EDPB Recommendations on supplementary measures

Supervision and Enforcement Unit
European Data Protection Supervisor
11/12/2020

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 GDPR[1] tool)
- identifying and implementing appropriate supplementary measures to the Art. 46[1] GDPR tool used to ensure effective compliance with that level of protection where the safeguards contained in the Art. 46 GDPR[1] 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 GDPR[1] tool used

[1]/ Art. 48 EUDPR

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

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

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 counrty 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

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

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**

+ Steps 5-6

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 GDPR[1] 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**

Use Case 1: Data storage for backup and other purposes that do not require access to data in the clear

79. A data exporter uses a hosting service provider in a third country to store personal data, e.g., for backup purposes.

If

1. the personal data is processed using strong encryption before transmission,
2. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the recipient country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them,
3. the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,
4. the encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification,
5. the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked), and
6. the keys are retained solely under the control of the data exporter, or other entities entrusted with this task which reside in the EEA or a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured,

then the EDPB considers that the encryption performed provides an effective supplementary measure.

Use Case 2: Transfer of pseudonymised Data

80. A data exporter first pseudonymises data it holds, and then transfers it to a third country for analysis, e.g., for purposes of research.

If

1. a data exporter transfers personal data processed in such a manner that the personal data can no longer be attributed to a specific data subject, nor be used to single out the data subject in a larger group, without the use of additional information[69],
2. that additional information is held exclusively by the data exporter and kept separately in a Member State or in a third country, territory or one or more specified sectors within a third country, or at an international organisation for which the Commission has established in accordance with Article 45 GDPR that an adequate level of protection is ensured,
3. disclosure or unauthorised use of that additional information is prevented by appropriate technical and organisational safeguards, it is ensured that the data exporter retains sole control of the algorithm or repository that enables re-identification using the additional information, and
4. the controller has established by means of a thorough analysis of the data in question taking into account any information that the public authorities of the recipient country may possess that the pseudonymised personal data cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information,

then the EDPB considers that the pseudonymisation performed provides an effective supplementary measure.

Use Case 3: Encrypted data merely transiting third countries

84. A data exporter wishes to transfer data to a destination recognised as offering adequate protection in accordance with Article 45 GDPR. The data is routed via a third country.

If

1. a data exporter transfers personal data to a data importer in a jurisdiction ensuring adequate protection, the data is transported over the internet, and the data may be geographically routed through a third country not providing an essentially equivalent level of protection,
2. transport encryption is used for which it is ensured that the encryption protocols employed are state-of-the-art and provide effective protection against active and passive attacks with resources known to be available to the public authorities of the third country,
3. decryption is only possible outside the third country in question,
4. the parties involved in the communication agree on a trustworthy public-key certification authority or infrastructure,
5. specific protective and state-of-the-art measures are used against active and passive attacks on transport-encrypted,
6. in case the transport encryption does not provide appropriate security by itself due to experience with vulnerabilities of the infrastructure or the software used, personal data is also encrypted end-to-end on the application layer using state-of-the-art encryption methods,
7. the encryption algorithm and its parameterization (e.g., key length, operating mode, if applicable) conform to the state-of-the-art and can be considered robust against cryptanalysis performed by the public authorities in the transiting country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them,
8. the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,
9. the encryption algorithm is flawlessly implemented by properly maintained software the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification,
10. the existence of backdoors (in hardware or software) has been ruled out,
11. the keys are reliably managed (generated, administered, stored, if relevant, linked to the identity of the intended recipient, and revoked), by the exporter or by an entity trusted by the exporter under a jurisdiction offering an essentially equivalent level of protection,

then the EDPB considers that transport encryption, if needed in combination with end-to-end content encryption, provides an effective supplementary measure.

Use Case 4: Protected recipient

85. A data exporter transfers personal data to a data importer in a third country specifically protected by that country's law, e.g., for the purpose to jointly provide medical treatment for a patient, or legal services to a client.

If

1. the law of a third country exempts a resident data importer from potentially infringing access to data held by that recipient for the given purpose, e.g. by virtue of a duty to professional secrecy applying to the data importer,
2. that exemption extends to all information in the possession of the data importer that may be used to circumvent the protection of privileged information (cryptographic keys, passwords, other credentials, etc.),
3. the data importer does not employ the services of a processor in a way that allows the public authorities to access the data while held by the processor, nor does the data importer forward the data to another entity that is not protected, on the basis of Article 46 GDPR transfer tools,
4. the personal data is encrypted before it is transmitted with a method conforming to the state of the art guaranteeing that decryption will not be possible without knowledge of the decryption key (end-to-end encryption) for the whole length of time the data needs to be protected,
5. the decryption key is in the sole custody of the protected data importer, and appropriately secured against unauthorised use or disclosure by technical and organisational measures conforming to the state of the art, and
6. the data exporter has reliably established that the encryption key it intends to use corresponds to the decryption key held by the recipient,

then the EDPB considers that the transport encryption performed provides an effective supplementary measure.

Use Case 5: Split or multi-party processing

86. The data exporter wishes personal data to be processed jointly by two or more independent processors located in different jurisdictions without disclosing the content of the data to them. Prior to transmission, it splits the data in such a way that no part an individual processor receives suffices to reconstruct the personal data in whole or in part. The data exporter receives the result of the processing from each of the processors independently, and merges the pieces received to arrive at the final result which may constitute personal or aggregated data.

If

1. a data exporter processes personal data in such a manner that it is split into two or more parts each of which can no longer be interpreted or attributed to a specific data subject without the use of additional information,
2. each of the pieces is transferred to a separate processor located in a different jurisdiction,
3. the processors optionally process the data jointly, e.g. using secure multi-party computation, in a way that no information is revealed to any of them that they do not possess prior to the computation,
4. the algorithm used for the shared computation is secure against active adversaries,
5. there is no evidence of collaboration between the public authorities located in the respective jurisdictions where each of the processors are located, which would allow them access to all sets of personal data held by the processors and enable them to reconstitute and exploit the content of the personal data in a clear form in circumstances where such exploitation would not respect the essence of the fundamental rights and freedoms of the data subjects. Similarly, public authorities of either country should not have the authority to access personal data held by processors in all jurisdictions concerned.
6. the controller has established by means of a thorough analysis of the data in question, taking into account any information that the public authorities of the recipient countries may possess, that the pieces of personal data it transmits to the processors cannot be attributed to an identified or identifiable natural person even if cross-referenced with such information,

then the EDPB considers that the split processing performed provides an effective supplementary measure.

Use Case 6: Transfer to cloud services providers or other processors which require access to data in the clear

88. A data exporter uses a cloud service provider or other processor to have personal data processed according to its instructions in a third country.

If

1. a controller transfers data to a cloud service provider or other processor,
2. the cloud service provider or other processor needs access to the data in the clear in order to execute the task assigned, and
3. the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,[71]

then the EDPB is, considering the current state of the art, incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights. The EDPB does not rule out that further technological development may offer measures that achieve the intended business purposes, without requiring access in the clear.

!

Use Case 7: Remote access to data for business purposes

90. A data exporter makes personal data available to entities in a third country to be used for shared business purposes. A typical constellation may consist of a controller or processor established on the territory of a Member State transferring personal data to a controller or processor in a third country belonging to the same group of undertakings, or group of enterprises engaged in a joint economic activity. The data importer may, for example, use the data it receives to provide personnel services for the data exporter for which it needs human resources data, or to communicate with customers of the data exporter who live in the European Union by phone or email.

If

1. a data exporter transfers personal data to a data importer in a third country by making it available in a commonly used information system in a way that allows the importer direct access of data of its own choice, or by transferring it directly, individually or in bulk, through use of a communication service,
2. the importer uses the data in the clear for its own purposes,
3. the power granted to public authorities of the recipient country to access the transferred data goes beyond what is necessary and proportionate in a democratic society,

! then the EDPB is incapable of envisioning an effective technical measure to prevent that access from infringing on data subject rights.

Additional contractual measures

- ✓ **GENERALLY ARE UNILATERAL, BILATERAL OR MULTILATERAL CONTRACTUAL COMMITMENTS IN ADDITION TO THOSE IN ARTICLE 46 GDPR[1] 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.**

Examples of additional contractual supplementary measures 2/6

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.**

Examples of additional contractual supplementary measures 4/6

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 GDPR[1] 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 EEA[1], 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 AUTHORITY[1] 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 organistional 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**

Thank you for your attention!

In a nutshell, EUIs have to

- ☑ Know transfers made by them or on their behalf!
- ☑ Control sub-processing and data flows!
- ☑ Ensure essentially equivalent level of protection as in EU for all international transfers!
- ☑ Assess if the third country or international organisation ensures the required level and if any supplementary measures are needed implement them!
- ☑ Consult you, their DPO!
- ☑ Re-evaluate periodically if the required level of protection is still ensured and take action if necessary!