



EUROPEAN DATA PROTECTION SUPERVISOR


The EU's independent data
protection authority



EUDPR: Conditions and Safeguards in International Transfers to Private Entities

Legal officers (Supervision and
Enforcement Unit at the EDPS)

EDPS training at EUSA for EUI staff,
14 September 2021



The Basics

Transfers of personal data

Transfer of personal data

What
is a
transfer

- communication,
 - transmission,
 - disclosure
 - or otherwise making available of personal data,
 - with the knowledge or intention of a sender subject to the EUDPR
 - the recipient(s) will have access to it
-
- ➡ deliberate transfer or permitted access
 - ➡ access is sufficient – no storage required
 - ➡ onward transfers

Recipients

**Recital 21
Article 9**

EUI

intra-EU
transfer =
transmission

EU Member State / EEA

Chapter V

Third country

(international)
transfer

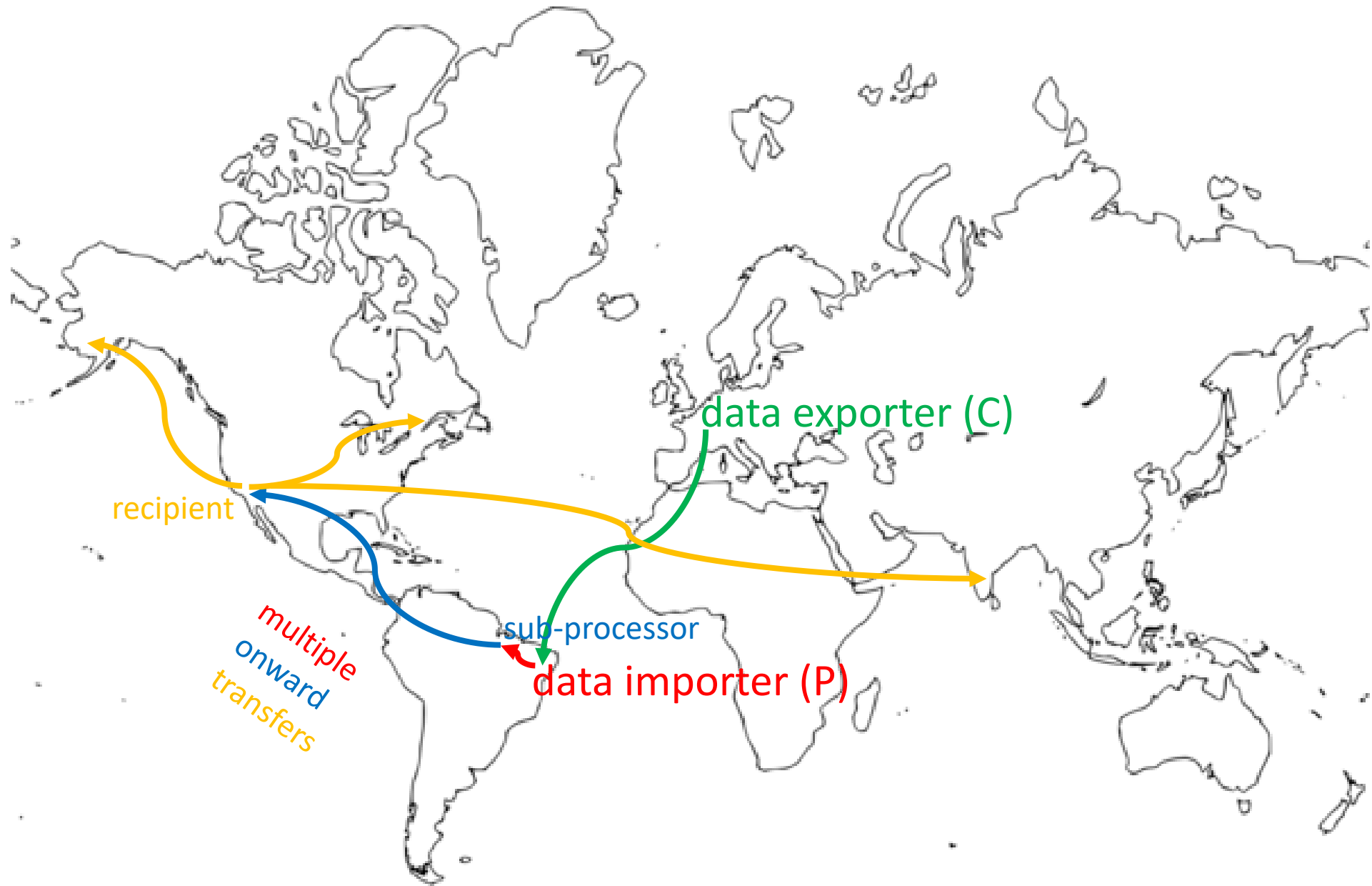
International organisation



Onward transfers

Transfer from recipient in the third country of destination or recipient in international organisation to:

- another third country or to another international organisation
- controllers, processors or other recipients in the same third country or in the same international organisation



"world map" is marked with [CC0 1.0](https://creativecommons.org/licenses/by/4.0/)



POLL 1:

Would transfers from your EUI to other entities within and outside EU/EEA have an impact on:

- 1) the processing Yes No
- 2) who you engage to process personal data for you Yes No
- 3) the contract Yes No
- 4) technical, organisational and security measures Yes No



POLL 1:

Would transfers from your EUI to other entities within and outside EU/EEA have an impact on:

- 1) the processing Yes No
- 2) who you engage to process personal data for you Yes No
- 3) the contract Yes No
- 4) technical, organisational and security measures Yes No



Accountability and transfers

- Control your data throughout the processing
- Take **informed decisions** when allowing transfers of personal data
- information on the processing:
 - types of personal data, data subjects affected
 - access rights
 - location of personal data
 - security of processing – technical and organisational measures in place
- appropriate safeguards in place (documented)
- verify compliance – carry out audits

**Golden Rule:
As controller,
you remain
responsible.
Always.**





EU standards of protection for transfers outside the EEA



Conditions & instruments for international transfers

The rules of Chapter V...





Article 46 – General principles

- ✓ Transfers to third countries and IOs
- ✓ Adequate (essentially equivalent) level of protection
- ✓ Protection of individuals not undermined
- ✓ Two step approach: comply EUDPR → Chapter V
- ✓ Lawful, necessary, proportionate
- ✓ No risks for data subjects
- ✓ Documented (assessment and transfer)
- ✓ Three types:
 - adequacy decisions
 - appropriate safeguards
 - derogations

Transfer of personal data to 3rd countries / int. org. (Art. 46-50 EUDPR)

Adequacy decision
+ solely to allow EUI tasks to be carried out

- [Andorra](#), [Argentina](#), [Canada](#) (commercial organisations), [Faroe Islands](#), [Guernsey](#), [Israel](#), [Isle of Man](#), [Japan](#), [Jersey](#), [New Zealand](#), [Switzerland](#), [Uruguay](#), [UK](#) and the ~~[USA](#)~~ (limited to the ~~[Privacy Shield framework](#)~~)

Appropriate safeguards no EDPS authorisation

- Legally binding instrument
- SCCs for transfers (EC)
- SCCs for transfers (EDPS)
- Binding corporate rules, Codes of conduct, Certification (under GDPR)

+ supplementary measures

Appropriate safeguards with EDPS authorisation

- *Ad hoc* contractual clauses for transfers
- Administrative arrangements
- Transfer under Art. 9(7) Reg 45/2001

Derogations

- Explicit consent of data subject to transfer
- Contract with data subject
- Contract in interest of data subject
- Important reasons of public interest
- Legal claims
- Vital interests of data subject / others
- Public register

inform EDPS about categories of cases in which these have been applied





Article 47 – Adequacy decision

- Two cumulative conditions:
 - ✓ **decision** adopted by the EC pursuant to GDPR or LED that a third country, territory, sector, an int. org. **ensures an adequate level of protection**
 - ✓ **personal data transferred solely to allow tasks within competence of the EUI to be carried out**
- No need for another transfer instrument or any further authorisation
- EUIs shall notify EC and EDPS if the third country, territory, sector or int. org. does not ensure an adequate level of protection

Adequacy referential



A. Content Principles:

- Concepts
- Grounds for lawful and fair processing for legitimate purposes
- The purpose limitation principle
- Data Retention principle
- The security and confidentiality principle
- The transparency principle
- The right of access, rectification, erasure and objection
- Restrictions on onward transfers

B. Examples of additional content principles to be applied to specific types of processing

- Special categories of data
- Direct marketing
- Automated decision making and profiling

Adequacy referential



C. Procedural and Enforcement Mechanisms

- Competent Independent Supervisory Authority
- The data protection system must ensure good level of compliance
- Accountability
- The data protection system must provide support and help to individual data subjects in the exercise of their rights and appropriate redress mechanisms

European Essential Guarantees

As regards access by public authorities

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

Article 48 – Appropriate safeguards



- no adequacy decision
- **appropriate safeguards provided + enforceable data subject rights** and effective legal remedies for data subjects are available
- to ensure an adequate level of protection for that transfer
- consultation or authorisation of the EDPS

Appropriate
safeguards
no EDPS
authorisation

- Legally binding instrument
- SCCs for transfers (EC)
- SCCs for transfers (EDPS)
- Binding corporate rules (BCR-C, BCR-P), Codes of conduct, Certification - under GDPR

+ supplementary
measures

Appropriate
safeguards
with EDPS
authorisation

- Contractual clauses
- Administrative arrangements
- Transfer under Art. 9(7) Reg 45/2001



Article 48 (2) – Appropriate safeguards (no EDPS authorisation)

Standard Contractual Clauses for transfers

- EC or EDPS + comitology procedure → none yet under EUDPR
- no changes apart from where foreseen (e.g. annexes)
- can be included in wider contract
- can be **supplemented** with other clauses or additional safeguards if there is no contradiction or prejudice to fundamental rights



Article 48 (3) – Appropriate safeguards (EDPS authorisation)

Ad hoc contractual clauses for transfers

- between controller – processor or processor – recipient in third country
- binding and enforceable
- appropriate safeguards → **supplementary** measures
- if SCCs are changed, they may become *ad hoc* clauses



Article 48 (2) – Appropriate safeguards (no EDPS authorisation)

Binding Corporate Rules

- data protection policy for multinational groups established in the EU for transfers
- legally binding and enforced by members
- data protection principles and enforceable rights
- approved by competent DPA through consistency mechanism
- EUIs to check if the scope of BCR is appropriate

Codes of Conduct | Certifications

- none yet approved for transfers



Schrems II Judgment

The world evolves and
so do the rules...



Case C-311/18 („Schrems II“)

- US not ensuring adequate (essentially equivalent) protection
- ✘ lack of proportionality of mass surveillance programmes (Section 702 of the FISA and E.O. 12333) and
 - ✘ the lack of effective remedies in the US essentially equivalent to those required by Article 47 of the Charter
- EU-US Privacy Shield adequacy decision invalidated



Case C-311/18 („Schrems II“)

required level is **adequate** protection = **essentially equivalent** protection as in EU

- ✓ SCCs for transfers valid if effective mechanisms
 - to ensure compliance with required level of protection
 - to suspend or prohibit the transfer if clauses breached or cannot be honoured
- ✓ can be used if **essentially equivalent level** of protection can be ensured
- ✓ contain **standard clauses** for any third country **to be supplemented** where necessary with additional measures
- ✓ same for other tools in Art. 46 GDPR / Art. 48 EUDPR

Mapping data flows



Know your transfers! Control your transfers!

In line with existing obligations in Arts. 4, 5, 6, 26, 29, 30, Ch V EUDPR

The mapping exercise to describe in particular:

- each processing activity for which data is transferred to / accessed from a third country (including purposes and means of processing);
- destinations of data transfers (including those of all processors and sub-processors);
- type of recipient (data importer);
- transfer tool used (of the ones provided in Chapter V);
- types of personal data transferred;
- categories of data subjects affected;
- any onward transfers (including to which countries and which recipients, transfer tool used, types of personal data and categories of data subjects affected).

Records, contracts, MoUs, JC arrangements, privacy statements, info from importer





Transfer impact assessment & supplementary measures

Brave new world...





Assessment in accordance with the Schrems II judgment

An **individual case-by-case** assessment to determine :

- whether, **in the context of the specific transfer**, the third country of **destination** affords an essentially equivalent level of protection
- if the safeguards of the intended transfer tool would be **effective**

To be carried out

- by the EUI, where appropriate with the data importer
- before any transfer (including by way of remote access) is made or a suspended transfer is resumed.





POLL 2:

We use SCCs to transfer personal data to our processor in Malaysia. We do not need to carry out any assessments on the impact of these transfers.

Is this correct?

Yes

No



POLL 2:

We use SCCs to transfer personal data to our processor in Malaysia. We do not need to carry out any assessments on the impact of these transfers.

Is this correct?

Yes

No

Assessment in accordance with the Schrems II judgment



- Mere use standard or ad hoc contractual clauses or another transfer tool Art. 48 EUDPR / 46 GDPR is **not sufficient** to ensure an essentially equivalent level of protection as in the EU.
- Use of Art. 48 EUDPR / 46 GDPR transfer tool does not substitute the individual case-by-case assessment in accordance with the Schrems II judgment.





Assessment in accordance with the Schrems II judgment

- Assessment needs to take into consideration the **specific circumstances of the transfer** (e.g. categories of transferred data, purposes for which they are transferred and processed in the third country and how)
- and **all the actors participating in the transfer** (e.g. controllers, processors and sub-processors processing data in the **third country(-ies) of destination**),
- as identified in the mapping of the transfers.
- Also need to factor into this assessment **any envisaged onward transfer.**

Article 46 EUDPR & paras. 33 - 34 of the EDPB Recommendations 01/2020





Assessment in accordance with the Schrems II judgment

- Where the required essentially equivalent level of protection for the transferred data is not effectively ensured,
- because the **law or practice of the third country impinges on the effectiveness of the appropriate safeguards** contained in the used SCCs for transfers or another transfer tool,
- the EUI must implement **contractual, technical and organisational measures**
- to **effectively supplement** the safeguards in the transfer tool,
- where necessary together with the data importer.

Paras. 54 and Annex 2 of the EDPB Recommendations 01/2020





Assessment in accordance with the Schrems II judgment

Is a process of

- assessing the level of protection in the third country and
- whether supplementary measures are needed, and
- then identifying effective supplementary measures.

Commonly called a **‘transfer impact assessment’**

No template, but methodology is available

Para. 54 and Annex 2 of the EDPB Recommendations 01/2020





**EDPB Recommendations 01/2020 on
measures that supplement transfer
tools to ensure compliance with the EU
level of protection of personal data**

new & updated

**EDPB Recommendations 02/2020 on
the European Essential Guarantees for
surveillance measures**

update of
WP29 EEG

**WP29 Adequacy Referential WP 254 rev.01, endorsed by
the EDPB**

EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

- assessing if third countries laws & practices relevant for the transfer ensure a level of protection of the personal data transferred that is essentially equivalent to that guaranteed in the EEA (no impingement on appropriate safeguards of Art. 46 GDPR¹ tool)
- identifying and implementing appropriate supplementary measures to the Art. 46 GDPR¹ tool used to ensure effective compliance with that level of protection where the safeguards contained in the Art. 46 GDPR¹ tool are not sufficient

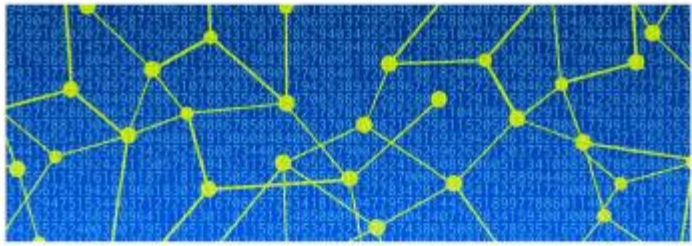
EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures

- elements to assess if relevant laws on access by public authorities for surveillance unjustifiably interfere with required level of protection

WP29 Adequacy Referential WP 254 rev.01, endorsed by the EDPB

- further inspiration for elements to consider when assessing relevant laws re: required level of protection in the specific transfer based on the Art. 46 GDPR¹ tool used

¹/ Art. 48 EUDPR



EUROPEAN DATA PROTECTION SUPERVISOR

Strategy for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling



29 October 2020



Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

Version 2.0
Adopted on 18 June 2021



Adopted

1

Roadmap of steps 1/2



Step 1

Know your transfers

- map all transfers (including from (sub-)processors, remote access, storage in cloud outside EEA and onward transfers to same of to another third country),
- check that you allowed that transfer and that it complies with data minimisation principle

Step 2

Identify the transfer tools of Chap. V you are relying on

- Art. 47 EUDPR → subject to compliance with other obligations, no need to proceed with next steps, but monitor validity of adequacy decision
- Art. 48 EUDPR / Art. 46 GDPR tool for regular and repetitive transfers → proceed with next steps
- Art. 50 EUDPR / Art. 49 GDPR* derogations → only in some cases of occasional and non-repetitive transfers if conditions met, no need to proceed with next steps

Step 3

Assess if anything in the law or practice of the third country impinges on effectiveness of appropriate safeguards of the Art. 48 EUDPR transfer tool you are relying on in context of your specific transfer

- including re: fundamental rights of individuals (data subject rights) & access by public authorities,
- likelihood of public authorities' access in practice should not be taken into account, importer's previous experience under conditions if corroborated and not contradicted and not as primary factor
- transfer tool effective – no measures; transfer tool not effective – need supplementary measures or stop





Roadmap of steps 1/2

Step 4

Identify and adopt effective supplementary measures

- This is a case-by-case analysis based on the circumstances of your transfer.
- Annex 2 – examples of supplementary measures, scenarios and conditions for measure to be effective
- Combine technical + contractual + organisational measures [not alone!],
- effective measures – go ahead; no effective measures – suspend or end, if not notify EDPS

Step 5

Take any formal procedural steps that may be required

- SCCs: no need to request an authorisation from the SA.
- BCRs and ad-hoc contractual clauses: Schrems II also applies. Precise impact still under the discussion and may be detailed in other documents (e.g. BCRs referentials).
- The EDPS will provide further advice to EUIs on any required procedural steps.

Step 6

Re-evaluate at appropriate intervals

- Monitor new developments on on-going basis, where appropriate together with importers.
- Re-evaluate your assessment of the level of protection, including supplementary measures. If necessary take appropriate action: - add more effective measures or - suspend or end transfer if importer breached or unable to honour commitments made in tr. tool or if measures no longer effective in that 3rd country





POLL 3:

We had already carried out a data protection impact assessment in 2015. We do not need to now carry out a transfer impact assessment.

Is this correct?

Yes

No



POLL 3:

We had already carried out a data protection impact assessment in 2015. We do not need to now carry out a transfer impact assessment.

Is this correct?

Yes

No

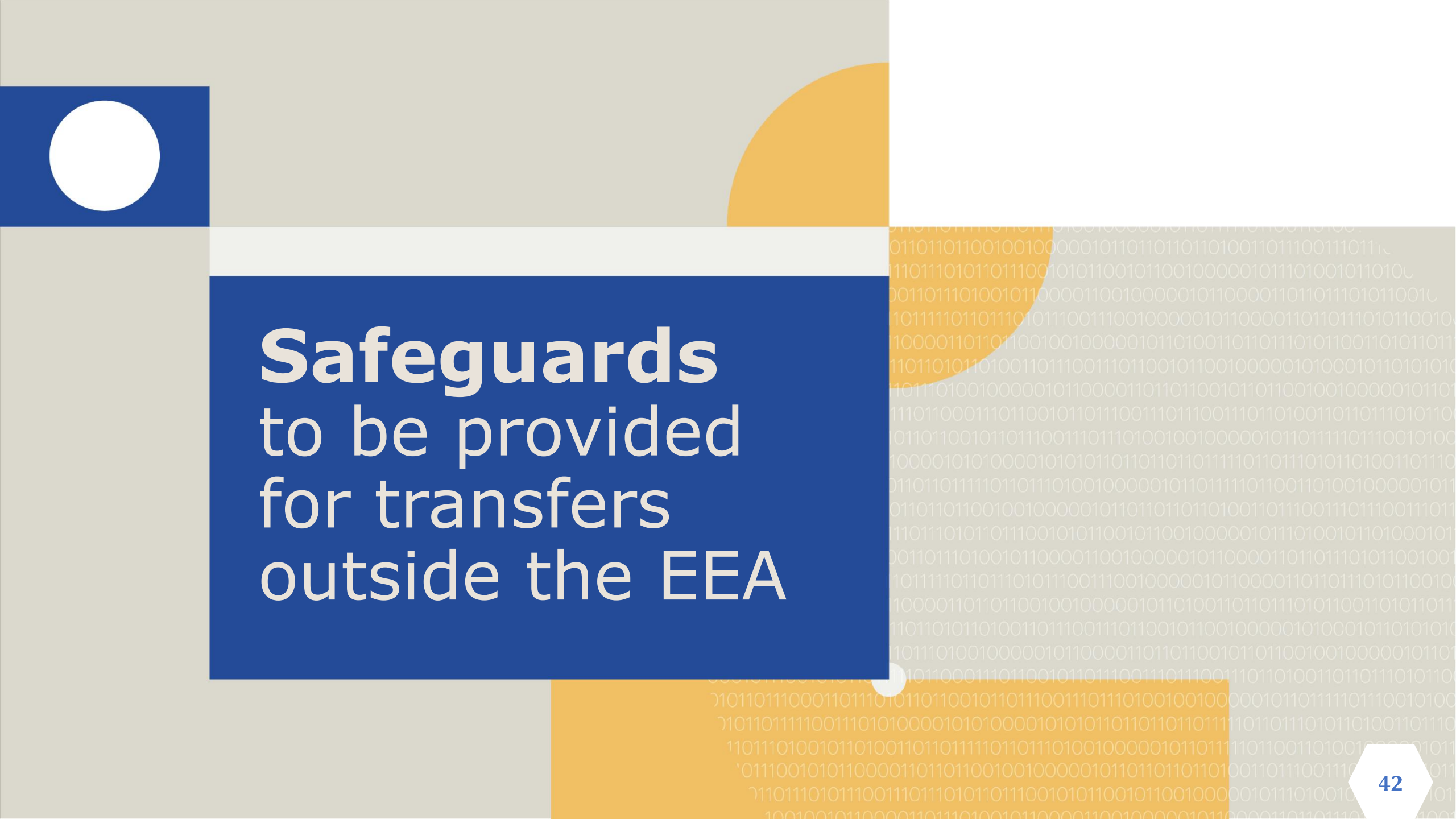


DPIA ≠ TIA



- **DPIA broader process pursuant to Art. 39 EUDPR**
- Assessment of the impact of the envisaged processing operations on the protection of personal data. Key tool to correctly implement data protection by design and by default.
- Must be carried out **only in certain cases (where high risk likely)**
- Assess risks to rights and freedoms of data subjects and envisage measures, safeguards and mechanisms for mitigating those risks
- Might assess also risks related to transfers to adequate & non-adequate third countries

- **TIA more specific process pursuant to Schrems II Judgment**
- Assessment of the impact of the envisaged transfer on the protection of personal data when that data is transferred to a non-adequate third country
- Must be carried out **for all transfers pursuant to Article 48 EUDPR**
- Assess whether, taking into account the circumstances of the specific transfer, an essentially equivalent level of protection, as provided in the EU/EEA, is afforded in the third country of destination or whether any "supplementary measures" may be needed to ensure the required level of protection and implementing identified measures



Safeguards to be provided for transfers outside the EEA



Safeguards to be provided for transfers outside the EEA

Need to know and control data flows





Need to know and control data flows

- Safeguards and measures based on all information necessary to fully assess all risks concerning international transfers and implement appropriate safeguards.
- **No ambiguity** whether certain personal data from a specific service is stored, transferred (including by remote access) or otherwise processed in a specific country.
- Information on **all data, all the actors and all the third countries involved** for transfers is the minimum essential information for a meaningful ‘transfer impact assessment’.
- Absolute clarity in this regard of utmost importance.

Step 1 „Know your transfers“ of EDPD Recm. 01/2020 and Arts. 4, 5, 6, 9, 26, 29, 30 and Ch V EUDPR; paras 127-132 and annex of EDPB-EDPS Joint Op. 2/2021



Need to know and control data flows

- **Detailed knowledge of which personal data from which services will be transferred (including by remote access) for which purpose to which recipients in which third country with which safeguards and measures. To be in a position to:**
 - i) make meaningful a TIA, including identifying effective safeguards and measures,
 - ii) implement those safeguards and measures itself and by provider,
 - iii) complete annexes of *ad hoc* contractual clauses with all due diligence and
 - iv) be able to demonstrate that all assessments have been made and measures implemented and effectiveness of those measures.



Safeguards to be provided for transfers outside the EEA

Appropriate safeguards reflecting EUDPR





2021 SCCs adopted by Commission

NEW

Standard contractual clauses between controllers and processors ([link](#))

- [EDPB-EDPS Joint Opinion 1/2021](#)
- [Annex 1](#)
- [Annex 2](#)

* Art. 28 GDPR /
Art. 29 EUDPR

Note: the annexes contain additional comments of a more technical nature that are made directly to the draft Implementing Decision and to the draft SCCs, notably in order to provide some examples of possible amendments.

Standard contractual clauses for the transfer of personal data to third countries ([link](#))

- [EDPB-EDPS Joint Opinion 2/2021](#)
- [Annex](#)

* Art. 46 GDPR (+
Art. 28 GDPR)

Note: the annex contains additional comments of a more technical nature that are made directly to the draft SCCs, notably in order to provide some examples of possible amendments.



2021 SCCs adopted by Commission

- Possible for several parties to sign a same set of new SCCs for processors or for transfers.
- SCCs under Art. 46 GDPR \neq SCCs under Art. 48 EUDPR.
- Processor of EUI could use SCCs under Art. 46 GDPR to transfer to sub-processor outside EEA.
- Relevant requirements of the EUDPR should be reflected throughout the entire chain of contracts when a EUI is the controller.



POLL 4:

Can we use new SCCs for transfers under GDPR as a basis for our *ad hoc* contractual clauses under EUDPR?

Yes

No

POLL 4:



Can we use new SCCs for transfers under GDPR as a basis for our *ad hoc* contractual clauses under EUDPR?

Yes

No

Such *ad hoc* CCs under Art. 48(3)(a) EUDPR could provide sufficient guarantees for transfers of personal data **if complemented** with :

- **additional guarantees to reflect all requirements of EUDPR**
- **effective supplementary measures**
- ensure that the processing will meet the requirements of EUDPR and
- ensure an essentially equivalent level of protection to that guaranteed in the EU/EEA
- You may need to change processing to limit transfers to only third countries where supplementary measures would be effective!



Limit transfers

- EDPS strongly advised against starting any new processing operations or new contracts with any service providers that would involve transfers of personal data to the US.
- A good reflex for EUI controllers to start considering limiting processing to the EU (using the same or alternative service providers), as
- in many situations it would be difficult to find effective supplementary measures to ensure the required level of protection.

EDPS Strategy for EUIs to comply with Schrems II ruling, EDPS order to EUIs of 02/10/2020



Question:



Our processor in a third country tells us that they do not have to use SCCs for transfers since they are also bound by the GDPR which applies by virtue of Article 3(2) GDPR. Is this correct?

Yes

No

Recital 7 COM Impl.
Dec. (EU) 2021/914

- The new SCCs not to be used by **GDPR controllers or processors** when Art. 3(2) GDPR applies since these SCCs not the appropriate tool for such transfers → instead use another Article 46 GDPR tool, e.g. *ad hoc* clauses under Art. 46(3) GDPR, providing for "missing" safeguards not already provided by virtue of direct application of GDPR obligations in order to ensure that the protection provided by the GDPR is not undermined by a third country legislation applicable to the importer and to the transferred data.
- **If controller is an EUI** → use **Article 48 EUDPR tool** reflecting all EUDPR requirements !

Question:



Can companies still rely on 2010 SCCs for transfers to their processors in third countries?

Yes

No

- Old 2001 and 2010 SCCs for transfers under Directive 95/46 are repealed with effect from 27 September 2021.
- Contracts concluded before 27/09/2021 on basis of those old SCCs for transfers shall be deemed to provide appropriate safeguards under Article 46 GDPR until 27/12/2022, provided:
 - the processing operations that are the subject matter of the contract remain unchanged and
 - that reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards.

Art. 4 COM Impl. Dec. (EU)
2021/914



Question:

Can our EUI still rely on 2010 SCCs for transfers to our processors in third countries?

Yes

No

If controller is an EUI:

- clauses have to reflect all requirements of EUDPR
 - supplementary measures will need to be included
 - processing may need to be changed to limit transfers
- old SCCs for transfers are outdated and do not provide for the required level of protection !

meet the requirements
of the EUDPR

Appropriate safeguards to
be provided for transfers
outside the EEA

ensure the protection of the
rights of the data subjects

essentially equivalent level
of protection outside EEA



ensure the protection of the rights of the data subjects

meet the requirements of the EUDPR

essentially equivalent level of protection

Appropriate safeguards for transfers outside the EEA

- Use new SCCs for transfers under Art. 46 GDPR as a model.
- Adapt them to the EUDPR reflecting its requirements.
No mere cutting & pasting!
- SCCs only cover some general obligations (“standard”), you will still have to fill in what exactly you want your recipient (not) to do.
- Include supplementary measures!

Safeguards to be provided



DATA PROTECTION SAFEGUARDS

- Purpose and scope of the Clauses
- Effect and invariability of the Clauses
- Third-party beneficiaries
- Interpretation in accordance with EUDPR
- Hierarchy
- Description of the transfer(s) in annexes
- Accession of others to the Clauses („docking clause“) - optional

Safeguards to be provided



DATA PROTECTION SAFEGUARDS

- Instructions
- Purpose limitation, Transparency, Accuracy
- Duration of processing and erasure or return of data
- Security of processing
- Sensitive data
- Onward transfers
- Documentation and compliance

Safeguards to be provided



OBLIGATIONS OF PARTIES

- Use of sub-processors
- Data subject rights
- Redress
- Liability
- Supervision

LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

- Local laws and practices affecting compliance with the Clauses
- Obligations of the data importer in case of access by public authorities

Safeguards to be provided



FINAL PROVISIONS

- Review or suspension of Clauses
- Non-compliance with Clauses & termination
- Governing law
- Choice of forum & jurisdiction

APPENDIX / ANNEXES

- List of parties
- Description of transfers (incl. sensitive PD)
- Competent supervisory authority
- Technical, organisational & security measures
- List of sub-processors



Safeguards to be provided for transfers outside the EEA

Imposing clear & binding obligations on all recipients





The Service Provider is a global company operating in different countries and providing global and interconnected services from various data centres around the world operated by its different establishments and its contractors. The Customer acknowledges and gives its final instruction to the Service Provider to proceed with the transfers in accordance with these Clauses and policies of the Service Provider.

examples of
clauses to assess



POLL 5:

The Parties agree that the exchange of personal data with the Service provider and its contractors is essentially necessary for the purpose of providing and improving the contracted services to the Customer and for the Service Provider to comply with its legal obligations.

Is this sufficient?

Yes

No



POLL 5:

The Parties agree that the exchange of personal data with the Service provider and its contractors is essentially necessary for the purpose of providing and improving the contracted services to the Customer and for the Service Provider to comply with its legal obligations.

Is this sufficient?

Yes

No



POLL 6:

The Parties agree that categories of data subjects, categories of personal data to be transferred and processed are described in the data protection notices of the Service Provider and policies of its partners.

Is this sufficient?

Yes

No



POLL 6:

The Parties agree that categories of data subjects, categories of personal data to be transferred and processed are described in the data protection notices of the Service Provider and policies of its partners.

Is this sufficient?

Yes

No



Imposing clear & binding obligations on all recipients

- Contractual safeguards and supplementary measures must impose **clear and binding obligations** on **all envisaged recipients** in third countries to which personal data will be transferred (including by remote access).
- Sign clauses with your direct recipients with possible adherence of other (indirect) recipients.
- Ensure that provisions of the clauses **apply to and are binding upon all** and are **not rendered ineffective** by the concurrent application of other obligations.



Imposing clear & binding obligations on all recipients

- Clearly detail in clauses in a binding way for processor & all sub-processors **which personal data from which services will be transferred for which purpose to which recipients in which third country with which safeguards & measures**
- If other recipients do not accede to clauses, **obtain sufficient guarantees** that processor has implemented appropriate contractual, technical and organisational measures with other sub-processors to ensure required level of protection.
- Satisfy yourself that such measures implemented for transfers to other recipients: i) correspond to the role and the processing of transferred data the recipient will carry out and ii) are in line with the assessments made and supplementary measures you identified during the TIA.



Safeguards to be provided for transfers outside the EEA

Necessary & appropriate contractual supplementary measures





These clauses provide safeguards for transfers in the Customer's use of contracted services to any third country where the Service Provider, its partners and sub-processors operate or will operate economically. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer prevent the data importer from fulfilling its obligations under the clauses.



Necessary & appropriate contractual supplementary measures

- Assessment of whether there is or not any such reason and then implementation of any necessary safeguards and measures to supplement safeguards present in the clauses are to be done **before** clauses are signed.
- Art. 46 GDPR / Art. 48 EUDPR transfer tools mainly contain appropriate safeguards of a contractual nature that may be applied to transfers to all third countries.
- Third countries where clauses, may, together with safeguards and measures (e.g. Art. 33 & 36 EUDPR) already foreseen by the controller and processor, ensure an essentially equivalent level of protection – e.g. a candidate country for accession to the EU or a country for which COM in process of adopting adequacy decision.



Necessary & appropriate contractual supplementary measures

- Third countries to which personal data may be transferred where clauses are unlikely alone to provide essentially equivalent protection.
- Additional contractual, technical and organisational measures ("**supplementary measures**") to ensure the required level of protection will thus be required for such countries.
- Some measures may be effective in one situation while not effective in another. The situation in **different third countries** to which personal data will be transferred may therefore require **different approaches** and **different combinations of supplementary measures**.
- **Annex 2 of EDPB Recommendations 01/2020** - examples of supplementary measures, use cases and conditions for effectiveness of the measures. Consider all examples to identify which measures it would be necessary and appropriate to implement for transfers in the EUI's use of provider's services.



Safeguards to be provided for transfers outside the EEA

Privileges and immunities





The Service Provider notes that the Customer is an EU institution subject to Protocol No 7 of the Treaty on the Functioning of the European Union on the privileges and immunities of the EU which provides for the inviolability of archives of the EU institution.

The Service Provider will not disclose Customer data except in accordance with these Clauses and to comply with the applicable national laws. The Service Provider will try to inform the Customer if it is prevented or unable to comply with these Clauses and commitments herein.

Privileges and immunities



- Respect of **privileges and immunities of EUIs**, as recognised in the Treaties, and **where extended to an EUI by a third country**, in particular e.g. the inviolability of the EUI's archives, contributes to the protection of personal data that EUIs process or that is processed on EUIs' behalf in the EU and outside the EU.
- However, the EDPS has already had the opportunity to also emphasise to EUIs, at the occasion of an investigation into EUIs' use of services of a US service provider, that **EUIs had few guarantees** under their contract with that provider to be actually in a position **to defend their privileges and immunities against disclosure requests** from third-country governments and processors subject to their jurisdiction. This was contrary to Arts. 4(1)(f) and 49 EUDPR.

Privileges and immunities



As part of the TIA, an EUI should **verify** to which extent:

- the privileges and immunities, as extended to the EUI by a third country of destination, apply to and are binding upon the public authorities in that third country and are not rendered ineffective by the concurrent application of other obligations of the third country's authorities;
- the EUI (as controller of the data transferred to and held by the provider and its sub-processors on the EUI's behalf) is in a position to effectively defend against disclosure requests not authorised by EU law from third country governments, by relying on its privileges and immunities; and
- the provider and its sub-processors subject to third-country jurisdiction are able to notify and redirect disclosure requests they receive to the EUI and legally challenge disclosure requests invoking privileges and immunities extended to the EUI.



Safeguards to be provided for transfers outside the EEA

Commitments concerning disclosure requests from third country authorities





The Service Provider will notify any legally binding request for disclosure of Customer data, unless legally prohibited to do so, and will try to redirect the requesting entity to the Customer where such possibility is provided by applicable law. The provider will not disclose Customer data or provide access to Customer data without Customer's consent unless required to do otherwise by applicable law. The Service Provider will make available to the Customer upon request a transparency report with aggregated high-level information on requests received from US authorities in the ten years preceding the last five years in accordance with the limitations imposed by applicable laws.

Commitments on disclosure requests



- Would only provide limited protection in case applicable law prohibits the notification and information.
 - Entails that e.g. provider will not notify the EUI a request for disclosure if provider were prohibited to do so by applicable law of a third country; provider is under no obligation to provide information if it were barred from providing disclosure of one or more such requests due to legal obligations.
 - Not clear how this provision applies to requests received by sub-processors. No transparency for other third countries and limited for US.
 - Some limited commitment to inform EUI if provider is prevented or unable to comply with the clauses and its commitments.
- Need **clear obligations and binding commitments** from provider to notify and redirect to the EUI **any disclosure requests** for EUI's data that it, its affiliates or its sub-processors receive and to legally challenge such disclosure requests.

Commitments on disclosure requests



- Contractual measures not be able to rule out application of a third country law not meeting the EDPB EEGs standard where the law obliges importers to comply with orders to disclose data they receive from public authorities.
- Contractual obligations imposed on the data importer (recipient) concerning disclosure requests from third country authorities is a means to ensure that the data exporter (controller) becomes and remains aware of the risks attached to the transfer of data to a third country.
- Such contractual obligations will enable data exporter to desist from concluding a contract if the law of the third country, the safeguards contained in the transfer tool used and any additional safeguards supplementing the transfer tool cannot ensure a level of protection essentially equivalent to that in the EEA.

Commitments on disclosure requests



Where the applicable law and practice of the third country of the data importer **initially** assessed and **deemed to provide the required level of protection** for the specific transfer, **and situation changes after the conclusion of the contract**, such contractual obligations will enable the data exporter:

- to become aware of any changes in the situation in that third country following the conclusion of the contract, and
- to reassess the situation and implement any additional supplementary measures to supplement the transfer tool used to effectively ensure the required level of protection, or
- to fulfil its obligation to suspend the transfer and/or terminate the contract if the law of the third country, the safeguards contained in the transfer tool used and any additional safeguards it may have adopted can no longer ensure the essentially equivalent level of protection.



Safeguards to be provided for transfers outside the EEA

,'No backdoor policy'





To the best of its knowledge the Service Provider has not implemented any „back doors“. The development and operations IT teams of the Service Provider will follow the internal guidelines and processes of the Service Provider.

„No backdoor policy“



- Internal guidelines and limited commitments provide for limited assurance.
- „No backdoor policy“ part of contractual supplementary measures that may need to be included in transfer tools following Schrems II – **turn principle into a contractual obligation and legally binding commitment for the parties.**
- **„No back door policy“ clause** important to guarantee an adequate level of protection of the personal data transferred and **should usually be required.**
- The existence of legislation or government policies preventing importers from disclosing this information may render this clause ineffective. The importer will thus not be able to enter into the contract or will need to notify to the exporter of its inability to continue complying with its contractual commitments.

„No backdoor policy“



Need to include clauses whereby provider **certifies** that:

- it has not purposefully created back doors or similar programming that could be used to access the system and/or personal data
- it has not purposefully created or changed its business processes in a manner that facilitates access to personal data or systems, and
- national law or government policy does not require the importer to create or maintain back doors or to facilitate access to personal data or systems or for the importer to be in possession or to hand over the encryption key.



Safeguards to be provided for transfers outside the EEA

Technical supplementary measures
- encryption at rest and in transit





Safeguards to be provided for transfers outside the EEA

Technical supplementary measures
- pseudonymisation





Safeguards to be provided for transfers outside the EEA

Technical supplementary measures
- access control





Safeguards to be provided for transfers outside the EEA

Organisational supplementary measures

- provision of information on transfers





Safeguards to be provided for transfers outside the EEA

Organisational supplementary measures
- processing as instructed





Safeguards to be provided for transfers outside the EEA

Organisational supplementary measures
- transparency reports

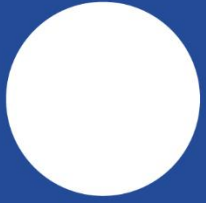




Safeguards to be provided for transfers outside the EEA

Organisational supplementary measures
- dedicated trainings





Recap TIA...

Transfer Impact Assessment 1/2



Before transfer, assess the impact of the transfer:

- take into account **circumstances of the transfer***
- assess whether **relevant legislation** of the third country of destination enables the data importer to **comply in practice with the guarantees** provided through the transfer tool of **Article 48 EUDPR** used:

✓ **If able** to comply in practice → **proceed with transfer**

✗ **If not able** to comply in practice → **assess further:**

- take into account **circumstances of the transfer***
- assess whether you can implement **supplementary measures** to ensure an **essentially equivalent level** of protection as provided in the EU and
- whether the relevant **measures** would be **effective** in light of the relevant legislation of the third country

→ *continued...*

Steps 1-2

Steps 3-4

Transfer Impact Assessment 2/2

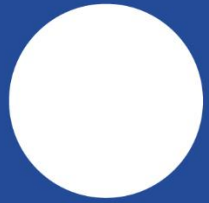


... continued

- Taking into account the **circumstances of the transfer and possible supplementary measures**, appropriate safeguards of Article 48 EUDPR:
 - ✗ **would not be ensured:**
 - **required to avoid, suspend or terminate the transfer of personal data to destination → notify EDPS**
 - if intending to **start / keep transferring data to destination despite negative conclusion → notify EDPS**
 - **EDPS decides to take enforcement action**
 - ✓ **would be ensured → proceed with transfer → periodically re-evaluate & take action**

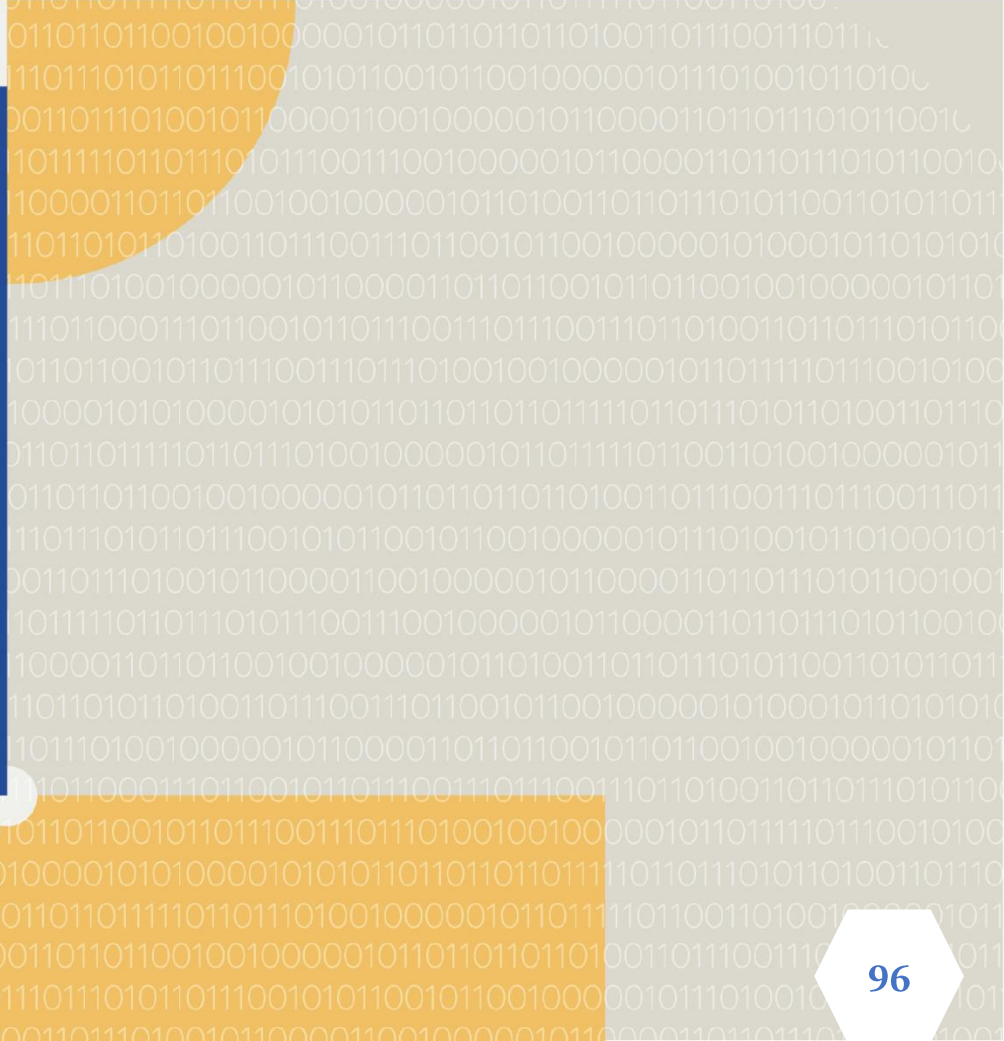
Steps 3-4

+ Steps 5-6



Whant now?

Take aways!



In a nutshell!



You have rights and obligations! Know your transfers!



Control sub-processing and data flows!



Essentially equivalent level of protection as in EU must be ensured for all international transfers!



Assess if the 3rd country / internat. organisation ensures the required level and if any supplementary measures are needed!



Consult your DPO!



Re-evaluate periodically if the required level of protection is still ensured and take action if necessary!



thank you!

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data
protection authority



@EU_EDPS



European Data
Protection Supervisor



EDPS