ANNEX 1: Non-exhaustive lists of preliminary questions for EUI controllers for identifying circumstances of transfer and effective supplementary measures

With the aim to facilitate TIAs, the EDPS is providing EUIs with non-exhaustive lists of preliminary questions for EUI controllers to ask processors / data importers in view of obtaining more information on circumstances of the transfer and situation of processor / data importer in the third country.

Some preliminary questions that EUIs might want to ask based on the mapping exercise to processors / data importers to obtain **more information on the circumstances of the transfer**:

1) What is third country of destination to which the personal data will be transferred and processed? Will there be any remote access to personal data stored in the EEA or in the third country of destination? *

2) What are the purposes of transfer and processing? *

3) Is the transfer part of a processing operation subject to DPIA? +

4) Which data is transferred or remotely accessed? Does the transfer or processing involve special categories of data or data relating to criminal convictions and offences? Does the transfer or processing involve any other personal data of sensitive or highly personal nature? *+

5) What categories of data subjects are concerned by the transfer or processing (e.g. children, elderly people, patients, employees)? *+

6) Description of the data exporter (if not the EUI) and importer (if private entity, in which sector? public authority? international organisation?) *

7) Does the transfer imply large scale processing? +

8) Is the transfer part of a complex processing operation? +

9) Are the transferred data simply stored or further analysed? By data exporter and/or data importer? *

10) In what format is the data *+ (e.g. in plain text? Is pseudonymisation used? How? Is encryption used? What type of encryption is used 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?

11) What other contractual, organisational or technical measures and safeguards have been implemented? Have you the EUI, processor and/or the data importer checked the implementation and effectiveness of these measure and safeguards?

12) 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?

13) Which transfer tool under Chapter V EUDPR / Chapter V GDPR is used? If an appropriate safeguard under Article 48 EUDPR / Article 46 GDPR is used [more specifically, the Standard Contractual Clauses for transfers under Directive 95/46/EC adopted by COM[1] and under the GDPR, binding corporate rules (Article 46(2)(b) GDPR and Article 48(2)(d) EUDPR)), ad hoc clauses for transfers under the GDPR or EUDPR], a copy is to be provided to the EUI. Is transfer not based on any transfer tool or is it based on derogations?

14) Have you the EUI (controller) envisaged (allowed) onward transfers or explicitly prohibited them? If onward transfers are allowed, who allowed them and to which recipients (e.g. sub-processors) and what safeguards have been put in place? *+

Some preliminary questions that EUIs might want to ask processors / data importers to obtain **more information on the situation of the processor / data importer in the third country, in particular applicable legislation**:

1) What is the legal framework of the third country directly or indirectly applicable to the specific transfer in question and to the processor / data importer? In particular, what is the applicable legislation in the field of surveillance by authorities in third country? *

2) In the view of the processor / data importer, could the relevant applicable third country legislation negatively impact on the effectiveness of the appropriate safeguards transfer tool used in the context of the specific transfer? *

3) In the view of the processor / data importer, is there any obligation or duty to which in the processor / data importer may be subject under the relevant applicable legislation of the third country that could prevent

[1] SCCs pursuant to Commission decision 2001/497/EC, SCCs pursuant to Commission decision 2004/915/EC, SCCs pursuant to Commission decision 2010/87/EU.

the processor / data importer from complying with commitments in the appropriate safeguards transfer tool used or with other commitments undertaken by the processor / data importer as regards the transfer and processing? *

4) If legislation of the third country governing the access to data by public authorities is not publicly available, are there any measures in practice in the third country that could negatively impact on the effectiveness of the appropriate safeguards transfer tool used or that may prevent the processor / data importer from complying with the safeguards contained in that tool or with other commitments undertaken by the processor / data importer as regards the transfer and processing? *

5) Is the processor / data importer under a legal prohibition of informing about a specific request for access to data received? Is the processor / data importer under a legally restricted as regards providing general information about requests for access to data received or the absence of requests received? *+

6) Is the processor / data importer in the third country specifically protected by that country's law for the purpose of the transfer and processing? Does the law of the third country exempt the resident processor/ data importer from potentially infringing access to data held by that processor/ data importer for the given purpose, e.g. by virtue of a duty to professional secrecy applying to the processor/ data importer? If so, does that exemption extend to all information in the possession of the processor/ data importer that may be used to circumvent the protection of privileged information (cryptographic keys, passwords, other credentials, etc.)? *+

7) For transfers of personal data to the U.S. and processing in the U.S., is there any specific U.S. legislation, in particular in the field of surveillance (e.g. Section 702 FISA, E.O. 12333), applicable directly or indirectly to the processor / data importer? *+

8) For transfers of personal data to the U.S. and processing in the U.S., is the processor / data importer subject to any obligation under EU law, EU/EEA Member State law, corporate or public or private international law to ignore or not give effect to any disclosure or access request from any U.S. entity to disclose or give access to data to the U.S. government under Section 702 FISA or E.O. 12333? *+

9) Have any measures been implemented to protect against mass surveillance in transit? Have those measures been tested for effectiveness? [Note that these specific questions correlate to the general questions on any implemented technical measures above.] +

10) What legal, technical and organisational measures have been implemented to block access by public authorities? Have those measures been tested for effectiveness? [Note that these specific questions correlate to the general questions on any implemented legal (contractual), technical and organisational measures above.] +

11) Can the processor / data importer provide its last transparency report on government access requests?

The questions are formulated based on the circumstances that could be relevant when assessing the level of protection and the need for supplementary measures. Answers to these questions, together with the information from the mapping exercise, will help the EUI to know the circumstances of the transfers to take into account for the TIA. There is a lot of correlation between elements of the mapping of data flows and circumstances of the transfers, e.g. the country of destination, who is the data importer, what data is transferred or accessed. There is also a lot of correlation with the elements for identifying the relevant applicable laws in the third country (marked with "*" purple asterisk) and for identifying the use case scenario and any supplementary measures (marked with "+" orange plus sign).

The applicable legal context will depend on the circumstances of the transfer, in particular[2]:

* 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);

[2] See paragraph 33 of the EDPB Recommendations 01/2020.

* Possibility that the data may be subject to onward transfers from the third country to another third country.

Non-exhaustive list of factors (from circumstances of transfer) to identify which supplementary measures would be most effective in protecting the data transferred[3]:

+ Format of the data to be transferred (i.e. in plain text/pseudonymised or encrypted);

+ Nature of the data (e.g. a higher level of protection is afforded in the EEA to categories of data covered by Articles 10 and 11 EUDPR);

+ 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).

[3] See paragraph 54 of the EDPB Recommendations 01/2020.