ANNEX 2: EXAMPLES OF SUPPLEMENTARY MEASURES

69. The following measures are examples of supplementary measures you could consider when you reach Step 4 "Adopt supplementary measures". This list is not exhaustive. Selecting and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires. You should select those supplementary measures that can effectively guarantee this level of protection for your transfers.

70. Any supplementary measure may only be deemed effective in the meaning of the CJEU judgment "Schrems II" if and to the extent that it addresses the specific deficiencies identified in your assessment of the legal situation in the third country. If, ultimately, you cannot ensure an essentially equivalent level of protection, you must not transfer the personal data.

71. As a controller or processor, you may already be required to implement some of the measures described in this annex, even if your data importer is covered by an adequacy decision, just as you may be required to implement them when you process data within the EEA.[66]

Technical measures

72. This section describes in a non-exhaustive manner examples of technical measures, which may supplement safeguards found in Article 46 GDPR transfer tools to ensure compliance with the level of protection required under EU law in the context of a transfer of personal data to a third country. These measures will be especially needed where the law of that country imposes on the data importer obligations which are contrary to the safeguards of Article 46 GDPR 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[67].

73. For further clarity, this section specifies first the technical measures that could potentially be effective in certain scenarios/use-cases to ensure an essentially equivalent level of protection. The section continues with some scenarios/use cases in which no technical measures could be found to ensure this level of protection.

Scenarios for which *effective* measures could be found

74. The measures listed below are intended to ensure that access to the transferred data by public authorities in third countries does not impinge on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. These measures apply even if the public authorities' access complies with the law of the importer's country, where such access goes beyond what is necessary and proportionate in a democratic society[68]. These measures aim to preclude potentially infringing access by preventing the authorities from identifying the data subjects, inferring information about them, singling them out in another context, or associating the transferred data with other

[66] Article 5.2 GDPR, Article 32 GDPR.
[67] C-311/18 (Schrems II), paragraph 135.
[68] See Articles 47 and 52 of the EU Charter of Fundamental Rights, Article 23.1 GDPR, and EDPB Recommendations on the European Essential Guarantees for Surveillance Measures.

datasets they may possess that may contain, among other data, online identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts.

75. Public authorities in third countries may endeavour to access transferred data

a) In transit by accessing the lines of communication used to convey the data to the recipient country. This access may be passive in which case the contents of the communication, possibly after a selection process, are simply copied. The access may, however, also be active in the sense that the public authorities interpose themselves into the communication process by not only reading the content, but also manipulating or suppressing parts of it.

b) While in custody by an intended recipient of the data by either accessing the processing facilities themselves, or by requiring a recipient of the data to locate, and extract data of interest and turn it over to the authorities.

76. This section considers scenarios where measures are applied that are effective in both cases. Different supplementary measures may apply and be sufficient in the given circumstance of a concrete transfer if only one type of access is foreseen by the law of the recipient country. It is therefore necessary for the data exporter to carefully analyse, with the support of the data importer, the obligations laid upon the latter.

As an example, US data importers that fall under 50 USC § 1881a (FISA 702) are under a direct obligation to grant access to or turn over imported personal data that are in their possession, custody or control. This may extend to any cryptographic keys necessary to render the data intelligible.

77. The scenarios describe specific circumstances, and measures taken. Any changes to the scenarios may give rise to different conclusions.

78. Controllers may have to apply some or all of the measures described here irrespective of the level of protection provided for by the laws applicable to the data importer because they are needed to comply with Articles 25 and 32 GDPR in the concrete circumstances of the transfer. In other words, exporters may be required to implement the measures described in this paper even if their data importers are covered by an adequacy decision, just as controllers and processors may be required to implement them when data is processed within the EEA.

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.

81. Note that in many situations, factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of a natural person, their physical location or their interaction with an internet

[69] In line with Article 4(5) GDPR: "'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;".

based service at specific points in time[70] may allow the identification of that person even if their name, address or other plain identifiers are omitted.

82. This is particularly true whenever the data concern the use of information services (time of access, sequence of features accessed, characterisitics of the device used etc.). These services might well be, as for the importer of personal data, under the obligation to grant access to the same public authorities in their jurisdiction, which will then likely possess data about the use of those information services by the person(s) they target.

83. Moreover, given the use of some information services is public by nature, or their exploitability by parties with substantial resources, controllers will have to take extra care considering that public authorities in their jurisdiction likely possess data about the use of information services by a person they target.

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,

[70] Art. 4(1) GDPR: "' personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;".

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.

Scenarios in which *no effective* measures could be found

87. The measures described below under certain scenarios would not be effective in ensuring an essentially equivalent level of protection for the data transferred to the third country. Therefore, they would not qualify as supplementary measures.

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]

[71] See Articles 47 and 52 of the EU Charter of Fundamental Rights, Article 23.1 GDPR, and EDPB Recommendations on the European Essential Guarantees for Surveillance Measures.

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.

89. In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.

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.

91. In the given scenarios, where unencrypted personal data is technically necessary for the provision of the service by the processor, transport encryption and data-at-rest encryption even taken together, do not constitute a supplementary measure that ensures an essentially equivalent level of protection if the data importer is in possession of the cryptographic keys.

Additional contractual measures

92. These measures will generally consist of unilateral, bilateral or multilateral[72] contractual commitments.[73] If an Article 46 GDPR transfer tool is used, it will in most cases already contain a number of (mostly contractual) commitments by the data exporter and the data importer aimed at serving as safeguards for the personal data.[74]

93. In some situations, these measures 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. Provided the nature of contractual measures, generally not capable of binding the authorities of that third country, when they are not party to the contract[75], these measures should be combined with other technical and organisational measures to provide the level of data protection required. Selecting and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires.

94. Depending on what contractual measures are already included in the Article 46 GDPR transfer tool that is relied on, additional contractual measures 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.

95. As said, contractual measures 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 to disclose data they receive from public authorities.[76]

96. Some examples of these potential contractual measures are listed below and classified in accordance with their nature:

Providing for the contractual obligation to use specific technical measures

97. Depending on the specific circumstances of the transfers, the contract may need to provide that for transfers to take place, specific technical measures would have to be put in place (see supra the technical measures suggested).

98. Conditions for effectiveness:

[72] E.g. within BCRs which should in any case regulate some of the measures listed below.
[73] They will have a private nature and not be considered as international agreements under public international law. Accordingly, they will normally fail to bind the third country's public authority as non-parties to the contract when concluded with private bodies in third countries, as the Court underlined in its judgment C-311/18 (Schrems II), paragraph 125.
[74] See judgment C-311/18 (Schrems II), paragraph 137 where the Court as a result recognised that the SCC contain *« effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to the clauses of such a decision are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them »* see also paragraph 148).
[75] C-311/18 (Schrems II), paragraph 125.
[76] CJEU judgment C-311/18 (Schrems II), paragraph 132.

- This clause could be effective in those situations where the need for technical measures has been identified by the exporter. It would then have to be provided in a legal form to ensure that the importer also commits to put in place the necessary technical measures if need be.

Transparency obligations:

99. The exporter could 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 EDPB European Essential Guarantees, 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.

100. The importer could be for instance required to:

(1) enumerate the laws and regulations in the destination country applicable to the importer or its (sub) processors that would permit access by public authorities to the personal data that are subject to the transfer, in particular in the areas of intelligence, law enforcement, administrative and regulatory supervision applicable to the transferred data;
(2) in the absence of laws governing the public authorities' access to data provide information and statistics based on the importer's experience or reports from various sources (e.g. partners, open sources, national case law and decisions from oversight bodies) on access by public authorities to personal data in situations of the kind of the data transfer at hand (i.e. in the specific regulatory area; regarding the type of entities to which the data importer belongs;…)
(3) indicate which measures are taken to prevent the access to transferred data (if any);
(4) provide sufficiently detailed information on all requests of access to personal data by public authorities which the importer has received over a specified period of time,[77] in particular in the areas mentioned under (1) above and comprising information about the requests received, the data requested, the requesting body and the legal basis for disclosure and to what extent the importer has disclosed the data request;[78]
(5) specify whether and to what extent the importer is legally prohibited to provide the information mentioned under (1) – (5) above.

101. This information could be provided by way of structured questionnaires that the importer would fill in and sign and compounded by the importer's contractual obligation to declare within a set period of time any potential change to this information, as is current practice for due diligence processes.

102. Conditions for effectiveness:

- The importer must be able to provide the exporter with these types of information to the best of its knowledge and after having used its best efforts to obtain it.[79]

[77] The length of period should depend on the risk for the rights and freedoms of the data subjects whose data are subject to the transfer at stake – e.g. the last year before closure of the data export instrument with the data exporter
[78] Complying with this duty does not as such amount to providing for an appropriate level of protection. At the same time any inappropriate disclosure that has actually happened leads to the necessity of implementing supplementary measures.
[79] See paragraph 32.5 above.

- This obligation imposed on the importer is a means to ensure that the exporter becomes and remains aware of the risks attached to the transfer of data to a third country. It will thus enable the exporter to desist from concluding the contract, or if the information changes following its conclusion, 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 Article 46 GDPR transfer tool used and any additional safeguards it may have adopted can no longer ensure a level of protection essentially equivalent to that in the EU. This obligation can however neither justify the importer's disclosure of personal data nor give rise to the expectation that there will be no further access requests.

***

103. The exporter could also 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.[80]

104. Conditions for effectiveness:

- 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.[81]
- The contract must include penalties and/or the exporter's ability to terminate the contract on short notice in those cases in which the importer does not reveal the existence of a back door or similar programming or manipulated business processes or any requirement to implement any of these or fails to promptly inform the exporter once their existence comes to its knowledge.

***

105. The exporter could reinforce its power to conduct audits[82] 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.

106. Conditions for effectiveness:

- The scope of the audit should legally and technically cover any processing by the importer's processors or sub-processors of the personal data transmitted in the third country to be fully effective.

[80] This clause is important to guarantee an adequate level of protection of the personal data transferred and should usually be required.
[81] See paragraph 32.5 above.
[82] See for instance Clause 5.f of SCCs between controllers and processors Decision 2010/87/EU, the audits could also be provided within a code of conduct or through certification.

- Access logs and other similar trails should be tamper proof so that the auditors can find evidence of disclosure. Access logs and other similar trails should also distinguish between accesses due to regular business operations and accesses due to orders or requests for access.

***

107. 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, the exporter could 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".[83]

108. This inability to comply may result from changes in the third country's legislation or practice.[84] The clauses could set specific and strict time limits and procedures for the swift suspension of the transfer of data and/or the termination of the contract and the importer's return or deletion of the data received. Keeping track of the requests received, their scope, and the effectiveness of the measures adopted to counter them, should provide the exporter with sufficient indications to exercise its duty to suspend or end the transfer and/or terminate the contract.

109. Conditions for effectiveness:

- The notification needs to take place before access is granted to the data. Otherwise, by the time the exporter receives the notification, the rights of the individual may have already been violated if the request is based on laws of that third country that exceed what the level of data protection afforded under EU law permits. The notification may still serve to prevent future violations and to allow the exporter to fulfil its duty to suspend the transfer of personal data to the third country and/or terminate the contract.
- The data importer must monitor any legal or policy developments that might lead to its inability to comply with its obligations, and promptly inform the data exporter of any such changes and developments, and if possible ahead of their implementation to enable the data exporter to recover the data from the data importer.
- The clauses should provide for a quick mechanism whereby the data exporter authorises the data importer to promptly secure or return the data to the data exporter, or if this is not feasible, delete or securely encrypt the data without necessarily waiting for the exporter's instructions, if a specific threshold to be agreed between the data exporter and the data importer is met. The importer should implement this mechanism from the beginning of the data transfer and test it regularly to ensure that it can be applied on short notice.
- Other clauses could enable the exporter to monitor the importer's compliance with these obligations via audits, inspections and other verification measures and to enforce them with

[83] Clause 5.a and d.i of SCCs Decision 2010/87/EU.

[84] See C-311/18 (Schrems II), paragraph 139 in which the Court asserts that *"although Clause 5(d)(i) allows a recipient of personal data not to notify a controller established in the European Union of a legally binding request for disclosure of the personal data by a law enforcement authority, in the event of legislation prohibiting that recipient from doing so, such as a prohibition under criminal law the aim of which is to preserve the confidentiality of a law enforcement investigation, the recipient is nevertheless required, pursuant to Clause 5(a) in the annex to the SCC Decision, to inform the controller of his or her inability to comply with the standard data protection clauses."*

penalties on the importer and/or the exporter's capacity to suspend the transfer and/or terminate immediately the contract.

***

110. 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.

111. Conditions for effectiveness:

- The regulations of the third country must permit the data importer to issue this form of passive notification to the exporter.
- The data exporter must automatically monitor the warrant canary notifications.
- The data importer must ensure that its private key for signing the Warrant Canary is kept safe and that it cannot be forced to issue false Warrant Canaries by the regulations of the third country. To this end, it might be of use if several signatures by different persons are needed and/or the Warrant Canary is issued by a person outside the third country's jurisdiction.

Obligations to take specific actions

112. 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.

113. Conditions for effectiveness:

- The legal order of the third country must offer effective legal avenues to challenge orders to disclose data.
- This clause will always offer a very limited additional protection as an order to disclose data may be lawful under the legal order of the third country, but this legal order may not meet EU standards. This contractual measure will necessarily need to be complementary to other supplementary measures.
- The challenges to the orders must have a suspensive effect under the law of the third country. Otherwise, public authorities would still have access to the individuals' data and any ensuing action in favor of the individual would have the limited effect of allowing him/her to claim damages for negative consequences resulting from the data disclosure.
- The importer will need to be able to document and demonstrate to the exporter the actions it has taken, exercising its best efforts, to fulfill this commitment.

***

114. In the same situation as described above, the 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 transfer tool[85] 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, insofar as possible under the third country legal order.

115. Conditions for effectiveness:

- Such information on the protection conferred by EU law and the conflict of obligations should have some legal effect in the legal order of the third country, such as a judicial or administrative review of the order or request for access, the requirement of a judicial warrant, and/or a temporary suspension of the order to add some protection to the data.
- The legal system of the country must not prevent the importer from notifying the exporter or at least the competent supervisory authority from the EEA of the order or request for access received.
- The importer will need to be able to document and demonstrate to the exporter the actions it has taken, exercising its best efforts, to fulfill this commitment.

Empowering data subjects to exercise their rights

116. The contract could provide that 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.

117. Conditions for effectiveness:

- This clause could be effective in those situations in which importers receive requests from public authorities to cooperate on a voluntary basis, as opposed to e.g. data access by public authorities that occurs without the data importer's knowledge or against its will.
- In some situations the data subject may not be in a position to oppose the access or to give a consent that meets all the conditions set out under EU law (freely given, specific, informed, and unambiguous) (e.g in the case of employees)[86].
- National regulations or policies compelling the importer not to disclose the order for access may render this clause ineffective, unless it can be backed with technical methods requiring the exporter's or the data subject's intervention for the data in plant text to be accessible. Such technical measures to restrict access may be envisaged in particular if access is only granted in specific support or service cases, but the data itself is stored in the EEA.

[85] For instance, the SCCs provide that the processing of data, including the transfer thereof, has been and will continue to be carried out in accordance with *"the applicable data protection law".* This law is defined as *"the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established".* The CJEU confirms that the provisions of the GDPR, read in light of the EU Charter of Fundamental rights, form part of that legislation, see CJEU C-311/18 (Schrems II), paragraph 138.
[86] Article 4(11) GDPR.

***

118. The contract could 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 and/or judicial authority and demonstrate his/her standing in the courts of the third country).

119. Conditions for effectiveness:

- This notification could alert the data subject to potential accesses by public authorities in third countries to his/her data. It could thus enable the data subject to seek additional information with the exporters and to lodge a claim with his/her competent supervisory authority. This clause could also address some of the difficulties an individual may face in demonstrating his/her standing *(locus standi)* before third country courts to challenge the public authorities' access to his/her data.
- National regulations and policies may prevent this notification to the data subject. The exporter and importer could nonetheless commit to informing the data subject as soon as the restrictions on the disclosure of data are lifted and to make its best efforts to obtain the waiver of the prohibition to disclose. At a minimum, the exporter or the competent supervisory authority could notify the data subject of the suspension or termination of the transfer of his/her personal data due to the importer's inability to comply with its contractual commitments as a result of its receipt of a request for access.

***

120. The contract could 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.

121. Conditions for effectiveness

- National regulations and policies may impose conditions that may undermine the effectiveness of the ad hoc redress mechanisms provided for.
- Legal counselling could be helpful for the data subject, especially considering how complex and costly it can be for a data subject to understand a third country's legal system and to exercise legal actions from abroad, potentially in a foreign language. However, this clause will always offer a limited additional protection, as providing assistance and legal counselling to data subjects cannot in itself remedy a third country's legal order failure to provide for a level of protection essentially equivalent to that guaranteed within the EU. This contractual measure will necessarily need to be complementary to other supplementary measures.

This supplementary measure would only be effective provided that the law of the third country provides for redress before its national courts or that an ad hoc redress mechanism exist. In any case, this would however not be an efficient supplementary measure against surveillance measures if no redress mechanism exists.

Organisational measures

122. Additional organisational measures may consist of internal policies, organisational methods, and standards controllers and processors could apply to themselves and impose on the importers of data in third countries. They may contribute to ensuring consistency in the protection of personal data during the full cycle of the processing. Organisational measures 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. Selecting and implementing one or several of these measures will not necessarily and systematically ensure that your transfer meets the essential equivalence standard that EU law requires. Depending on the specific circumstances of the transfer and the assessment performed on the legislation of the third country, organisational measures are needed to complement contractual and/or technical measures, in order to ensure a level of protection of the personal data essentially equivalent to that guaranteed within the EU.

123. The assessment of the most suitable measures has to be done on a case by cases basis keeping in mind the need for controllers and processors to respect the accountability principle. Below, the EDPB lists some examples of organisational measures that exporters can implement, albeit the list is not exhaustive and other measures may also be appropriate :

Internal policies for governance of transfers especially with groups of enterprises

124. 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. Especially in case of transfers among groups of enterprises, these policies may include, among others, the appointment of a specific team, which should be based within the EEA, composed by experts on IT, data protection and privacy laws, 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.

125. Development of specific training procedures for personnel in charge of managing requests for access to personal data from public authorities, which should be periodically updated to reflect new legislative and jurisprudential developments in the third country and in the EEA. The training procedures should include the requirements of EU law as to access by public authorities to personal data, in particular as following from Article 52 (1) of the Charter of Fundamental Rights. Awareness of personnel should be raised in particular by means of assessment of practical examples of public authorities' data access requests and by applying the standard following from Article 52(1) of the Charter of Fundamental Rights to such practical examples. Such training should take into account the particular situation of the data importer, e.g. legislation and regulations of the third country to which the data importer is subject to, and should be developed where possible in cooperation with the data exporter.

126. Conditions for effectiveness:

- These policies may only be envisaged for those cases where the request from public authorities in the third country is compatible with EU law.[87] When the request is incompatible,

[87] See Case C-362/14 (« Schrems I »), par. 94; C-311/18 (Schrems II), paragraphs 168, 174, 175 and 176.

these policies would not suffice to ensure an equivalent level of protection of the personal data and, as said above, transfers must be stopped or appropriate supplementary measures to avoid the access must be put in place.

Transparency and accountability measures

127. 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.

128. Conditions for effectiveness:

- National legislation in the third country may prevent disclosure of the requests or substantial information thereof and therefore render this practice ineffective. The data importer should inform the exporter of its inability to provide such documents and records, thus offering the exporter the option to suspend the transfers if such inability would lead to a decrease of the level of protection.

***

129. 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.

130. Conditions for effectiveness:

- The information provided should be relevant, clear and as detailed as possible. National legislation in the third country may prevent disclosure of detailed information. In those cases, the data importer should employ its best efforts to publish statistical information or similar type of aggregated information.

Organisation methods and data minimisation measures

131. Already existing organisational requirements under the accountability principle, such as the 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 may also be useful measures in a transfer context. Data minimisation should be considered in this regard, in order to limit the exposure of personal data to unauthorised access. For example, in some cases it might not be necessary to transfer certain data (e.g. in case of remote access to EEA data, such as in support cases, when restricted access is granted instead of full access; or when the provision of a service only requires the transfer of a limited set of data, and not an entire database).

132. Conditions for effectiveness:

- Regular audits and strong disciplinary measures should be in place in order to monitor and enforce compliance with the data minimisation measures also in the transfer context.

- The data exporter shall perform an assessment of the personal data in its possession before the transfer takes place, in order to identify those sets of data that are not necessary for the purposes of the transfer and, therefore, won't be shared with the data importer.
- Data minimisation measures should be accompanied with technical measures as to ensure that data are not subject to unauthorised access. For example, the implementation of secure multiparty computation mechanisms and the spread of encrypted datasets among different trusted entities can prevent by design that any unilateral access lead to the disclosure of identifiable data.

***

133. Development of best practices to appropriately and timely involve and provide access to information to the data protection officer, if existent, and to the legal and internal auditing services on matters related to international transfers of personal data transfers.

134. Conditions for effectiveness:

- The data protection officer, if existent, and the legal and internal auditing team shall be provided with all the relevant information prior to the transfer, and shall be consulted on the necessity of the transfer and the additional safeguards, if any.
- Relevant information should include, for example, the assessment on the necessity of the transfer of the specific personal data, an overview of the laws of the third country applicable and the safeguards the importer committed to implement.

Adoption of standards and best practices

135. 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

136. 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.

***

137. 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.[88]

[88] C-311/18 (Schrems II), paragraphs 135 and 137.