

International Data Transfers Post Schrems-II

Paul Breitbarth
EADPP 2020 Conference
26 November 2020

Paul Breitbarth

TrustArc

Director, EU Policy & Strategy



Senior Visiting Fellow & Member of the Board



Podcast Co-Host

<https://seriousprivacy.buzzsprout.com>

Previously



Senior International Officer



Depute Committee Clerk



Paul Breitbarth

paul.breitbarth@trustarc.com

@EuroPaulB

International Data Transfers post Schrems-II

The Schrems-II Judgment - 16 July 2020 (C-311/18)

The Schrems cases all revolve around the question if personal data from Facebook users can be transferred from Facebook Ireland to Facebook Inc, and if so, what legal safeguards should be put in place. The first arrest saw the annulment (*ex tunc*) of the EU-U.S. Safe Harbour Arrangement. In the second case, the main question was if the data transfers could continue on the basis of Standard Contractual Clauses.

The CJEU determined:

- The exception for national security as included in the EU Treaties does not apply to the data transfers at hand;
- Standard Contractual Clauses are and remain a valid means to transfer personal data to non-EU countries;
- Also when transferring personal data on the basis of appropriate safeguards (i.e. contracts) the level of protection offered to the data needs to be “essentially equivalent” to that in the EU; and
- The Privacy Shield does not meet the “essentially equivalent” standard and is thus declared invalid.

International Data Transfers post Schrems-II

The Schrems-II Judgment - 16 July 2020 (C-311/18)

On the carve-out for national security

The transfer from the EU to a third country is taking place between two commercial entities, in the Schrems-II case between Facebook Ireland and Facebook Inc. in the U.S., and that is a regular transfer that is covered by the provisions of the GDPR. The fact that in theory the data at some point may be intercepted by, or need to be handed over to, intelligence and security services in the U.S., does not make a difference.

International Data Transfers post Schrems-II

The Schrems-II Judgment - 16 July 2020 (C-311/18)

On Privacy Shield

- The Privacy Shield was an agreement between the EU and the U.S. offering an adequate level of data protection. The CJEU determined the level of protection offered by the Privacy Shield was insufficient, because:
 - The applicable U.S. surveillance legislation is not sufficiently clear and transparent for individuals to understand what their data might be subject to;
 - There are insufficient effective means of oversight and redress for EU persons. The instituted Ombudsperson has no effective powers to gain access to personal data processed by the intelligence community, nor can they order compliance.
- Both the EU and Swiss versions of the Privacy Shield can no longer be used as a transfer mechanism.
- The Privacy Shield remains enforceable by the U.S. authorities as an accountability tool, allowing companies to demonstrate compliance with high data protection standards.

International Data Transfers post Schrems-II

The Schrems-II Judgment - 16 July 2020 (C-311/18)

The Essentially Equivalent standard

- The level of protection of natural persons guaranteed by the GDPR can not be undermined by a data transfer.
- The term ‘adequate level of protection’ must be understood as requiring the third country in fact to ensure, by reason of its domestic law or its international commitments, a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union. [*Schrems-I*]
- Also when transferring personal data on the basis of Article 46 GDPR, using appropriate safeguards like Standard Contractual Clauses (SCCs), (...) such appropriate guarantees must be capable of ensuring that data subjects whose personal data are transferred to a third country (...) are afforded, as in the context of a transfer based on an adequacy decision, a level of protection essentially equivalent to that which is guaranteed within the European Union. [*Schrems-II*]

International Data Transfers post Schrems-II

The Schrems-II Judgment - 16 July 2020 (C-311/18)

The Essentially Equivalent standard

- What is the remaining difference between an adequate level of protection and offering appropriate safeguards now both need to lead to an essentially equivalent of protection?
 - Adequacy decisions require a general evaluation of the third country's legislation
 - The contractual appropriate safeguards always apply on a case-by-case basis. In principle, they can have different effects in different situations, also because supplementary safeguards could be implemented.
- For the U.S., offering appropriate safeguards may prove to be difficult, given the judgment of the CJEU regarding the lack of clear and transparent legislation and effective means of oversight and redress.

International Data Transfers post Schrems-II

The Privacy International & La Quadrature du Net Cases – 1 October 2020 (C-623/17, C-511/18, C-512/18 and C-520/18)

- Four joint cases, with two largely overlapping judgments, all revolving around the collection and use of telecoms traffic data (metadata) of cellphones to fight organised crime and terrorism.
- The CJEU determined the legislation in the Member States involved (Belgium, France and the UK) goes beyond what is acceptable according to the EU Charter of Fundamental Rights. The interference with the fundamental rights to privacy and data protection goes beyond what is “proportional and necessary in a democratic society”.
- The CJEU creates new standards for such interferences: the more sensitive and large-scale the data set, the more limited the collection and use of these data may be.
- The cases show the CJEU does not just criticise the level of data protection in third countries, but also within the EU.

International Data Transfers post Schrems-II

The draft EDPB Recommendations on International Transfers: 6 steps

1. Know your transfers - reassess all data processing operations on a case-by-case basis
 2. Identify the transfer tools you are relying on
 3. When relying upon “Appropriate Safeguards”, assess which instrument is most effective in light of all circumstances of the transfer
 4. Adopt supplementary measures
 5. Depending on the chosen transfer mechanism, obtain DPA approval for the data transfer (mainly in case of BCRs and ad hoc contracts)
 6. Re-evaluate at appropriate intervals
- If no appropriate safeguards can be implemented, not even using supplementary measures, the data transfer can not be initiated or continued.
 - When choosing the most effective transfer mechanism and appropriate safeguards, the legislation in the third country needs to be taken into account.

International Data Transfers post Schrems-II

The draft EDPB Recommendations: Supplementary Measures

- Distinction between technical, contractual and organisational measures
- The contractual and organisational measures are largely aimed at informing all parties involved (both the data exporter and data subjects) in case of received government requests to hand-over personal data, as well as mandatory transparency reports.
 - Of note: the Warrant Canary, a technical mechanism providing (at least) daily encrypted notifications indicating no government requests have been received. If the indications is not sent, this could mean a government request was received, without explicitly saying so.
- The technical safeguards are scenario-based. As long as personal data cannot be accessed outside of the EEA (for example by only using a non-EEA server for a completely encrypted backup, or when sending pseudonymised data for research purposes, while leaving the key in Europe), supplementary measures could be used, under very strict conditions.

International Data Transfers post Schrems-II

The draft EDPB Recommendations: Supplementary Measures

- No supplementary measures are considered to be sufficient for two scenarios:
 - Cloud storage outside the EEA, when personal data needs to be accessed in the clear;
 - Access from a non-EEA country to personal data hosted in the EEA.
- The EDPB does not provide a definition of what constitutes a data transfer, but does clarify that access to personal data from outside the EEA is considered to be a data transfer.

International Data Transfers post Schrems-II

Evaluating Third Countries: European Essential Guarantees

In 2015 the EDPB has developed four European Essential Guarantees that can be used when assessing the legislation of a third country for (non-)justified government interferences. These are based on case-law from the CJEU and ECtHR, and have now been revised.

- A. Processing should be based on clear, precise and accessible rules
- B. Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
- C. An independent oversight mechanism should exist
- D. Effective remedies need to be available to the individual

International Data Transfers post Schrems-II

Initial Comments

- No risk-based approach
- EDPB does not explain which options for scenario 6 and 7 have been discarded as insufficient
- No definition of data transfer
- No clarity on further guidance, for example white listing certain jurisdictions, sectors or laws, or making shared assessments available.

International Data Transfers post Schrems-II

New Standard Contractual Clauses

Section I

- Clause 1 - Purpose and Scope
- Clause 2 - Third Party Beneficiaries
- Clause 3 - Interpretation
- Clause 4 - Hierarchy
- Clause 5 - Description of the Transfer
- Clause 6 - Docking Clause

Section II - Obligations of the Parties

- Clause 1 - Data Protection Safeguards
 - Module 1: C-C
 - Module 2: C-P
 - Module 3: P-P
 - Module 4: P-C
- Clause 2 - Local Laws Affecting Compliance with the Clauses
 - Warranties
 - Assessments
 - Safeguards

Section II (cont'd)

- Clause 3 - Government Access Requests
- Clause 4 - Sub-processors
- Clause 5 - Data subject rights
- Clause 6 - Redress
- Clause 7 - Liability
- Clause 8 - Indemnification
- Clause 9 - Supervision

Section III - Final Provisions

- Clause 1 - Non-compliance
- Clause 2 - Governing Law
- Clause 3 - Choice of Forum and Jurisdiction

Annex I - The processing

Annex II - Technical and Organisational Measures

Annex III - List of Sub-processors

International Data Transfers post Schrems-II

Initial Comments

- More flexibility: four scenarios instead of two.
- More administrative burdens - will this be doable for SMEs?
 - Onward transfers to third party processors will require more documentation
 - Possible impact on competitiveness from EU players
- More reliance on data importer in the third country
- Discussed if recitals 7 and 9 of the Draft SCC Decision imply that the SCCs are not relevant if the non-EU based data controller is still subject to the GDPR.

International Data Transfers post Schrems-II

What's Next?

- Internet consultations ongoing for both the EDPB Recommendations and the draft SCCs.
 - EDPB: until 21 December (extended from 30 November)
 - European Commission: until 10 December
- Final texts should be available Q1 2021
 - The EDPB Recommendations have immediate applicability, since they are interpreting existing legislation
 - The new SCCs will apply only once they are adopted in their final form. They will be subject to a 1 year transition period, after which the old SCCs (based on Directive 95/46/EC) may no longer be used.

Thank You!

paul.breitbarth@trustarc.com
[@EuroPaulB](#)