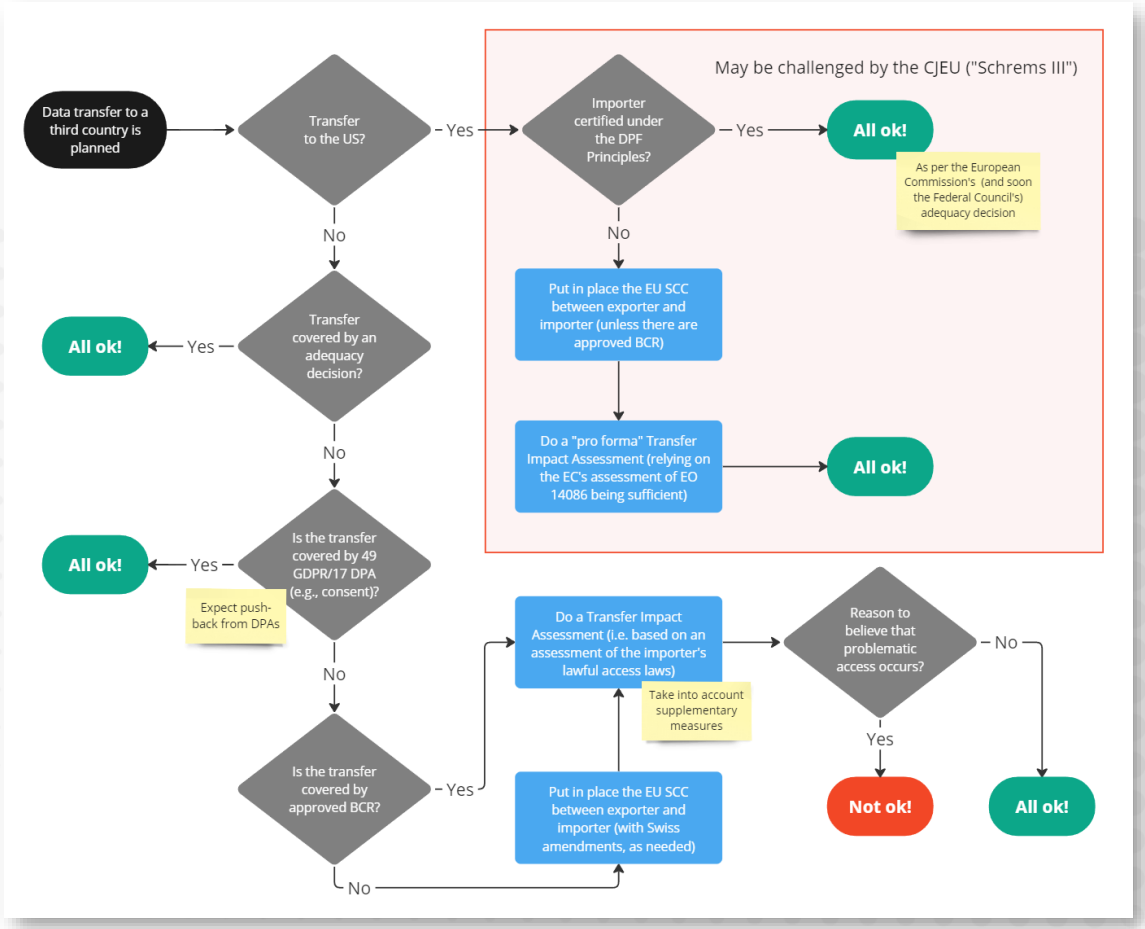
- **Next step:** U.S. Attorney General will have to determine that Switzerland is a "qualifying state" under EO 14086
  - U.S. currently evaluating Swiss level of data protection …
  - Once we are qualified, a pro-forma TIA will be sufficient for U.S. transfers where they rely on the EU SCC (same as with GDPR)
  - Thereafter: Federal Council will amend Ordinance with **adequacy decision** for transfers to US entities with CH-US DPF certification
- What to do **until then**?
  - Transfer personal data to U.S. under a "risk-based approach"
  - Transfer personal data to U.S. with stop-over in the EEA
    - All three large hyperscalers do this anyway; you can use our template (2nd page) as an annex to your TIA



And other countries?



How to do cross-border data transfers

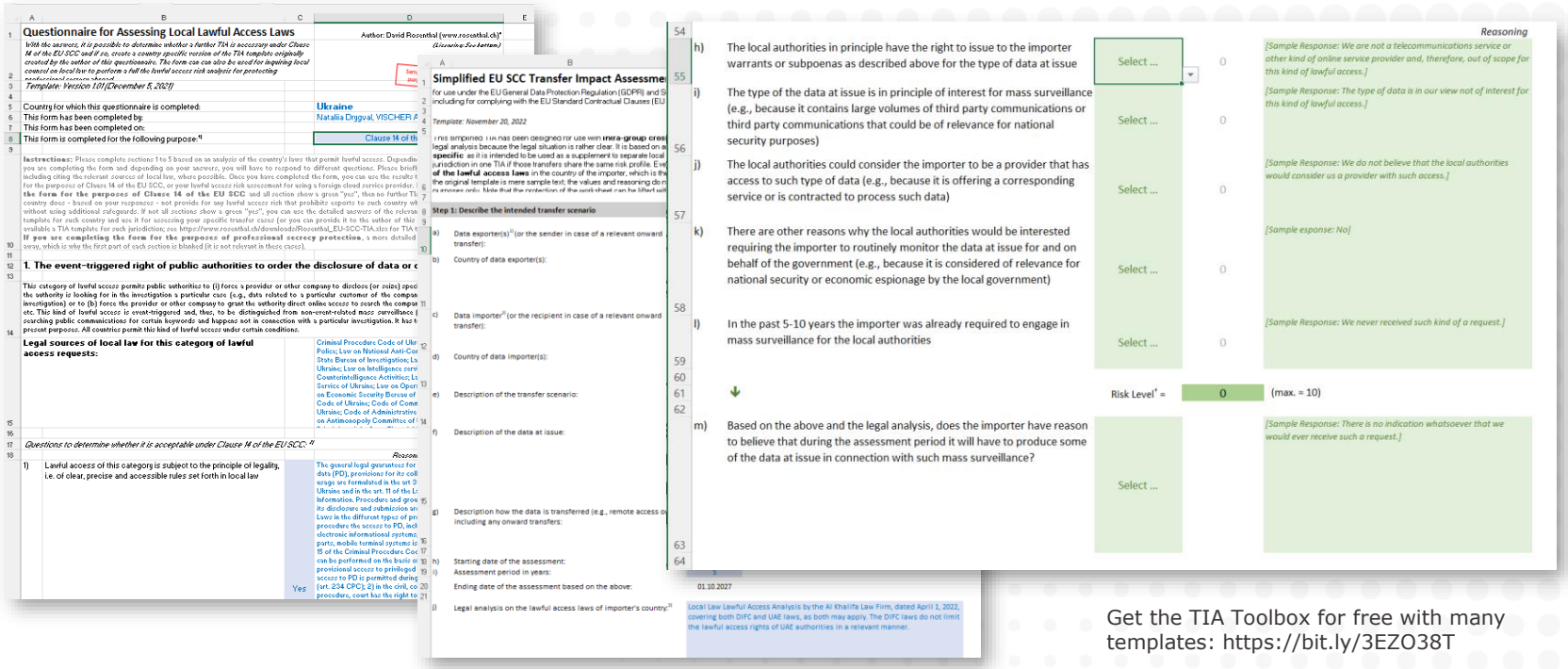


How to do a Transfer Impact Assessment

- There are **three options** in practice
- **Option A:** Do a full transfer impact assessment
  - Ext. costs usually about CHF 2-15k, incl. local counsel
  - Preferred choice for sensitive/critical transfers
- **Option B:** Do a "simplified" transfer impact assessment
  - Ext. costs usually about CHF 1-7k, incl. local counsel, if needed
  - Preferred choice for group internal transfers
- **Option C:** Do nothing
  - May result in fines under both the GDPR and Swiss DPA

Watch out, there are a lot of very poor transfer impact assessments on the market that do not address the issue and will not give you much protection

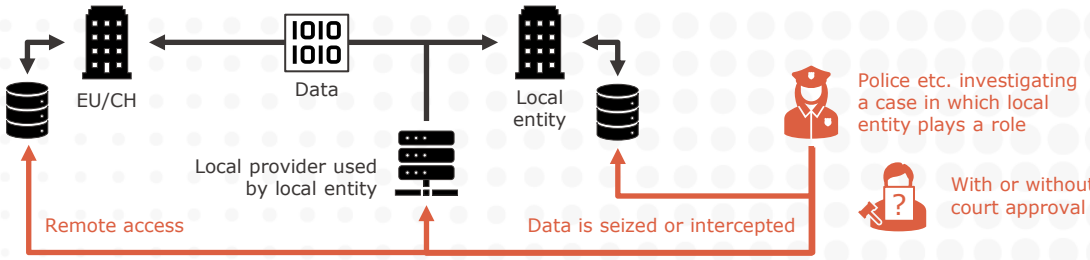
Simplified TIA



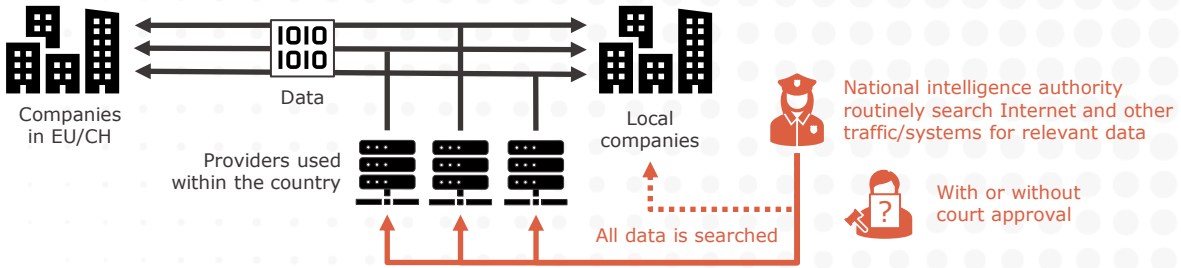
Get the TIA Toolbox for free with many templates: https://bit.ly/3EZO38T

Consider the three forms of lawful access

Targeted lawful access (investigations)



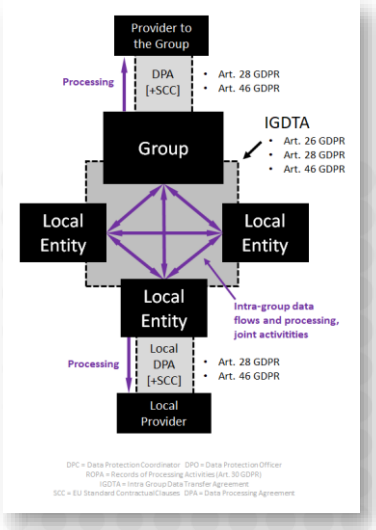
Non-targeted lawful access (mass surveillance)

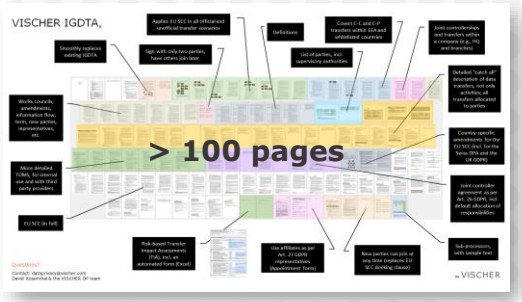


Self-reporting obligations

Solutions for intra-group transfers

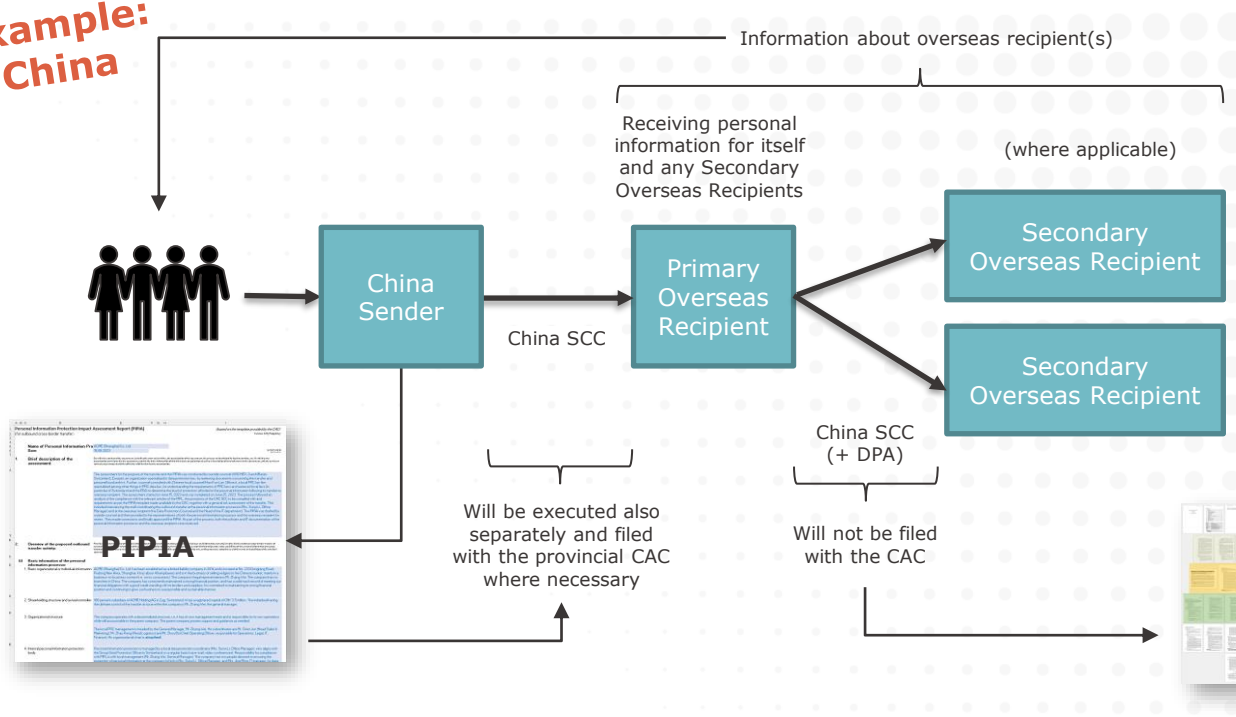
- **The issue**
  - Cover cross-border transfers with EU SCC, with amendments
  - Cover group-internal processors (with a DPA) and controllers
  - Cover joint controllerships with a joint controller agreement
  - Regulate branch transfers, local representative, TIA etc.
  - Cover not only the GDPR/DPA, but also all local DP laws
  - Amendments with no repapering
- **The solution**
  - Intra-Group Data Transfer Agreement (IGDTA)
  - Multiparty agreement that governs any internal personal data transfer (but does not trigger transfers)





On the rise: European inbound data regulations

Example: China



Some features of the China SCC:

- Strict conditions for onward transfers abroad
- Third-party beneficiary rights
- PRC law as governing law
- Re-filing and assessment in case of changes of contract or the processing (incl. duration)

Intra-Group Data Transfer Agreement (IGDTA), a multi-party agreement governing all personal data transfers within a group

Solutions for provider transfers

- **The issue**
  - Most cloud providers (incl. Microsoft, AWS and Google) depend to some extent on U.S. access to their EEA or Swiss data centers
  - Requires the conclusion of the EU SCC (absent DPF or as backup)
- **The solution**
  - Option A: Do nothing, rely only on DPF → not recommended
  - Option B: Have the EU SCC (i.e. module 3) entered into by the European subsidiary (e.g., Microsoft, Google)
    - For liability reasons, they will often primarily rely on the DPF
  - Option C: Have the EU SCC entered into by the client directly with US parent of the provider (e.g., AWS) → not recommended

Some special cases

- **Home office or branches abroad**
  - Technically no GDPR transfer, but duty to protect remains
- **Cross-border joint controllerships**
  - Swiss joint controller is not subject to the GDPR, but usually bound by contract; onward transfers are subject to the GDPR
- **Art. 271 Swiss Penal Code**
  - Prohibits access to data on Swiss territory by foreign authorities incl. for foreign proceedings, with the Federal Tribunal having taken a rather restrictive position (see vischerlnk.com/3wL1l6W)
- **Professional and Official Secrecy**
  - Stricter standards regarding foreign lawful access than under data protection law; additional measures & assessments needed

Conclusion

- Even with the adequacy decision for transfers to the U.S. in place and valid, international data transfers often remain a burden for international groups of companies that are active in countries without an "adequate" data protection or own, materially deviating requirements
- The issues can be solved, at least with a risk-based approach, but this comes with a compliance cost

VISCHER

Thank you for your attention!

Questions: drosenthal@vischer.com

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

www.vischer.com

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

Much more materials are available for free at www.rosenthal.ch