Schrems-2

Changing regulations, practical issues, possible approaches

Magdalena Rzaca
GDPR & IPR Legal Advisor

Géant – EUNIS Cloud Management workshop
1/04/2022

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

Agenda

- Historical context
- Schrems 2 judgement
- Approaches

TERMINOLOGY

- Personal data, Processing
- Schrems I (Safe Harbour)
- Schrems II (Privacy Shield)
- International transfers

Timeline

- 2015 – Safe Harbour invalidated (as a result of a complaint filed by Schrems)
- 2016 – Privacy Shield adopted
- 2020 – Privacy Shield invalidated (Schrems 2 judgement)
- March 2022 – EU-USA statement regarding new mechanism for transfer (minute 41 of https://www.youtube.com/watch?v=Laj8JcLVr2c)

What was the Privacy Shield?

- As a result of Schrems I judgement and invalidation of Safe Harbour, the Privacy Shield was an adequacy decision, adopted on 12 July 2016, allowing the free transfer of data to companies certified in the US under the Privacy Shield:

  https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016D1250&from=EN

- In its judgement of 16 July 2020 the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield (Case C-311/18)

  https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62018CJ0311&from=en)

Schrems II short summary

In its recent judgment C-311/18 (Schrems II) the Court of Justice of the European Union (CJEU) reminds us that the protection granted to personal data in the European Economic Area (EEA) must travel with the data wherever it goes. Transferring personal data to third countries cannot be a means to undermine or water down the protection it is afforded in the EEA. The Court also asserts this by clarifying that the level of protection in third countries does not need to be identical to that guaranteed within the EEA but essentially equivalent. The Court also upholds the validity of standard contractual clauses, as a transfer tool that may serve to ensure contractually an essentially equivalent level of protection for data transferred to third countries.

Standard contractual clauses and other transfer tools mentioned under Article 46 GDPR do not operate in a vacuum. The Court states that controllers or processors, acting as exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. In those cases, the Court still leaves open the possibility for exporters to implement supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law. The Court does not specify which measures these could be. However, the Court underlines that exporters will need to identify them on a case-by-case basis. This is in line with the principle of accountability of Article 5.2 GDPR, which requires controllers to be responsible for, and be able to demonstrate compliance with the GDPR principles relating to processing of personal data.

Schrems II - the problem

In the Schrems II judgment, the CJEU highlighted that:

- The SCCs remain valid, while making international transfers there is a need to verify in advance that the personal data being transferred will be properly protected.
- The **EU-U.S. Privacy Shield is invalid** because the U.S. state surveillance powers are not properly circumscribed. In particular, the Ombudsman mechanism does not provide sufficient protection for EU citizens.

The EU-US Privacy Shield is therefore **no longer a valid mechanism to transfer personal data** from the EU to the US.

The core problem: international transfers of personal data

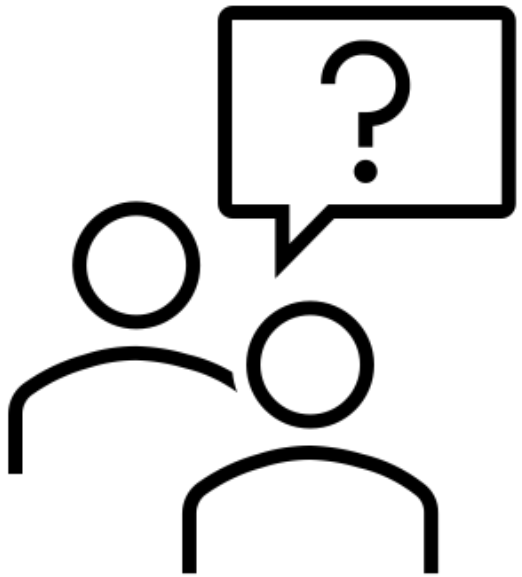
- A transfer of personal data to a third country or an international organization may take place where the Commission has decided that the third country (…) in question ensures an adequate level of protection (art. 45 GDPR)
- Very limited number of countries deemed as ensuring an adequate level of protection: Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay (ongoing: South Korea & UK)

International transfers – appropriate safeguards

- In the absence of adequacy decision, a controller or processor may transfer personal data to a third country only if the controller or processor has provided **appropriate safeguards** (art. 46 GDPR).
- The appropriate safeguards may be provided for by (…):
  - binding corporate rules;
  - **Standard Contractual Clauses;**
  - an approved code of conduct (…).

Implications of invalidation of the Privacy Shield

- Lack of adequacy decision allowing for international transfer of personal data to the USA
- A problem for businesses relying on the Privacy Shield
- Uncertainty regarding engaging US suppliers
- **What to do next?**
- **Evaluate your data and transfers (see https://connect.geant.org/2022/03/02/compliance-made-easy-with-new-gdpr-transfer-guide-for-nrens-on-the-2020-iaas-framework)**



List of actions (**6 steps**)

1) **Know your transfers** – know what personal data you are processing and where data goes to

2) **Verify the transfer tool** your transfer relies on (e.g., SCC, adequacy decision, BCR)

3) **Assess if there is anything in the law or practice of the third country** that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer

4) **Identify and adopt supplementary measures** that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence. This step is only necessary if your assessment reveals that the third country legislation impinges on the effectiveness of the Article 46 GDPR transfer tool you are relying on or you intend to rely on in the context of your transfer (Annex 2 of the EDPB Recommendations 1/2020)

5) **Take any formal procedural steps** the adoption of your supplementary measure may require, depending on the Article 46 GDPR transfer tool you are relying on (e.g., consulting Data Protection Authority)

6) **Re-evaluate at appropriate intervals the level of protection** afforded to the data you transfer to third countries and to monitor if there have been or there will be any developments that may affect it – be vigilant!

What to do when there is international transfer and lack of adequacy decision?

- The data exporter must verify "**on a case-by-case basis**" what protections apply (where appropriate in collaboration with the data importer).
- The judgment states this must include an **assessment** (transfer impact assessment) **of the laws** of the third country, **the existence of any independent supervisory authority** and any **international commitments** made by the country. However, in order to ensure a proper case-by-case assessment it seems likely that a broader legal review would be appropriate.

Transfer Impact Assessment

The assessment shall include the following:

- What personal data is being transferred? How sensitive is it? How much is accessible publicly?
- Where did that personal data originate from?
- What technical measures are used to protect that data? For example, where customer managed encryption keys are used, the ability of third country authorities to access that data will necessarily be limited.
- What national laws apply in that jurisdiction? How are they exercised in practice? How likely are they to be exercised in relation to the specific personal data transfer?

Transfer Impact Assessment is a flexible risk assessment, which needs to be monitored on an ongoing basis and updated in the light of any changes in the laws of the third country.

Actions of the European Data Protection Board

- Standard Contractual Clauses (SCC) were revised, but after the judgement those shall be accompanied by Transfer Impact Assessment
- Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Practical tips for transfers relying on SCC

- Institutions relying both on SCC and the Privacy Shield before July 2020, had still **valid appropriate safeguard** to rely on (SCC while the Privacy Shield was invalidated); each and every transfer: 1) shall be subjected to Transfer Impact Assessment (TIA) and 2) once revised SCC are available – SCC shall be replaced
- In pre-Schrems 2 world SCC were considered as enough, in post-Schrems reality they require additional measures (TIA)
- As far TIA templates are not provided by the Data Protection Authorities neither the EDPB
- Institutions relying solely on the Privacy Shield, need to start from the scratches

Q&A

'The most pressing problem I encounter with Schrems-2 GDPR rules, in my daily work is …?'

Thank you!

www.geant.org