

**Transfers of personal data to
third countries in an
academic context**

Sandrine Munoz
Data Protection Officer of University of
Luxembourg

Science and research have no borders

Collaboration with partners located outside EU&EEA



Online recruitment, apps....
(provider located outside EU& EEA)

Science & research have to handle the GDPR requirements **related to transfers of personal data to third countries (also named international transfers)**

In collaborations
with **partners
located outside
EU & EEA** (e.g
access, sharing)



With **external
providers located
outside EU & EEA**
(online recruitment,
apps...)

The decision of the European Court of Justice Schrems II

16 July 2020

Decision about legal mechanisms of international transfers

Invalidation of the Privacy Shield to transfer personal data of users from EU to USA in relation with service providers

Additional **clarifications & requirements** about **the use of the Standard Contractual Clauses**

The CJEU added that “[s]ince by their inherently contractual nature standard data protection clauses cannot bind the public authorities of third countries [...] it may prove **necessary to supplement the guarantees contained in those standard data protection clauses**

THE LEGAL CONTEXT

SCHREMS II CASE QUICK DETAILS

- **Mr Schrems** who introduced the case has been a **Facebook user** since 2008. Facebook processes user data in the United States
- **Original complaint in 2013** with the Irish Data Protection Commissioner about surveillance activities undertaken by US intelligence agencies
- Mr Schrems argued that Law & practice in the US relating to this was **not provided adequate protection for personal data transferred from the EU to USA**
- The CJEU declared the EU-US Privacy Shield to be invalid with **immediate effect**

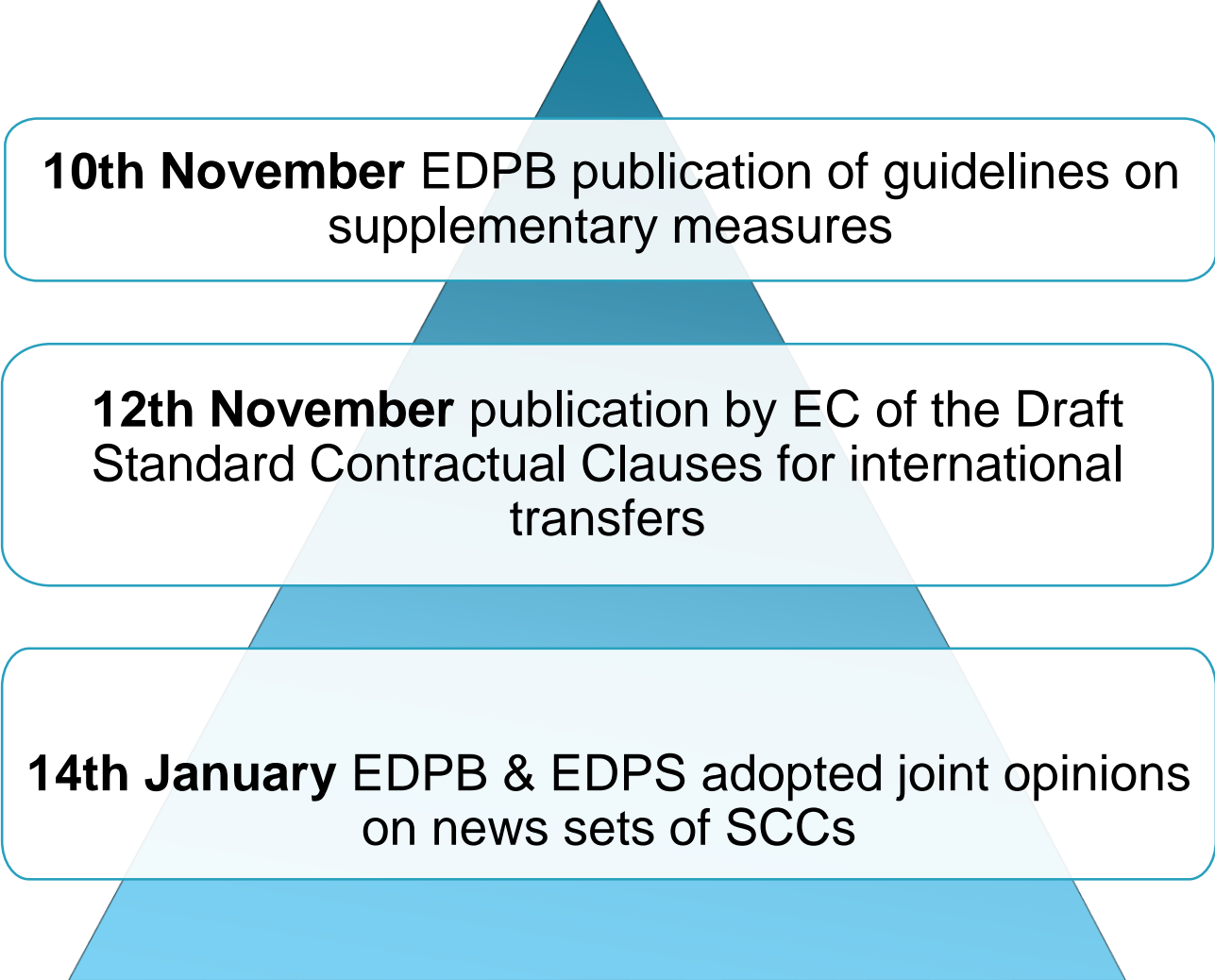
All the transfer of personal data from EU to USA based on the Privacy Shield are illegal

Standard Contractual clauses can be used as appropriate safeguard under conditions

Providers cannot argue anymore they are privacy shield certified

The trend is that big IT /cloud providers already adapted their agreement and proposes to add the SCC in their Data Processing Agreement

REGULATORY EVOLUTIONS RELATED TO TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES



10th November EDPB publication of guidelines on supplementary measures

12th November publication by EC of the Draft Standard Contractual Clauses for international transfers

14th January EDPB & EDPS adopted joint opinions on news sets of SCCs

FOCUS ON THE STANDARD CONTRACTUAL CLAUSES BEFORE THE GDPR

- On 15 June 2001, the Commission adopted Decision 2001/497/EC on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (“**the 2001 SCCs**”), complemented by Commission Decision of 27 December 2004 (“**the 2004 SCCs**”)
- On 5 February 2010, the Commission adopted Decision 2010/87/EU on **standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC**, later amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (“**the 2010 SCCs**”)

FOCUS ON THE STANDARD CONTRACTUAL CLAUSES AFTER THE GDPR

- On 12 November 2020, the Commission published:
 - A draft Commission Implementing **Decision on standard contractual clauses for the transfer of personal data to third countries** pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (“the Draft Decision”); and
 - An **Annex** to the Commission Implementing Decision on **standard contractual clauses** for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (“the Draft SCCs”)

WHY NEW STANDARD CONTRACTUAL CLAUSES?

Adapt to technologies
and GDPR

- SCC in line with the GDPR
- Covering additional scenario e.g processor to processor, processor to controller

Binding requests from
public authorities in a
third country (data
importer)

- Mechanism to be able to deal with requests from public authorities from a third country of the data importer
- e.g US Public Authorities to FC

COMBINATION OF GENERAL CLAUSES WITH **MODULAR APPROACH**

Module 1

Transfer controller to controller

Module 2

Transfer controller to processor

Module 3

Transfer processor to processor

Module 4

Transfer processor to controller

Level of data subject protection reinforced

Introduction of **specific modules for each transfer scenarios**

Necessary **to clarify whether the SCCs can include several modules** in practice to address different situations or whether this should amount to the signing of several sets of the SCCs

Publication of flow charts & FAQ is encouraged

Recommendations of supplementary measures remain relevant to be applied after the adoption of the SCCs

FOCUS ON THE STANDARD CONTRACTUAL CLAUSES APPLICATION OF THE MODULAR APPROACH IN A RESEARCH CONTEXT

- A research institution **A** in **Europe** wants to lead a research project with an institution **B** located in **Australia**
 - Collection of personal data will be done in Europe and in Australia
 - Sharing of personal data will occur in both side
- Research institutions **A** & **B** want to launch an application/a platform to collect personal data of research participants using the services of a provider **C** located in USA and having a subprocessor **D** located in India



FOCUS ON THE STANDARD CONTRACTUAL CLAUSES APPLICATION OF THE MODULAR APPROACH IN A RESEARCH CONTEXT

- Modular approach of the future SCC can apply
 - Transfer controller to controller A to B
 - Transfer controller to processor A, B to C
 - Transfer processor to processor C to D

**SOME QUESTIONS FOR THE APPLICABILITY REMAIN UNTIL
ADOPTION OF NEW SCC & FAQ AND GUIDANCE WOULD BE VERY
RELEVANT**



WHAT IS EXPECTING FROM ORGANISATIONS REGARDING DATA TRANSFERS

1. Know your transfers

- Research collaborations can involve transfer of personal data to **research institutions located outside EU & EEA** or
- Use services of **external provider located outside EU & EEA** involving personal data processing e.g online recruitment (or service provider with subprocessors located outside EU & EEA)
- Necessary to know **in which country your partner** is located outside EU & EEA
- Necessary to know **in which country the service provider or its subprocessor** is located outside EU & EEA
- NB: It is necessary to check that the data you transfer is adequate, relevant & limited to which necessary in relation to the purposes

2. Check the transfer tool you rely on

- Check with your DPO or legal officer in charge of Data Protection if there is **an adequacy decision** meaning adequacy decision between EU & the country where your partner/provider
- In absence of adequacy decision
 - Appropriate safeguards or
 - Derogations



Appropriate safeguards (art.46 GDPR) e.g:

- Standard contractual clauses of EC
- Binding Corporate Rules
- Code of conduct approved (not already)
- Mechanism of certification
- Ad hoc clauses
- Etc...

Derogations (art.49 GDPR) e.g:

- **Explicit consent** of the data subject
- Transfer necessary for the **performance of a contract** between the data subject & the controller
- Transfer necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller & another natural or legal person
- The transfer is necessary for **important reasons of public interest** e.g the fight against Covid 19, ...

Not easy for organisations to rely on in practice e.g consent is revocable

3. Assess if anything in the law or practice of the third country may affect the efficiency of appropriate safeguards
 - **IF NOT** the transfer may occur with appropriate safeguard or derogations
 - **IF YES** transfer may occur with additional measures



4. Identify & adopt supplementary measures

Examples of supplementary measures are provided by EDPB: technical, contractual & organisational measures

Technical measures

Encryption measures under specific requirements in relation with the robustness

Pseudonymisation: transfer of pseudonymised data



4. Identify & adopt supplementary measures

Additional contractual measures

- Requiring **technical measures** such as encryption of the transport
- **Transparency of the importer** (on its best efforts) providing information on the access to data by public authorities
- Certification by the data importer of not created back doors or similar programming
- **Empowering data subjects to exercise their rights**

Requiring through the agreement that personal data transmitted in plain text in the normal course of business may only be accessed with the express or implied consent of the exporter and/or data subject (only when cooperation of data importer on a voluntary basis)

4. Identify & adopt supplementary measures

Organisational measures

Adoption of internal policies with clear allocation of responsibilities for data transfers, reporting channels & standard operating procedures



CONCLUSION

SOME TIPS

Do

- Check if your collaboration or the service provider involved international transfer of personal data
- Involve the relevant stakeholders (DPO, CISO etc...)
- Discuss with them the appropriate legal instruments & supplemental measures
(CASE BY CASE ANALYSIS)

Don't

- Assume that international transfer will not occur
- Involve the relevant stakeholders to the last minute
- Leave implementation to the last minute & presume that all measures will be in the agreement

THANK YOU FOR YOUR ATTENTION

- Questions?
- Remarks?

