



EUDPR:

International Transfers

EDPS training at EUSA, 18 November 2020

Legal officers


Supervision and Enforcement Unit, EDPS

What is Personal data ?

*"Any
information
relating to an
identified
or identifiable
natural
person."*

- **Any information**
 - Name, e-mail address, signature, credit card number, photo, phone number...
- **Identified or identifiable**
 - VAT number, tax number, fingerprint, location data ...
 - **Not** anonymous data
- **Natural person** ≠ EU institutions, companies, legal entities
- **NB: personal ≠ confidential:** public information on the internet or submitted personal data are protected personal data





Not all data
are equal

- Some data are more sensitive than others and require ‘special’ protection: risks for freedoms
- These are data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.
- **Principle of PROHIBITION of processing**

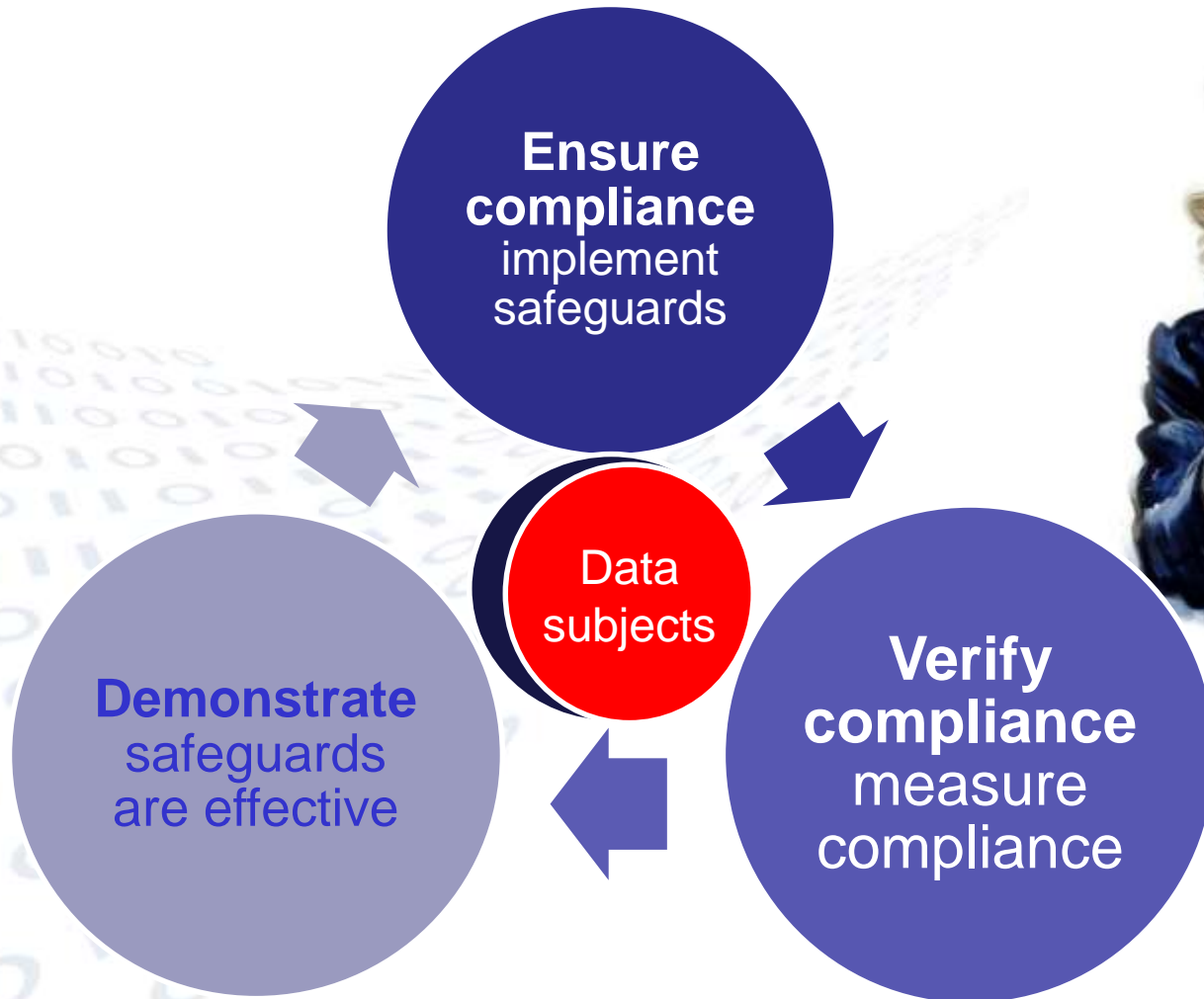
What is a processing operation?

- Operation performed upon personal data;
- Manual or automatic, such as
 - ✓ collection,
 - ✓ recording,
 - ✓ organisation,
 - ✓ storage,
 - ✓ adaptation or alteration,
 - ✓ retrieval,
 - ✓ consultation,
 - ✓ use,
 - ✓ disclosure by transmission,
 - ✓ dissemination,
 - ✓ blocking,
 - ✓ restriction,
 - ✓ erasure,
 - ✓ destruction etc.

Accountability

(*NEW* Articles 4(2) & 26 EUDPR)

Shift from mere (formal) compliance to risk-based approach



How should EUIs ensure, verify and demonstrate compliance?

Implement all DP principles

- Lawfulness
- Purpose limitation
- Data minimisation
- Data quality
- Data storage
- Security measures

Records

- **written description** of your processing
- allows for your **risk assessment**
- easy way for **answering access requests**

Data protection notice

- **inform** all individuals concerned in a clear & plain language, visible manner = **fair processing**



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



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



Transfer of personal data

What is a transfer

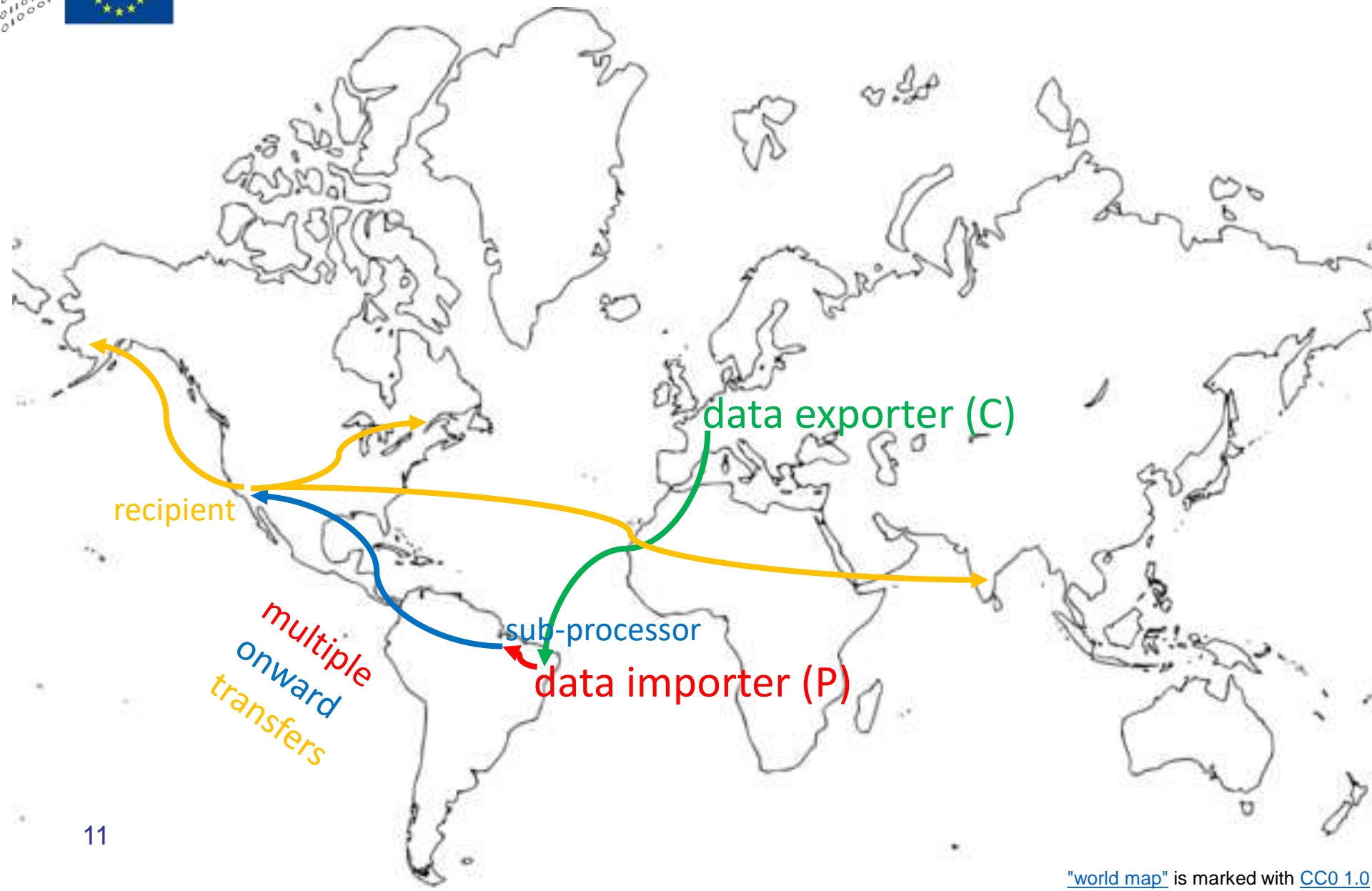
- "deliberate transfer" of personal data
- "permitted access" to personal data
- excludes cases of access through illegal actions (e.g. hacking)
- access is sufficient – no storage required



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.





Recipients

Recital 21
Article 9

EUI

EU Member State / EEA

Chapter V

Third country

International organisation

Conditions apply

Compliance with Regulation 2018/1725

Data transfer

- lawful
- necessary
- proportionate
- no risks for data subjects
- documented (assessment and transfer)



Consult DPO / DPC



International Transfers

Chapter V Article 46 – General principles

- ✓ Transfers to third countries and International Organisations
- ✓ Essentially equivalent level of protection
- ✓ Protection of individuals not undermined
- ✓ Two step approach: comply EUDPR → Chapter V
- ✓ Three types: → adequacy decisions
 - appropriate safeguards
 - derogations



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

Adequacy decision

- Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, Uruguay 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)

Appropriate safeguards with EDPS authorisation

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

Derogations

- Explicit consent 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



International Transfers

Article 47 – Adequacy

- ✓ adopted by the EC
- ✓ essentially equivalent level of protection
- ✓ can cover a third country, an IO, specific sector
- ✓ no need to adopt additional safeguards
- ✓ EUIs shall notify EC and the EDPS if conditions are no longer met



Adequacy decisions (Art. 46 EUDPR)

Adequacy decision

- Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan (GDPR), Jersey, New Zealand, Switzerland, Uruguay and the USA (~~limited to the Privacy Shield framework~~)
- ongoing talks with South Korea
- do not cover law enforcement sector (Art. 36 LED)



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 a 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
- enforceable data subject rights and effective legal remedies for data subjects are available
- consultation or authorization 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)

Appropriate
safeguards
with EDPS
authorisation

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



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

Legally binding instrument

- international agreement
- establish transfer and appropriate safeguards
 - legally binding safeguards
 - Article 42 consultation



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

Standard Contractual Clauses

- EC or EDPS + comitology procedure
- no authorization required
- no changes
- included in contract or complemented if there is no contradiction
- under revision



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

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

Codes of Conduct and Certifications



Article 48 (3) – Appropriate safeguards (EDPS authorization required)

Ad-hoc contractual clauses

- between controller – processor or processor –recipient in third country
- EDPS authorization required for the transfer
- if SCCs are changed they may become ad-hoc clauses
- appropriate safeguards



Article 48 (3) – Appropriate safeguards (EDPS authorization required)

Administrative arrangements

- between public authorities
- EDPS authorization required for the transfer
- non-binding
- enforceable and effective rights for data subjects
- EDPB guidelines 2/2020



Transfers to public authorities and international organisations

Practical requirements
- provide basic, but comprehensive information on the transfer

- definitions of the basic personal data concepts and rights
- scope of competencies and list of the authorities in the third country that would receive the data,
- categories of personal data affected and type of processing of the personal data that are transferred and processed,
- prohibition of further processing incompatible with the initial purpose of the exchange of data.
- scope and principle of purpose limitation



Transfers to public authorities and international organisations

Practical requirements
- provide basic, but comprehensive information on the transfer

- other basic principles of data protection, data accuracy and data minimisation, storage limitation, commitment to have technical and organisational measures in place to ensure confidentiality and security of processing,
- transparency obligations towards data subjects, reference to data subjects' rights, restrictions, redress mechanisms
- prohibition of onward transfers or sharing data with third parties
- internal and independent external review mechanism
- procedures for personal data breaches



Article 49 - Transfers and disclosures not authorised by Union law

- judgements or administrative decisions of third countries can be a basis for transfer
- only if an international agreement is in place (MLAT)
- no transfer without specific legal basis in EU law
- level of protection for individuals to be guaranteed
- Protocol on Privileges and Immunities TFEU



Article 50 - Derogations

Transfers:

- ✓ occasional
- ✓ not regular
- ✓ outside the regular course of actions
- ✓ exceptional circumstances

Transfers

- ✗ repeated
- ✗ massive
- ✗ structural
- ✗ regular in course of stable relationship

Art. 48 EUDPR



Article 50 - Derogations

- a) Explicit consent to transfer
- b) Contract with data subject
- c) Contract in interest of data subject
- d) Important reasons of public interest
- e) Legal claims
- f) Vital interests of data subject / others
- g) Public register

Necessity test for b), c), d), e) and f) for the specific purpose of the derogation to be used.

EDPB 2/2018 Guidelines



Article 50 - Derogations

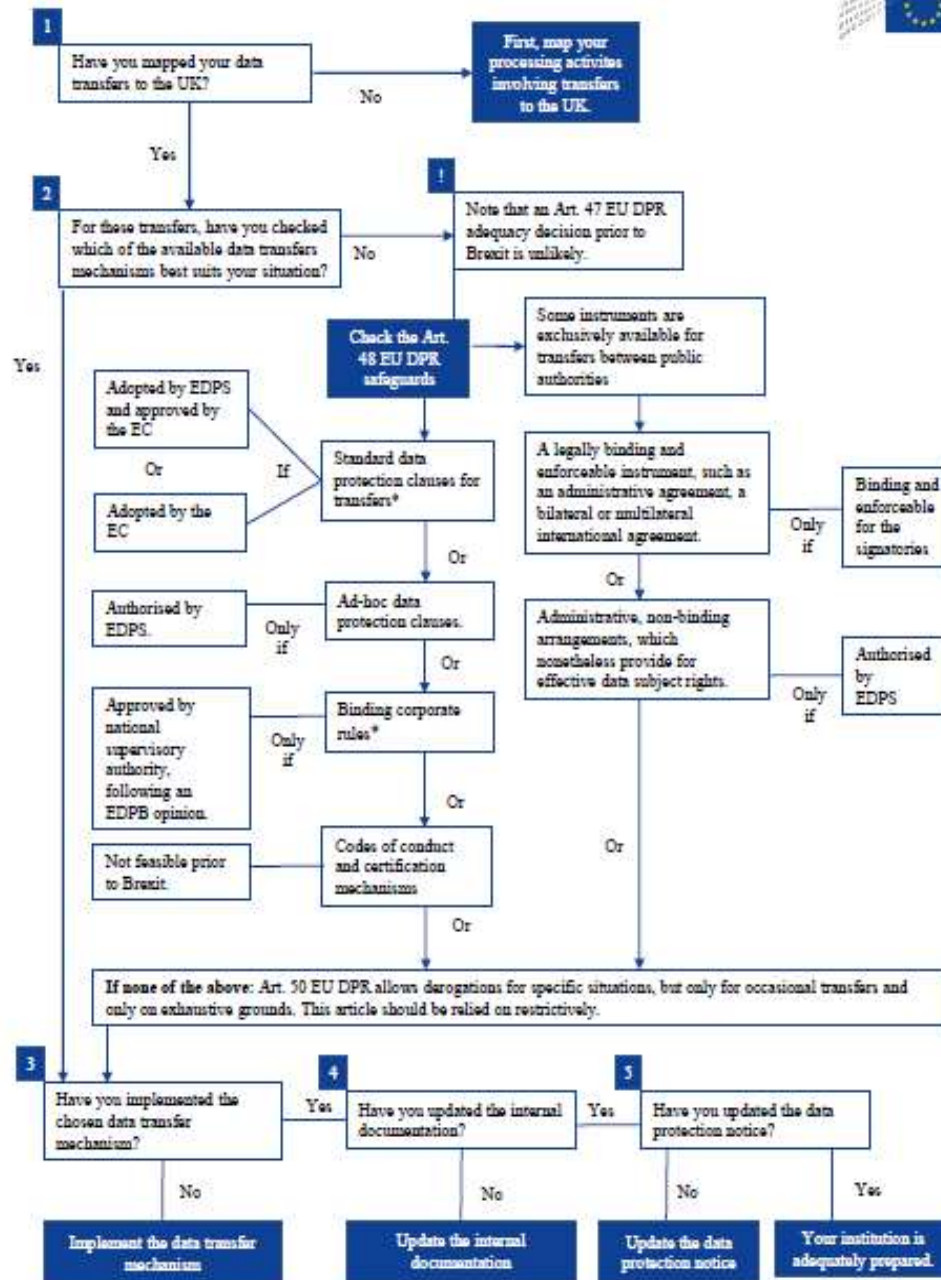
Consent

- - explicit
 - specific for the particular data transfer/set of transfers
 - informed as to the possible risks of the transfer

BREXIT

- Brexit 31 January 2020
- Transitory period – GDPR applies
- 31 December 2020
- 1 January 2021 – UK will be a third country
- no adequacy decision yet
- no codes of conduct or certifications
- further action or approval needed for BCRs authorised / approved by ICO if to apply within EEA

Flowchart: data transfers in the context of Brexit



* Binding corporate rules and standard contractual clauses (adopted by the EC) under the old Directive 95/46 are still valid, but will need to be updated over time in line with the GDPR. In any case, before using old EC standard contractual clauses, you should make sure to adapt them to Regulation (EU) 2018/1725 [EU DPR].



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**
- ➔ ~~Privacy Shield~~**

required level is adequate protection = essentially equivalent protection

- ✓ SCCs for transfers 2010/87/EC valid**
 - if effective mechanisms to ensure compliance with required level of protection**
 - if not possible, suspend or prohibit the transfer of personal data to the third country concerned**
- ✓ tools in Art. 46 GDPR¹ / ¹ Art. 48 EUDPR can be used if essentially equivalent level of protection can be ensured**



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

new

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

updated

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 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. 46¹ GDPR 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



EDPS Strategy for EU institutions to comply with “Schrems II” Ruling

**What
EUIs
need
to do**

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

Annex 2 of EDPB Rec. 1/2020 – 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),
- check that your transfer 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 tool for regular and repetitive transfers → proceed with next steps
- Art. 50 EUDPR 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,
- for what elements to assess on surveillance, see EDPB EEG recommendations,
- likelihood of public authorities' access in practice should not be taken into account

Roadmap of steps 2/2



Step 4

Identify and adopt effective supplementary measures

- combine technical + contractual + organisational measures [not alone!],
- not guarantee 0 risk, but ensure essentially equivalent level of protection

Step 5

Take any formal procedural steps that may be required

- EDPB will give further guidance 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, and if necessary take appropriate action



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 list 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, data protection notices, info from importer



Circumstances of the transfer 1/3

Could be relevant:

- Third country of destination? Remote access?*
- Purposes of transfer and processing?*
- Is the transfer part of a processing operation subject to DPIA?*
- Does the transfer involve special categories of data or data relating to criminal convictions and offences? Does the transfer involve any other personal data of sensitive or highly personal nature?***
- What categories of data subjects are concerned by the transfer (e.g. children, elderly people, patients, employees)?***

→ *continued...*



Circumstances of the transfer 2/3

- Description of the data importer and exporter (if not you) (if private entity, in which sector? public authority? international organisation?)*
- Does the transfer imply large scale processing?*
- Is the transfer part of a complex processing operation?*
- Are the transferred data simply stored or further analysed? By data exporter and/or data importer?*
- In what format is the data?* * Is pseudonymisation used? How? Is encryption used? What type of encryption and how (protocols and keys, in transit and/or at rest, end-to-end or server to server etc.)? Are there any other technical measures (specific privacy enhancing technologies) used?

continued...



Circumstances of the transfer 3/3

- What other contractual, organisational or technical measures and safeguards have been implemented? Have you, processor and/or the data importer checked the implementation and effectiveness of these measure and safeguards?
- In case the involvement of sub-processors is provided, are the organisational or technical measures and safeguards implemented by the data importer also implemented by the sub-processors?
- Which appropriate safeguard of Chapter V is used? Is transfer not based on any transfer tool or is it based on derogations?
- Have you (controller) envisaged (allowed) onward transfers or explicitly prohibited them? If onward transfers are allowed, to which recipients (e.g. sub-processors)?**



The applicable legal context will depend on the circumstances of the transfer, in particular:

- * Purposes for which the data are transferred and processed (e.g. marketing, HR, storage, IT support, clinical trials)
- * Types of entities involved in the processing (public/private; controller/processor).
- * Sector in which the transfer occurs (e.g. adtech, telecommunication, financial, etc)
- * Categories of personal data transferred (e.g. personal data relating to children may fall within the scope of specific legislation in the third country)
- * Whether the data will be stored in the third country or whether there is only remote access to data stored within the EU/EEA
- * Format of the data to be transferred (i.e. in plain text/ pseudonymised or encrypted)
- * Possibility that the data may be subject to onward transfers from the third country to another third country



Elements for assessing relevant 3rd country laws applicable to transfer and importer

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

- not referred to in EDPB recommendations on supplementary measures, however could be source for further inspiration for
- elements to consider when assessing relevant laws re: required level of protection in the specific transfer based on the Art. 48 EUDPR tool used
- do the relevant laws impinge on the specific commitments in the specific Art. 48 EUDPR tool used (e.g. effective execution of data subject rights, retention limitation, purpose limitation)?

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

- referred to in EDPB recommendations on supplementary measures to look at
- elements to assess if relevant laws on access by public authorities for surveillance unjustifiably interfere with required level of protection



Non-exhaustive list of factors (from circumstances of transfer) to identify which supplementary measures would be most effective in protecting the data transferred:

- * Format of the data to be transferred (i.e. in plain text/pseudonymised or encrypted)
- * Nature of the data
- * Length and complexity of data processing workflow, number of actors involved in the processing, and the relationship between them (e.g. do the transfers involve multiple controllers or both controllers and processors, or involvement of processors which will transfer the data from you to your data importer (considering the relevant provisions applicable to them under the legislation of the third country of destination))
- * Possibility that the data may be subject to onward transfers, within the same third country or even to other third countries (e.g. involvement of sub-processors of the data importer)



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...*



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**



Annex 2 of EDPB Rec. 1/2020 – Examples of supplementary measures

Technical measures

- ✓ Scenario's for which effective measures could be found
- ✗ Scenarios in which no effective measures could be found
- + Conditions for effectiveness

Additional contractual measures

- ✓ Supplementary measures
- ❖ Supplementary measures to complement other supplementary measures
- + Conditions for effectiveness

Additional organisational measures

- ✓ Supplementary measures
- ❖ Supplementary measures to complement other supplementary measures
- + Conditions for effectiveness



Technical measures

- ✓ **EXAMPLES DESCRIBED IN A NON-EXHAUSTIVE MANNER IN DIFFERENT SCENARIOS OF USE CASES**
- **ESPECIALLY WHERE THE RELEVANT LAW OF THE THIRD COUNTRY IMPOSES ON THE IMPORTER OBLIGATIONS WHICH:**
 - **ARE CONTRARY TO SAFEGUARDS OF ARTICLE 46 GDPR¹ TRANSFER TOOLS AND**
 - **ARE, IN PARTICULAR, CAPABLE OF IMPINGING ON THE CONTRACTUAL GUARANTEE OF AN ESSENTIALLY EQUIVALENT LEVEL OF PROTECTION AGAINST ACCESS BY THE PUBLIC AUTHORITIES OF THAT THIRD COUNTRY TO THAT DATA**
 - **MAY NEED TO BE COMPLEMENTED WITH CONTRACTUAL AND ORGANISATIONAL MEASURES**
 - **BUT AT LEAST WITH ADDITIONAL CONTRACTUAL COMMITMENT THAT THE SPECIFIC TECHNICAL MEASURES WILL BE IMPLEMENTED**

¹ Article 48 EUDPR



Examples of technical supplementary measures

Scenario's for which effective measures could be found

- ✓ **USE CASE 1: DATA STORAGE FOR BACKUP AND OTHER PURPOSES THAT DO NOT REQUIRE ACCESS TO DATA IN THE CLEAR** – robust state-of-the-art encryption of data with reliably managed cryptographic keys under sole control of data exporter
- ✓ **USE CASE 2: TRANSFER OF PSEUDONYMISED DATA** – pseudonymisation of data
- ✓ **USE CASE 3: ENCRYPTED DATA MERELY TRANSITING THIRD COUNTRIES** – transport encryption + if needed end-to-end content encryption
- ✓ **USE CASE 4: PROTECTED RECIPIENT** – end-to-end content encryption + transport encryption
- ✓ **USE CASE 5: SPLIT OR MULTI-PARTY PROCESSING** – split processing + (optionally) secure multi-party computation

Scenarios in which no effective measures could be found

- ✗ **USE CASE 6: TRANSFER TO CLOUD SERVICES PROVIDERS OR OTHER PROCESSORS WHICH REQUIRE ACCESS TO DATA IN THE CLEAR**
- ✗ **USE CASE 7: REMOTE ACCESS TO DATA FOR BUSINESS PURPOSES**





Additional contractual measures

- ✓ **GENERALLY ARE UNILATERAL, BILATERAL OR MULTILATERAL CONTRACTUAL COMMITMENTS IN ADDITION TO THOSE IN ARTICLE 46 GDPR¹ TRANSFER TOOLS**
- **MAY COMPLEMENT AND REINFORCE THE SAFEGUARDS THE TRANSFER TOOL AND RELEVANT LEGISLATION OF THE THIRD COUNTRY MAY PROVIDE, WHEN, TAKING INTO ACCOUNT THE CIRCUMSTANCES OF THE TRANSFER, THESE DO NOT MEET ALL THE CONDITIONS REQUIRED TO ENSURE A LEVEL OF PROTECTION ESSENTIALLY EQUIVALENT TO THAT GUARANTEED WITHIN THE EU**
- **NEED TO BE COMPLEMENTED WITH TECHNICAL AND ORGANISATIONAL MEASURES**

/¹ Article 48 EUDPR



Additional contractual measures

- **WILL NOT NECESSARILY AND SYSTEMATICALLY ENSURE THAT YOUR TRANSFER MEETS THE ESSENTIAL EQUIVALENCE STANDARD THAT EU LAW REQUIRES**
- **MAY ALSO BE HELPFUL TO ALLOW EEA-BASED DATA EXPORTERS TO BECOME AWARE OF NEW DEVELOPMENTS AFFECTING THE PROTECTION OF THE DATA TRANSFERRED TO THIRD COUNTRIES**
- **WILL NOT BE ABLE TO RULE OUT THE APPLICATION OF THE LEGISLATION OF A THIRD COUNTRY WHICH DOES NOT MEET THE EDPB EUROPEAN ESSENTIAL GUARANTEES STANDARD IN THOSE CASES IN WHICH THE LEGISLATION OBLIGES IMPORTERS TO COMPLY WITH THE ORDERS THEY RECEIVE FROM PUBLIC AUTHORITIES TO DISCLOSE DATA**



Examples of additional contractual supplementary measures

1/6

Obligation to use specific technical measures:

- ✓ **DEPENDING ON THE SPECIFIC CIRCUMSTANCES OF THE TRANSFERS, PROVIDE FOR THE CONTRACTUAL OBLIGATION TO USE SPECIFIC TECHNICAL MEASURES FOR TRANSFERS TO TAKE PLACE**

Transparency obligations:

- ❖ **ADD ANNEXES TO THE CONTRACT WITH INFORMATION THAT THE IMPORTER WOULD PROVIDE, BASED ON ITS BEST EFFORTS, ON THE ACCESS TO DATA BY PUBLIC AUTHORITIES, INCLUDING IN THE FIELD OF INTELLIGENCE PROVIDED THE LEGISLATION COMPLIES WITH THE EEGS, IN THE DESTINATION COUNTRY. THIS MIGHT HELP THE DATA EXPORTER TO MEET ITS OBLIGATION TO DOCUMENT ITS ASSESSMENT OF THE LEVEL OF PROTECTION IN THE THIRD COUNTRY.**



Transparency obligations:

- ❖ **ADD CLAUSES WHEREBY THE IMPORTER CERTIFIES THAT (1) IT HAS NOT PURPOSEFULLY CREATED BACK DOORS OR SIMILAR PROGRAMMING THAT COULD BE USED TO ACCESS THE SYSTEM AND/OR PERSONAL DATA, (2) IT HAS NOT PURPOSEFULLY CREATED OR CHANGED ITS BUSINESS PROCESSES IN A MANNER THAT FACILITATES ACCESS TO PERSONAL DATA OR SYSTEMS, AND (3) THAT 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.**
- ❖ **REINFORCE EXPORTER'S POWER TO CONDUCT AUDITS OR INSPECTIONS OF THE DATA PROCESSING FACILITIES OF THE IMPORTER, ON-SITE AND/OR REMOTELY, TO VERIFY IF DATA WAS DISCLOSED TO PUBLIC AUTHORITIES AND UNDER WHICH CONDITIONS (ACCESS NOT BEYOND WHAT IS NECESSARY AND PROPORTIONATE IN A DEMOCRATIC SOCIETY), FOR INSTANCE BY PROVIDING FOR A SHORT NOTICE AND MECHANISMS ENSURING THE RAPID INTERVENTION OF INSPECTION BODIES AND REINFORCING THE AUTONOMY OF THE EXPORTER IN SELECTING THE INSPECTION BODIES.**



Examples of additional contractual supplementary measures

3/6

- ✓ **WHERE THE LAW AND PRACTICE OF THE THIRD COUNTRY OF THE IMPORTER WAS INITIALLY ASSESSED AND DEEMED TO PROVIDE AN ESSENTIALLY EQUIVALENT LEVEL OF PROTECTION AS PROVIDED IN THE EU FOR DATA TRANSFERRED BY THE EXPORTER, STILL STRENGTHEN THE OBLIGATION OF THE DATA IMPORTER TO INFORM PROMPTLY THE DATA EXPORTER OF ITS INABILITY TO COMPLY WITH THE CONTRACTUAL COMMITMENTS AND AS A RESULT WITH THE REQUIRED STANDARD OF “ESSENTIALLY EQUIVALENT LEVEL OF DATA PROTECTION”**
- ❖ **INSOFAR AS ALLOWED BY NATIONAL LAW IN THE THIRD COUNTRY, THE CONTRACT COULD REINFORCE THE TRANSPARENCY OBLIGATIONS OF THE IMPORTER BY PROVIDING FOR A “WARRANT CANARY” METHOD, WHEREBY THE IMPORTER COMMITS TO REGULARLY PUBLISH (E.G. AT LEAST EVERY 24 HOURS) A CRYPTOGRAPHICALLY SIGNED MESSAGE INFORMING THE EXPORTER THAT AS OF A CERTAIN DATE AND TIME IT HAS RECEIVED NO ORDER TO DISCLOSE PERSONAL DATA OR THE LIKE. THE ABSENCE OF AN UPDATE OF THIS NOTIFICATION WILL INDICATE TO THE EXPORTER THAT THE IMPORTER MAY HAVE RECEIVED AN ORDER.**



OBLIGATIONS TO TAKE SPECIFIC ACTIONS:

- ❖ **THE IMPORTER COULD COMMIT TO REVIEWING, UNDER THE LAW OF THE COUNTRY OF DESTINATION, THE LEGALITY OF ANY ORDER TO DISCLOSE DATA, NOTABLY WHETHER IT REMAINS WITHIN THE POWERS GRANTED TO THE REQUESTING PUBLIC AUTHORITY, AND TO CHALLENGE THE ORDER IF, AFTER A CAREFUL ASSESSMENT, IT CONCLUDES THAT THERE ARE GROUNDS UNDER THE LAW OF THE COUNTRY OF DESTINATION TO DO SO. WHEN CHALLENGING AN ORDER, THE DATA IMPORTER SHOULD SEEK INTERIM MEASURES TO SUSPEND THE EFFECTS OF THE ORDER UNTIL THE COURT HAS DECIDED ON THE MERITS. THE IMPORTER WOULD HAVE THE OBLIGATION NOT TO DISCLOSE THE PERSONAL DATA REQUESTED UNTIL REQUIRED TO DO SO UNDER THE APPLICABLE PROCEDURAL RULES. THE DATA IMPORTER WOULD ALSO COMMIT TO PROVIDING THE MINIMUM AMOUNT OF INFORMATION PERMISSIBLE WHEN RESPONDING TO THE ORDER, BASED ON A REASONABLE INTERPRETATION OF THE ORDER.**



Examples of additional contractual supplementary measures

5/6

- ❖ **THE IMPORTER COULD COMMIT TO INFORM THE REQUESTING PUBLIC AUTHORITY OF THE INCOMPATIBILITY OF THE ORDER WITH THE SAFEGUARDS CONTAINED IN THE ARTICLE 46 GDPR¹ TRANSFER TOOL AND THE RESULTING CONFLICT OF OBLIGATIONS FOR THE IMPORTER. THE IMPORTER WOULD NOTIFY SIMULTANEOUSLY AND AS SOON AS POSSIBLE THE EXPORTER AND/OR THE COMPETENT SUPERVISORY AUTHORITY FROM THE EEA¹, INsofar AS POSSIBLE UNDER THE THIRD COUNTRY LEGAL ORDER.**

Empowering data subjects to exercise their rights:

- ✓ **PROVIDE THAT ACCESS TO THE PERSONAL DATA TRANSMITTED IN PLAIN TEXT IN THE NORMAL COURSE OF BUSINESS (INCLUDING IN SUPPORT CASES) MAY ONLY BE ACCESSED WITH THE EXPRESS OR IMPLIED CONSENT OF THE EXPORTER AND/OR THE DATA SUBJECT**

^{/1} ART. 48 EUDPR, EDPS



Examples of additional contractual supplementary measures

6/6

- ✓ **OBLIGE THE IMPORTER AND/OR THE EXPORTER TO NOTIFY PROMPTLY THE DATA SUBJECT OF THE REQUEST OR ORDER RECEIVED FROM THE PUBLIC AUTHORITIES OF THE THIRD COUNTRY, OR OF THE IMPORTER'S INABILITY TO COMPLY WITH THE CONTRACTUAL COMMITMENTS, TO ENABLE THE DATA SUBJECT TO SEEK INFORMATION AND AN EFFECTIVE REDRESS (E.G. BY LODGING A CLAIM WITH HIS/HER COMPETENT SUPERVISORY AUTHORITY¹ AND/OR JUDICIAL AUTHORITY ¹ AND DEMONSTRATE HIS/HER STANDING IN THE COURTS OF THE THIRD COUNTRY)**
- ✓ **COMMIT THE EXPORTER AND IMPORTER TO ASSIST THE DATA SUBJECT IN EXERCISING HIS/HER RIGHTS IN THE THIRD COUNTRY JURISDICTION THROUGH AD HOC REDRESS MECHANISMS AND LEGAL COUNSELLING**

/¹ EDPS, CJEU



Additional organisational measures

- ✓ **INTERNAL POLICIES, ORGANISATIONAL METHODS, AND STANDARDS CONTROLLERS AND PROCESSORS COULD APPLY TO THEMSELVES AND IMPOSE ON THE IMPORTERS OF DATA IN THIRD COUNTRIES**
- **MAY CONTRIBUTE TO ENSURING CONSISTENCY IN THE PROTECTION OF PERSONAL DATA DURING THE FULL CYCLE OF THE PROCESSING**
- **MAY ALSO IMPROVE THE EXPORTERS' AWARENESS OF RISK OF AND ATTEMPTS TO GAIN ACCESS TO THE DATA IN THIRD COUNTRIES, AND THEIR CAPACITY TO REACT TO THEM**
- **MAY NEED TO COMPLEMENT CONTRACTUAL AND/OR TECHNICAL MEASURES**



Examples of additional organisational supplementary measures 1/4

Internal policies for governance of transfers especially with groups of enterprises:

- ❖ **ADOPTION OF ADEQUATE INTERNAL POLICIES WITH CLEAR ALLOCATION OF RESPONSIBILITIES FOR DATA TRANSFERS, REPORTING CHANNELS AND STANDARD OPERATING PROCEDURES FOR CASES OF COVERT OR OFFICIAL REQUESTS FROM PUBLIC AUTHORITIES TO ACCESS THE DATA; CREATING SPECIFIC EEA BASED EXPERT TEAMS TO DEAL WITH REQUESTS THAT INVOLVE PERSONAL DATA TRANSFERRED FROM THE EU; THE NOTIFICATION TO THE SENIOR LEGAL AND CORPORATE MANAGEMENT AND TO THE DATA EXPORTER UPON RECEIPT OF SUCH REQUESTS; THE PROCEDURAL STEPS TO CHALLENGE DISPROPORTIONATE OR UNLAWFUL REQUESTS AND THE PROVISION OF TRANSPARENT INFORMATION TO DATA SUBJECTS**



Examples of additional organisational supplementary measures 2/4

Transparency and accountability measures:

- ❖ **DOCUMENT AND RECORD THE REQUESTS FOR ACCESS RECEIVED FROM PUBLIC AUTHORITIES AND THE RESPONSE PROVIDED, ALONGSIDE THE LEGAL REASONING AND THE ACTORS INVOLVED (E.G. IF THE EXPORTER HAS BEEN NOTIFIED AND ITS REPLY, THE ASSESSMENT OF THE TEAM IN CHARGE OF DEALING WITH SUCH REQUESTS, ETC.). THESE RECORDS SHOULD BE MADE AVAILABLE TO THE DATA EXPORTER, WHO SHOULD IN TURN PROVIDE THEM TO THE DATA SUBJECTS CONCERNED WHERE REQUIRED**
- ❖ **REGULAR PUBLICATION OF TRANSPARENCY REPORTS OR SUMMARIES REGARDING GOVERNMENTAL REQUESTS FOR ACCESS TO DATA AND THE KIND OF REPLY PROVIDED, INSOFAR PUBLICATION IS ALLOWED BY LOCAL LAW**



Examples of additional organisational supplementary measures 3/4

Organisation methods and data minimisation measures:

- ❖ **ALREADY EXISTING ORGANISATIONAL REQUIREMENTS UNDER THE ACCOUNTABILITY PRINCIPLE (E.G. ADOPTION OF STRICT AND GRANULAR DATA ACCESS AND CONFIDENTIALITY POLICIES AND BEST PRACTICES, BASED ON A STRICT NEED-TO-KNOW PRINCIPLE, MONITORED WITH REGULAR AUDITS AND ENFORCED THROUGH DISCIPLINARY MEASURES). DATA MINIMISATION IN ORDER TO LIMIT THE EXPOSURE OF PERSONAL DATA TO UNAUTHORISED ACCESS**
- ❖ **DEVELOPMENT OF BEST PRACTICES TO APPROPRIATELY AND TIMELY INVOLVE AND PROVIDE ACCESS TO INFORMATION TO THE DPO, IF EXISTENT, AND TO THE LEGAL AND INTERNAL AUDITING SERVICES ON MATTERS RELATED TO INTERNATIONAL TRANSFERS OF PERSONAL DATA TRANSFERS**



Examples of additional organisational supplementary measures 4/4

Adoption of standards and best practices:

- ❖ **ADOPTION OF STRICT DATA SECURITY AND DATA PRIVACY POLICIES, BASED ON EU CERTIFICATION OR CODES OF CONDUCTS OR ON INTERNATIONAL STANDARDS (E.G. ISO NORMS) AND BEST PRACTICES (E.G. ENISA) WITH DUE REGARD TO THE STATE OF THE ART, IN ACCORDANCE WITH THE RISK OF THE CATEGORIES OF DATA PROCESSED AND THE LIKELIHOOD OF ATTEMPTS FROM PUBLIC AUTHORITIES TO ACCESS IT**

Others:

- ❖ **ADOPTION AND REGULAR REVIEW OF INTERNAL POLICIES TO ASSESS THE SUITABILITY OF THE IMPLEMENTED COMPLEMENTARY MEASURES AND IDENTIFY AND IMPLEMENT ADDITIONAL OR ALTERNATIVE SOLUTIONS WHEN NECESSARY, TO ENSURE THAT AN EQUIVALENT LEVEL OF PROTECTION TO THAT GUARANTEED WITHIN THE EU OF THE PERSONAL DATA TRANSFERRED IS MAINTAINED**
- ❖ **COMMITMENTS FROM THE DATA IMPORTER TO NOT ENGAGE IN ANY ONWARD TRANSFER OF THE PERSONAL DATA WITHIN THE SAME OR OTHER THIRD COUNTRIES, OR SUSPEND ONGOING TRANSFERS, WHEN AN EQUIVALENT LEVEL OF PROTECTION OF THE PERSONAL DATA TO THAT AFFORDED WITHIN THE EU CANNOT BE GUARANTEED IN THE THIRD COUNTRY**



What now?

Take aways



In a nutshell for EUIs!



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 transfers!



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



Consult your DPO! Re-evaluate periodically and take action if necessary!

