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

Version 2.0

Adopted on 18 June 2021

Version history

Version 2.0	18 June 2021	Adoption of the Recommendations after public consultation
Version 1.0	10 November 2020	Adoption of the Recommendations for public consulation

Executive summary

The EU General Data Protection Regulation (GDPR) was adopted to serve a dual-purpose: facilitating the free flow of personal data within the European Union, while preserving the fundamental rights and freedoms of individuals, in particular their right to the protection of personal data.

In its recent judgment C-311/18 (Schrems II) the Court of Justice of the European Union (CJEU) reminds us that the protection granted to personal data in the European Economic Area (EEA) must travel with the data wherever it goes. Transferring personal data to third countries cannot be a means to undermine or water down the protection it is afforded in the EEA. The Court also asserts this by clarifying that the level of protection in third countries does not need to be identical to that guaranteed within the EEA but essentially equivalent. The Court also upholds the validity of standard contractual clauses, as a transfer tool that may serve to ensure contractually an essentially equivalent level of protection for data transferred to third countries.

Standard contractual clauses and other transfer tools mentioned under Article 46 GDPR do not operate in a vacuum. The Court states that controllers or processors, acting as exporters, are responsible for verifying, on a case-by-case basis and, where appropriate, in collaboration with the importer in the third country, if the law or practice of the third country impinges on the effectiveness of the appropriate safeguards contained in the Article 46 GDPR transfer tools. In those cases, the Court still leaves open the possibility for exporters to implement supplementary measures that fill these gaps in the protection and bring it up to the level required by EU law. The Court does not specify which measures these could be. However, the Court underlines that exporters will need to identify them on a case-by-case basis. This is in line with the principle of accountability of Article 5.2 GDPR, which requires controllers to be responsible for, and be able to demonstrate compliance with the GDPR principles relating to processing of personal data.

To help exporters (be they controllers or processors, private entities or public bodies, processing personal data within the scope of application of the GDPR) with the complex task of assessing third countries and identifying appropriate supplementary measures where needed, the European Data Protection Board (EDPB) has adopted these recommendations. These recommendations provide exporters with a series of steps to follow, potential sources of information, and some examples of supplementary measures that could be put in place.

As a **first step**, the EDPB advises you, exporters, to **know your transfers**. Mapping all transfers of personal data to third countries can be a difficult exercise. Being aware of where the personal data goes is however necessary to ensure that it is afforded an essentially equivalent level of protection wherever it is processed. You must also verify that the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

A **second step** is to **verify the transfer tool your transfer relies on**, amongst those listed under Chapter V GDPR. If the European Commission has already declared the country, region or sector to which you are transferring the data as adequate, through one of its adequacy decisions under Article 45 GDPR or under the previous Directive 95/46 as long as the decision is still in force, you will not need to take any further steps, other than monitoring that the adequacy decision remains valid. In the absence of an adequacy decision, you need to rely on one of the transfer tools listed under Articles 46 GDPR. Only in some cases you may be able to rely on one of the derogations provided for in Article 49 GDPR if you meet the conditions. Derogations cannot become “the rule” in practice, but need to be restricted to specific situations.

A **third step** is to **assess** if there is anything in the law and/or practices in force of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer. Your assessment should be focused first and foremost on third country legislation that is relevant to your transfer and the Article 46 GDPR transfer tool you are relying on. Examining also the practices of the third country’s public authorities will allow

you to verify if the safeguards contained in the transfer tool can ensure, in practice, the effective protection of the personal data transferred. Examining these practices will be especially relevant for your assessment where:

(i) legislation in the third country formally meeting EU standards is manifestly not applied/complied with in practice;

(ii) there are practices incompatible with the commitments of the transfer tool where relevant legislation in the third country is lacking;

(iii) your transferred data and/or importer fall or might fall within the scope of problematic legislation (i.e. impinging on the transfer tool's contractual guarantee of an essentially equivalent level of protection and not meeting EU standards on fundamental rights, necessity and proportionality).

In the first two situations, you will have to suspend the transfer or implement adequate supplementary measures if you wish to proceed with it.

In the third situation, in light of uncertainties surrounding the potential application of problematic legislation to your transfer, you may decide to: suspend the transfer; implement supplementary measures to proceed with it; or alternatively, you may decide to proceed with the transfer without implementing supplementary measures if you consider and are able to demonstrate and document that you have no reason to believe that relevant and problematic legislation will be interpreted and/or applied in practice so as to cover your transferred data and importer.

For evaluating the elements to be taken into account when assessing the law of a third country dealing with access to data by public authorities for the purpose of surveillance, please refer to the EDPB European Essential Guarantees recommendations.

You should conduct this assessment with due diligence and document it thoroughly. Your competent supervisory and/or judicial authorities may request it and hold you accountable for any decision you take on that basis.

A **fourth step** is to **identify and adopt supplementary measures** that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence. This step is only necessary if your assessment reveals that the third country legislation and/or practices impinge on the effectiveness of the Article 46 GDPR transfer tool you are relying on or you intend to rely on in the context of your transfer. These recommendations contain (in Annex 2) a non-exhaustive list of examples of supplementary measures with some of the conditions they would require to be effective. As is the case for the appropriate safeguards contained in the Article 46 transfer tools, some supplementary measures may be effective in some countries, but not necessarily in others. You will be responsible for assessing their effectiveness in the context of the transfer, and in light of the third country law and practices and the transfer tool you are relying on, as you will be held accountable for any decision you take on that basis. This might also require you to combine several supplementary measures. You may ultimately find that no supplementary measure can ensure an essentially equivalent level of protection for your specific transfer. In those cases where no supplementary measure is suitable, you must avoid, suspend or terminate the transfer to avoid compromising the level of protection of the personal data. You should also conduct this assessment of supplementary measures with due diligence and document it.

A **fifth step** is to **take** any **formal procedural steps** the adoption of your supplementary measure may require, depending on the Article 46 GDPR transfer tool you are relying on. These recommendations specify some of these formalities. You may need to consult your competent supervisory authorities on some of them.

The **sixth and final step** is to **re-evaluate** at appropriate intervals the level of protection afforded to the personal data you transfer to third countries and to monitor if there have been or there will be any

developments that may affect it. The principle of accountability requires continuous vigilance of the level of protection of personal data.

Supervisory authorities will continue exercising their mandate to monitor the application of the GDPR and enforce it. Supervisory authorities will pay due consideration to the actions exporters take to ensure that the data they transfer is afforded an essentially equivalent level of protection. As the Court recalls, supervisory authorities will suspend or prohibit data transfers in those cases where they find that an essentially equivalent level of protection cannot be ensured, following an investigation or a complaint.

Supervisory authorities will continue developing guidance for exporters and coordinating their actions in the EDPB to ensure consistency in the application of EU data protection law.

TABLE OF CONTENTS

The European Data Protection Board

Having regard to Article 70(1)(e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (hereinafter "GDPR"),

Having regard to the European Economic Area (EEA) Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018[1],

Having regard to Article 12 and Article 22 of its Rules of Procedure,

Whereas:

(1) The Court of Justice of the European Union (CJEU) concludes in its judgment of 16 July 2020 *Data Protection Commissioner v. Facebook Ireland LTD, Maximillian Schrems,* C-311/18 that Article 46 (1) and 46 (2)(c) of the GDPR must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter of the Fundamental Rights of the European Union.[2]

(2) As underlined by the Court, a level of protection of natural persons essentially equivalent to that guaranteed within the European Union by the GDPR, read in the light of the Charter, must be guaranteed irrespective of the provision of Chapter V on the basis of which a transfer of personal data to a third country is carried out. The provisions of Chapter V intend to ensure the continuity of that high level of protection where personal data is transferred to a third country.[3]

(3) Recital 108 and Article 46 (1) GDPR provide that in the absence of an EU adequacy decision, a controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. A controller or processor may provide appropriate safeguards, without requiring any specific authorisation from a supervisory authority, through its use of one of the transfer tools listed under Article 46 (2) GDPR, such as standard data protection clauses.

(4) The Court clarifies that the standard data protection clauses adopted by the Commission are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union. Due to their contractual nature, standard data protection clauses cannot bind the public authorities of third countries, since they are not party to the contract. Consequently, data exporters may need to supplement the guarantees contained in those

[1] References to "Member States" made throughout this document should be understood as references to "EEA Member States".
[2] CJEU judgment of 16 July 2020, Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems, (hereinafter C-311/18 (Schrems II)), second finding.
[3] C-311/18 (Schrems II), paragraphs 92 and 93.

standard data protection clauses with supplementary measures to ensure compliance with the level of protection required under EU law in a particular third country. The Court refers to recital 109 of the GDPR, which mentions this possibility and encourages controllers and processors to use it.[4]

(5) The Court stated that it is above all, for the data exporter to verify, on a case-by-case basis and, where appropriate, in collaboration with the importer of the data, whether the law of the third country of destination ensures an essentially equivalent level of protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, supplementary measures to those offered by those clauses.[5]

(6) If the controller or a processor established in the European Union is not able to take appropriate supplementary measures to guarantee an essentially equivalent level of protection under EU law, the controller or processor or, failing that, the competent supervisory authority, are required to suspend or end the transfer of personal data to the third country concerned.[6]

(7) The GDPR or the Court do not define or specify the "additional safeguards", "additional measures" or "supplementary measures" to the safeguards of the transfer tools listed under Article 46.2 of the GDPR that controllers and processors may adopt to ensure compliance with the level of protection required under EU law in a particular third country.

(8)The EDPB has decided, on its own initiative, to examine this question and to provide controllers and processors, acting as exporters, with recommendations on the process they may follow to identify and adopt supplementary measures. These recommendations aim at providing a methodology for the exporters to determine whether and which additional measures would need to be put in place for their transfers. It is the primary responsibility of exporters to ensure that the data transferred is afforded in the third country of a level of protection essentially equivalent to that guaranteed within the EEA. With these recommendations, the EDPB seeks to encourage consistent application of the GDPR and the Court's ruling, pursuant to the EDPB's mandate.[7]

HAS ADOPTED THE FOLLOWING RECOMMENDATIONS:

[4] C-311/18 (Schrems II), paragraphs 132 and 133.
[5] C-311/18 (Schrems II), paragraph 134.
[6] C-311/18 (Schrems II), paragraphs 135.
[7] Article 70.1.e GDPR.

1 ACCOUNTABILITY IN DATA TRANSFERS

1. EU primary law considers the right to data protection as a fundamental right.[8] Accordingly, the right to data protection is afforded a high level of protection and limitations may only be made if they are provided for by law, respect the essence of its right, are proportionate, necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.[9] The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.[10]

2. An essentially equivalent level of protection to that guaranteed within the EU must accompany the data when it travels to third countries outside the EEA to ensure that the level of protection guaranteed by the GDPR is not undermined, both during and after the transfer.

3. The right to data protection has an active nature. It requires exporters and importers (whether they are controllers and/or processors) to go beyond an acknowledgement or passive compliance with this right.[11] Controllers and processors must seek to comply with the right to data protection in an active and continuous manner by implementing legal, technical and organisational measures that ensure its effectiveness. Controllers and processors must also be able to demonstrate these efforts to data subjects and data protection supervisory authorities. This is the so called principle of accountability.[12]

4. The principle of accountability, which is necessary to ensure the effective application of the level of protection conferred by the GDPR also applies to data transfers to third countries[13] since they are a form of data processing in themselves.[14] As the Court underlined in its judgment, a level of protection essentially equivalent to that guaranteed within the European Union by the GDPR read in the light of the Charter must be guaranteed irrespective of the provision of that chapter on the basis of which a transfer of personal data to a third country is carried out.[15]

5. In the Schrems II judgment, the Court emphasizes the responsibilities of exporters and importers to ensure that the processing of personal data has been and will continue to be carried out in compliance with the level of protection set by EU data protection law and to suspend the transfer and/or terminate the contract where the importer of the data is not, or is no longer, able to comply with standard data protection clauses incorporated in the relevant contract between the exporter and the importer.[16] The controller or processor acting as exporter must ensure that the importers collaborate with the exporter, where appropriate, in its performance of these responsibilities, by keeping it informed, for instance, of any development affecting the level of

[8] Article 8(1) Charter of Fundamental Rights and Article 16 (1) TFEU, preamble 1, Article 1 (2) GDPR.
[9] Article 52(1) of the EU Charter of Fundamental Rights.
[10] Recital 4 of the GDPR and C-507/17 Google LLC, successor in law to Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL), paragraph 60.
[11] C-92/09 and C-93/02, Volker und Markus Schecke GbR v. Land Hessen, Opinion of Advocate General Sharpston, 17 June 2010, paragraph 71.
[12] Article 5.2 and Article 28.3 (h) GDPR.
[13] Article 44 and recital 101 GDPR, as well as Article 47(2)(d) GDPR.
[14] CJEU judgment of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner, (hereinafter* C-362/14 (Schrems I)), paragraph 45.
[15] C-311/18 (Schrems II), paragraphs 92 and 93.
[16] C-311/18 (Schrems II), paragraphs 134, 135, 139, 140, 141, 142.

protection of the personal data received in the importer's country.[17] These responsibilities are an application of the GDPR principle of accountability to the data transfers.[18]

2 ROADMAP: APPLYING THE PRINCIPLE OF ACCOUNTABILITY TO DATA TRANSFERS IN PRACTICE

6. What follows is a roadmap of the steps to take in order to find out if you (the data exporter) need to put in place supplementary measures to be able to legally transfer data outside the EEA. "You" in this document means the controller or processor acting as data exporter,[19] processing personal data within the scope of application of the GDPR – including processing by private entities and public bodies when transferring data to private bodies-.[20] As for transfers of personal data carried out between public bodies, specific guidance is provided for in the *Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies.*[21]

7. You will need to document appropriately this assessment and the supplementary measures you select and implement and make such documentation available to the competent supervisory authority upon request.[22]

2.1 Step 1: Know your transfers

8. To know what may be required for you (the data exporter) to be able to continue with or to conduct new transfers of personal data,[23] the first step is to ensure that you are fully aware of your transfers (know your transfers). Recording and mapping all transfers can be a complex exercise for entities engaging into multiple, diverse and regular transfers with third countries and using a series of processors and sub-processors. Knowing your transfers is an essential first step to fulfil your obligations under the principle of accountability.

9. To gain full awareness of your transfers, you can build on the records of processing activities that you may be obliged to maintain as controller or processor under Article 30 GDPR.[24] Previous

[17] C-311/18 (Schrems II), paragraph 134.
[18] Article 5 (2) and Article 28 (3) (h) GDPR.
[19] Therefore, for example, you will not be considered a data exporter if you are a data subject providing your personal data via an online questionnaire to a controller established in a third country.
[20] See EDPB Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en
[21] EDPB Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies; see https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-22020-articles-46-2-and-46-3-b_en
[22] Article 5(2) GDPR and Article 24 (1) GDPR.
[23] Please note that remote access by an entity from a third country to data located in the EEA is also considered a transfer.
[24] See Article 30 GDPR and in particular paragraphs 1.e and 2.c. Moreover, your records of processing should contain a description of your processing activities (including, but not limited to, the categories of data subjects, the categories of personal data and purposes of the processing and specific information about data transfers. Some controllers and processors are exempt from the obligation to keep records of processing (Article 30.5 GDPR). For guidance on this exemption, see Article 29 Working Party, Position Paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30.5 GDPR (endorsed by the EDPB on 25 May 2018).

actions to fulfil the obligations to inform data subjects under Articles 13.1.f and 14.1.f GPDR about your transfers of their personal data to third countries may also assist you.[25]

10. When mapping transfers, do not forget to also take into account onward transfers, for instance whether your processors outside the EEA transfer the personal data you entrusted to them to a sub-processor in another third country or in the same third country.[26]

11. In line with the GDPR principle of "data minimisation",[27] you must verify that the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

12. These activities must be carried out before any transfer is made and updated prior to resuming transfers after suspension of data transfer operations: you must know where the personal data you exported may be located or processed by the importers (map of destinations).

13. Keep in mind that remote access from a third country (for example in support situations) and/or storage in a cloud situated outside the EEA offered by a service provider, is also considered to be a transfer.[28] More specifically, if you are using an international cloud infrastructure you must assess if your data will be transferred to third countries and where, unless the cloud provider is established in the EEA and it clearly states in its contract that the data will not be processed at all in third countries.

2.2 Step 2: Identify the transfer tools you are relying on

14. A second step you must take is to identify the transfer tools you are relying on amongst those Chapter V GDPR lists and envisages.

Adequacy decisions

15. The European Commission may recognise through its **adequacy decisions** relating to some or all of the third countries to which you are transferring personal data that they offer an adequate level of protection for personal data.[29]

[25] Under GDPR transparency rules, you must inform data subjects about transfers of personal data to third countries (Articles 13.1.f and 14.1.f GDPR). In particular, you must inform them of the existence or absence of an adequacy decision by the European Commission, or in the case of transfers referred to in Articles 46 or 47 GDPR, or the second subparagraph of Article 49.1 GDPR, refer to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available. The information provided to the data subject must be correct and current, especially in light of the Court's case law concerning transfers.
[26] Where the controller has granted its prior specific or general written authorisation in accordance with Article 28.2 GDPR.
[27] Article 5.1.c GDPR.
[28] See FAQ nr. 11 "it should be borne in mind that even providing access to data from a third country, for instance for administration purposes, also amounts to a transfer", EDPB Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, 23 July 2020.
[29] The European Commission has the power to determine, on the basis of Article 45 GDPR whether a country outside the EU offers an adequate level of data protection. Likewise the European Commission has the power to determine that an international organisation offers an adequate level of protection.

16. The effect of such an adequacy decision is that personal data can flow from the EEA to that third country without any Article 46 GDPR transfer tool being necessary.

17. Adequacy decisions may cover a country as a whole or be limited to a part of it. Adequacy decisions may cover all data transfers to a country or be limited to some types of transfers (e.g. in one sector).[30]

18. The European Commission publishes the list of its adequacy decisions on its website.[31]

19. If you transfer personal data to third countries, regions or sectors covered by a Commission adequacy decision (to the extent applicable), **you do not need to take any further steps as described in these recommendations.**[32] However, you must still monitor if adequacy decisions relevant to your transfers are revoked or invalidated.[33]

20. However, adequacy decisions do not prevent data subjects from filing a complaint. Nor do they prevent supervisory authorities from bringing a case before a national court if they have doubts about the validity of a decision, so that a national court can make a reference for a preliminary ruling to the CJEU for the purpose of examining that validity.[34]

Example:

An EU citizen, Mr. Schrems, filed a complaint on June 2013 with the Irish Data Protection Commission (DPC) and asked this supervisory authority to prohibit or suspend the transfer of his personal data from Facebook Ireland to the United States, as he considered that the law and practice of the United States did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities. The DPC rejected the complaint, on the ground, in particular, that in Decision 2000/520 the European Commission considered that, under the 'safe harbour' scheme, the United States ensured an adequate level of protection of the personal data transferred (the Safe Harbour Decision). Mr. Schrems challenged the decision of the DPC and the Irish High Court referred a question on the validity of Decision 2000/520 to the Court of Justice of the European Union (CJEU). The CJEU subsequently decided to invalidate the Commission Decision 2000/520 on the adequacy of the protection provided by the safe harbour privacy principles.[35]

[30] Article 45.1 GDPR.

[31] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[32] Provided you and data importer have implemented measures to comply with the other obligations under the GDPR; otherwise implement those measures.

[33] The European Commission must review periodically all adequacy decisions and monitor if the third countries benefitting from adequacy decisions continue to ensure an adequate level of protection (see Art. 45.3 and 45.4 GDPR). Also, the CJEU may invalidate adequacy decisions (see its judgments on the cases C-362/14 (Schrems I) and C-311/18 (Schrems II).

[34] C-311/18 (Schrems II), paragraphs 118 - 120. Supervisory authorities may not disregard the adequacy decision and suspend or prohibit transfers of personal data to such countries citing only the inadequacy of the level of protection. They may only exercise their power to suspend or prohibit transfers of personal data to that third country on other grounds (e.g. insufficient security measures in violation of Article 32 GDPR, no legal basis validly underpins the data processing as such in violation of Article 6 GDPR). Supervisory authorities may examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the GDPR and, where relevant, bring an action before the national courts in order for them, if they have doubts as to the validity of the Commission adequacy decision, to make a reference for a preliminary ruling before the European Court of Justice for the purposes of examining its validity.

[35] Case C-362/14 (Schrems I).

Article 46 GDPR transfer tools

21. Article 46 GDPR lists a series of transfer tools containing *"appropriate safeguards*" that exporters may use to transfer personal data to third countries in the absence of adequacy decisions. The main types of Article 46 GDPR transfer tools are:

- standard data protection clauses clauses (SCCs);
- binding corporate rules (BCRs);
- codes of conduct;
- certification mechanisms;
- ad hoc contractual clauses.

22. Whatever Article 46 GDPR transfer tool you choose, you must ensure that, overall, the transferred personal data will benefit from an essentially equivalent level of protection.

23. Article 46 GDPR transfer tools mainly contain appropriate safeguards of a contractual nature that may be applied to transfers to all third countries. The situation in the third country to which you are transferring data may still require that you supplement these transfer tools and the safeguards they contain with additional measures ("supplementary measures") to ensure an essentially equivalent level of protection.[36]

Derogations

24. Besides adequacy decisions and Article 46 GDPR transfer tools, the GDPR contains a third avenue allowing transfers of personal data in certain situations. Subject to specific conditions, you may still be able to transfer personal data based on a derogation listed in Article 49 GDPR.

25. Article 49 GDPR has an exceptional nature. The derogations it contains must be interpreted in a way which does not contradict the very nature of the derogations as being exceptions from the rule that personal data may not be transferred to a third country unless the country provides for an adequate level of data protection or, alternatively, appropriate safeguards are put in place. Derogations cannot become "the rule" in practice, but need to be restricted to specific situations. The EDPB has issued its Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679.[37]

26. Before relying on an Article 49 GDPR derogation, you must check whether your transfer meets the strict conditions this provision sets forth for each of them.

***

27. If your transfer can neither be legally based on an adequacy decision, nor on an Article 49 derogation, you need to continue with Step 3.

[36] C-311/18 (Schrems II), paragraphs 130 and 133. See also sub-section 2.3 below.
[37] For further guidance on this see https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en.

2.3 Step 3: Assess whether the Article 46 GDPR transfer tool you are relying on is effective in light of all circumstances of the transfer

28. The selected Article 46 GDPR transfer tool must be effective in ensuring that the level of protection guaranteed by the GDPR is not undermined by the transfer in practice.[38]

29. In particular, the protection afforded to the transferred personal data in the third country must be essentially equivalent to that guaranteed in the EEA by the GDPR, read in light of the Charter of Fundamental Rights of the EU.[39] This is not the case if the data importer is prevented from complying with its obligations under the chosen Article 46 GDPR transfer tool due to the third country's legislation and practices applicable to the transfer, including during the transit of data from the exporter to the importer's country.[40]

30. You must first assess, where appropriate in collaboration with the importer, if there is anything in the law and/or practices in force[41] in the third country that may impinge on the effectiveness of the appropriate safeguards of the Article 46 GDPR transfer tool you are relying on, in the context of your specific transfer. This implies determining whether your transfer falls within the scope of legislation and/or practices which may impinge on the effectiveness of your Article 46 GDPR transfer tool. The assessment required must be based first and foremost on legislation publicly available.

31. This assessment must contain elements concerning access to data by public authorities of the third country of your importer such as:

    - Elements on whether public authorities of the third country of your importer may seek to access the data with or without the data importer's knowledge, in light of legislation, practice and reported precedents;
    - Elements on whether public authorities of the third country of your importer may be able to access the data through the data importer or through the telecommunication providers or communication channels in light of legislation, legal powers, technical, financial, and human resources at their disposal and of reported precedents.

Identifying laws and practices relevant in light of all circumstances of the transfer

32. You will need to look into the characteristics of each of your transfers and determine whether the domestic legal order and/or practices in force of the country to which data is transferred (or onward transferred) affect your transfers. The scope of your assessment is thus limited to the legislation and practices relevant to the protection of the specific data you transfer, in contrast with the general and wide encompassing adequacy assessments the European Commission carries out in accordance with Article 45 GDPR.

[38] Article 44 GDPR and paragraphs 126, 137 and 148 of C-311/18 (Schrems II).
[39] C-311/18 (Schrems II), paragraphs 105 and second finding.
[40] See C-311/18 (Schrems II), paragraph 183 in conjunction with paragraph 184.
[41] See paragraph 126 of the C-311/18 (Schrems II) Judgment in which the Court explicitly alludes to "the law and practices in force in the third country concerned" and requires "(...) ensuring, in practice, the effective protection of personal data transferred to the third country concerned." (emphasis added), and paragraph 158.

33. The applicable legal context and/or practices will depend on the specific circumstances of your 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);[42]
    - Whether the data will be stored in the third country or whether there is remote access to data stored within the EU/EEA;
    - Format of the data to be transferred (i.e. in plain text/ pseudonymised or encrypted[43]);
    - Possibility that the data may be subject to onward transfers from the third country to another third country.[44]

34. Your assessment should take into consideration all the actors participating in the transfer (e.g. controllers, processors and sub-processors processing data in the third country), as identified in the mapping exercise of transfers. The more controllers, processors or importers involved, the more complex your assessment will be. You will also need to factor into this assessment any envisaged onward transfer.

35. You should in any case pay specific attention to any relevant laws, in particular laws laying down requirements to disclose personal data to public authorities or granting such public authorities powers of access to personal data (for instance for criminal law enforcement, regulatory supervision or national security purposes). If these requirements or powers restrict the fundamental rights of data subjects while respecting their essence and being necessary and proportionate measures in a democratic society to safeguard important objectives as also recognised in Union or EU Member States' law,[45] they may not impinge on the commitments contained in the Article 46 GDPR transfer tool you are relying on.

36. You will need to assess relevant rules and practices of a general nature insofar as they have an impact on the effective application of the safeguards contained in the Article 46 GDPR transfer tool.

---

[42] A transfer of personal data is a processing operation (Article 4.2 GDPR). If you wish to transfer sensitive data falling under Articles 9 and 10 GDPR you may only conduct a transfer if it falls within one of the derogations and conditions set forth in Articles 9 and 10 GDPR and EU Member States' law. In accordance with Article 32 GDPR, you will also need to implement, with the importer acting as controller or processor, appropriate technical and organisational measures to ensure a level of security appropriate to the risks to the rights and freedoms of data subjects posed by a potential personal data breach of the data transferred (Article 4.12 GDPR). The categories of data transferred and their sensitiveness will be relevant to the assessment of the risk and the appropriateness of the measures.

[43] Some third countries do not permit encrypted data to be imported.

[44] Where the controller has granted its prior specific or general written authorisation in accordance with Article 28.2 GDPR.

[45] See Articles 47 and 52 of the EU Charter of Fundamental Rights, Article 23.1 GDPR, and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en .

37. In carrying out this assessment, different aspects of the legal system of that third country, e.g. the elements listed in Article 45(2) GDPR, are also relevant. For example, the rule of law situation in a third country may be relevant to assess the effectiveness of available mechanisms for individuals to obtain (judicial) redress against unlawful government access to personal data. The existence of a comprehensive data protection law or an independent data protection authority, as well as adherence to international instruments providing for data protection safeguards, may contribute to ensuring the proportionality of government interference.

38. The obligations or powers resulting from such laws and practices will be considered to impinge on/be incompatible with the commitments of the Article 46 GDPR transfer tool if they[46]:

- Do not respect the essence of the fundamental rights and freedoms of the EU Charter of Fundamental Rights, or

- Exceed what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in Union or member state law such as those listed in Article 23 (1) GDPR.

39. You should verify if the data importer's commitments enabling data subjects to exercise their rights as provided in the Article 46 GDPR transfer tool (such as access, correction and deletion requests for transferred data, as well as (judicial) redress) can be effectively applied in practice and are not thwarted by the laws and/or practices in the third country of destination.

40. EU standards, such as Articles 47 and 52 of the EU Charter of Fundamental Rights, must be used as a reference, in particular to assess whether access by public authorities is limited to what is necessary and proportionate in a democratic society and whether data subjects are afforded effective redress.

41. The EDPB European Essential Guarantees (EEG) recommendations[47] provide clarifications on the elements which have to be assessed to determine whether the legal framework governing access to personal data by public authorities in a third country, being national security agencies or law enforcement authorities, can be regarded as a justifiable interference[48] or not. In particular, this should be carefully considered when the legislation governing the access to data by public authorities is ambiguous or not publicly available. The first requirement of the European Essential Guarantees is that there should be a legal framework providing for such access, when it is envisaged, that is publicly available and sufficiently clear.

42. Applied to the situation of data transfers based on Article 46 transfer tools, the EDPB European Essential Guarantees recommendations can guide the data exporter in assessing whether such powers unjustifiably interfere with the data exporter and importer's obligations to ensure essential equivalence pursuant to the GDPR or the commitments contained in the transfer tool. The lack of an essentially equivalent level of protection will be especially evident where the legislation and/or practices of the third country relevant to your transfer do not meet the requirements of the European Essential Guarantees. The EDPB reiterates that the European Essential Guarantees are a referential standard when assessing the interference, entailed by third

[46] See Articles 47 and 52 of the EU Charter of Fundamental Rights, Article 23.1 GDPR, C-311/18 (Schrems II), paragraphs 174 and 187, and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020.
[47] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020.
[48] And therefore as not impinging on the commitments taken in the art 46 GDPR transfer tool.

country surveillance measures, in the context of international data transfers. These standards stem from EU law and the jurisprudence of the CJEU and the ECtHR, which is binding on EU Member States.

43. Your assessment must be based first and foremost on legislation publicly available. Examining also the practices of the third country's public authorities will allow you to verify if the safeguards contained in the Article 46 GDPR transfer tool can be a sufficient means of ensuring, in practice, the effective protection of the personal data transferred.[49] Examining the practices in force in the third country will be especially important for your assessment in the situations described below.

43.1 **Relevant legislation in the third country may formally meet EU standards on fundamental rights and freedoms and the necessity and proportionality of restrictions thereto.** However, the practices of its public authorities (e.g. accessing personal data held by the private sector or when enforcing -or not- legislation as supervisory or judicial bodies) may clearly indicate that they do not normally apply/comply with the legislation that governs, in principle, their activities. In this case, you must take these practices into account in your assessment and consider that the Article 46 GDPR tool will not be able to effectively ensure, by itself (i.e. without supplementary measures), an essentially equivalent level of protection. In such case, if you wish to proceed with the transfer, you will have to implement adequate supplementary measures.

43.2 **Relevant legislation in the third country (e.g. on access to personal data held by the private sector) may be lacking**. In this case you cannot automatically infer from this absence of relevant legislation that your Article 46 GDPR transfer tool can be effectively applied. You will have to check if there are indications of practices in force in the country that are incompatible with EU law and the commitments of the Article 46 GDPR transfer tool. If there are incompatible practices, the Article 46 GDPR transfer tool will not be able to effectively ensure, by itself (i.e. without adequate supplementary measures), an essentially equivalent level of protection. In such case, if you wish to proceed with the transfer, you will have to implement adequate supplementary measures.

43.3 **The assessment may reveal that relevant legislation in the third country may be problematic**[50] **and that the transferred data and/or the importer at hand fall or might fall within the scope of this problematic legislation.**[51]

In light of uncertainties surrounding the potential application of problematic legislation to your transfer, you may then decide to:

- Suspend the transfer;
- Implement supplementary measures[52] to prevent the risk of potential application to your importer and/or to your transferred data of laws and/or practices of the third country of

[49] C-311/18 (Schrems II), paragraph 126.

[50] 'Problematic legislation' is understood as legislation that 1) imposes on the recipient of personal data from the European Union obligations and/or affect the data transferred in a manner that may impinge on the transfer tools' contractual guarantee of an essentially equivalent level of protection and 2) does not respect the essence of the fundamental rights and freedoms recognised by the EU Charter of Fundamental Rights or exceeds what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in Union or EU Member States' law, such as those listed in Article 23 (1) GDPR.

[51] It may be unclear whether the importer and/or the data transferred fall under the scope of general terms often used in national security legislation to limit their scope of application, such as for instance "electronic communication service provider" and "foreign intelligence information".

[52] See recital 109 GDPR and C-311/18 (Schrems II), paragraph 132.

the data importer, which are capable of impinging on the transfer tool's contractual guarantees of an essentially equivalent level of protection to that guaranteed in the EEA; or

- Alternatively, you may decide to proceed with the transfer without being required to implement supplementary measures, if you consider that you have no reason to believe that relevant and problematic legislation will be applied, in practice, to your transferred data and/or importer. You will need to have demonstrated and documented through your assessment, where appropriate in collaboration with the importer, that the law is not interpreted and/or applied in practice so as to cover your transferred data and importer, also taking into account the experience of other actors operating within the same sector and/or related to similar transferred personal data and the additional sources of information described further below.[53]

  Therefore, you will need to have demonstrated and documented with a detailed report[54] that problematic legislation will not be applied in practice to your transferred data and/or importer, and, consequently, that it will not prevent the importer from fulfilling its obligations under the Article 46 GDPR transfer tool.[55]

Possible sources of information

44. Your data importer should provide you with the relevant sources and information relating to the third country in which it is established and the laws and practices in force applicable to the transfer.

45. You and your importer may complete your assessment with information obtained from sources, such as those listed as examples in Annex 3.

46. In addition to the legal framework of the third country applicable to the transfer, sources and information should be relevant, objective, reliable, verifiable and publicly available or otherwise accessible to determine whether your Article 46 transfer tool can be effectively applied[56] and you will have to assess and document that they are.

[53] See paragraphs 45 to 47.

[54] Reports you will establish will have to include comprehensive information on the legal assessment of the legislation and practices, and of their application to the specific transfers, the internal procedure to produce the assessment (including information on actors involved in the assessment-e.g. law firms, consultants, or internal departments-) and dates of the checks. Reports should be endorsed by the legal representative of the exporter.

[55] Demonstrating that problematic legislation is not applied in practice to your transferred data and importer, also taking into account the experience of other actors operating within the same sector and/or related to similar transferred personal data, does not exempt you from providing for the necessary supplementary measures to protect personal data during its transmission and processing in the third country of destination (e.g. end-to-end encryption of data – see examples of technical supplementary measures in Annex 2-) if your analysis of the applicable legislation of the third country of destination indicates that access to data may also take place, even in the absence of the importer's intervention, at this moment of the transfer. You may have already foreseen such measures with the importer acting as controller or processor in accordance with Article 32 of the GDPR.

[56] See Annex 3 for a non-exhaustive list of sources of information that you and the importer may use.

Relevant: the information must be relevant to the specific transfer and/or importer and their compliance with the requirements set in EU law and the Article 46 GDPR transfer instrument, and not overly general or abstract.

Objective information: is information that is supported by empirical evidence based on knowledge gained from the past, not assumptions about potential events and risks.

Reliable: the exporter and the importer must objectively assess the reliability of the source of information and of the information itself, and evaluate them separately.

Verifiable: information and conclusions should be verifiable or contrastable with other types of information or sources, as part of an overall assessment, also to allow the competent supervisory or judicial authority to check the objectivity and reliability of this information if needed.

Publicly available or otherwise accessible information: information should preferably be public or at least accessible to facilitate the verification of the criteria made above and ensure its possible sharing with supervisory authorities, judicial authorities and ultimately data subjects.

47. You may also take into consideration documented practical experience of the importer with relevant prior instances of requests for access received from public authorities in the third country. You will only be able to use the experience of the importer as an additional source of information if the legal framework of the third country does not prohibit the importer to provide information on requests for disclosure from public authorities or on the absence of such requests (and you should also document such an assessment). You must however note that the absence of prior instances of requests received by the importer can never be considered, by itself, as a decisive factor on the effectiveness of the Article 46 GDPR transfer tool that allows the transfer to proceed without supplementary measures. You will be able to consider this information, together with other types of information obtained from other sources, as part of your overall assessment of the laws and practices of the third country in relation to your transfer. The relevant and documented experience of the importer should be corroborated and not contradicted by relevant, objective, reliable, verifiable and publicly available or otherwise accessible information on the practical application of the relevant law (e.g. the existence or absence of requests for access received by other actors operating within the same sector and/or related to similar transferred personal data[57] and/or the application of the law in practice, such as case law and reports by independent oversight bodies).

Results of your assessment

48. You should conduct this overall assessment of the law and practice of the third country of your importer applicable to your transfer with due diligence and document it thoroughly. Your competent supervisory and/or judicial authorities may request it and hold you accountable for any decision you take on that basis.[58]

[57] The experience could be that of other entities you directly know because of previous transfers of the same kind you put in place, or which is reported in relevant case-law, reports of NGOs, etc. (see Annex 3).
[58] Article 5(2) GDPR.

49. Your assessment may ultimately reveal that the Article 46 GDPR transfer tool you rely on either:

- Effectively ensures that the transferred personal data is afforded a level of protection in the third country that is essentially equivalent to that guaranteed in the EEA. The third country's legislation and practices applicable to the transfer allow the data importer to comply with its obligations under the chosen transfer tool. You should re-evaluate at appropriate intervals, or when significant changes come to light (see Step 6); or

- Does not effectively ensure an essentially equivalent level of protection. The data importer cannot comply with its obligations, owing to the third country's legislation and/or practices applicable to the transfer not meeting EU standards on fundamental rights and freedoms and the necessity and proportionality of restrictions thereto to safeguard legitimate objectives of public interest. The CJEU underlined that where Article 46 GDPR transfer tools fall short, it is the responsibility of the data exporter to either put in place effective supplementary measures or to not transfer personal data.[59]

Example:

Background:
The CJEU held that Section 702 of the U.S. FISA does not respect the minimum safeguards resulting from the principle of proportionality under EU law and cannot be regarded as limited to what is strictly necessary. This means that the level of protection of the programs authorised by Section 702 FISA is not essentially equivalent to the safeguards required under EU law.

Assessment:
If your assessment of the relevant U.S. legislation leads you to consider that your transfer might fall within the scope of Section 702 FISA, but you are unsure if it falls within its practical scope of application, you may decide either:

1. To stop the transfer;
2. To adopt appropriate supplementary measures that ensure effectively a level of protection of the data transferred essentially equivalent to that guaranteed in the EEA; or
3. To look at other objective, reliable, relevant, verifiable and preferably publicly available information (which may include information provided to you by your data importer) to clarify the scope of application in practice of Section 702 FISA to your particular transfer. This information should provide answers to some relevant questions, such as the following:

- Does publicly available information show that there is a legal prohibition of informing about a specific request for access to data received and wide restrictions on providing general information about requests for access to data received or the absence of requests received?

- Has your data importer confirmed that it has received requests for access to data from U.S. public authorities in the past? Or has your data importer confirmed that it has not received requests for access to data from U.S. public authorities in the past and that it is not prohibited from providing information about such requests or their absence?

[59] CJEU C-311/18 (Schrems II), paragraphs 134 and 135.

- Does publicly available information you obtained on U.S. case law and reports from oversight bodies, civil society organisations, and academic institutions[60] reveal data importers of the same sector as your importer have received requests for access to data for similar transferred data in the past?

The answers to these questions that you obtain through your overall assessment lead you to conclude that:

- Section 702 FISA applies in practice to your particular transfer and therefore, impinges on the effectiveness of your Article 46 GDPR transfer tool. Consequently, if you wish to proceed with the transfer, you must consider, where appropriate in collaboration with the importer, if you can adopt supplementary measures that ensure effectively a level of protection of the transferred data essentially equivalent to that guaranteed in the EEA. If you cannot find effective supplementary measures, you must not transfer the personal data.

Or

- Section 702 FISA does not apply in practice to your particular transfer and therefore, does not impinge on the effectiveness of your Article 46 GDPR transfer tool. You may then proceed with the transfer without any supplementary measures.

2.4 Step 4: Adopt supplementary measures

50. If your assessment under Step 3 has revealed that your Article 46 GDPR transfer tool is not effective, then you will need to consider, where appropriate in collaboration with the importer, if supplementary measures exist, which, when added to the safeguards contained in transfer tools, could ensure that the data transferred is afforded in the third country a level of protection essentially equivalent to that guaranteed within the EU.[61] "Supplementary measures" are by definition supplementary to the safeguards the Article 46 GDPR transfer tool already provides and to any other applicable security requirements (e.g. technical security measures) established in the GDPR.[62]

51. You must identify on a case-by-case basis which supplementary measures could be effective for a set of transfers to a specific third country when using a specific Article 46 GDPR transfer tool. You do not need to repeat the assessment every time you conduct the same transfer of a specific type of data to the same third country. Some of the data planned for transfer may require supplementary measures whereas other data may not (considering formal and/or practical application of the third country law). You will be able to build on your previous assessments and conclusions under Steps 1, 2 and 3 above and check against their findings the potential effectiveness of the supplementary measures in guaranteeing the required level of protection.

[60] e.g. Provisions of Section 702 FISA; Rules of Procedure of the Foreign Intelligence Surveillance Court (FISC), declassified FISC opinions and decisions, case law of U.S. courts; reports and hearing transcripts of the Privacy and Civil Liberties Oversight Board (PCLOB); reports by the Office of the Inspector General - U.S. Department of Justice; reports by the NSA Director of Civil Liberties and Privacy Office; reports prepared by the Congressional Research Service; reports by the American Civil Liberties Union Foundation (ACLU).
[61] C-311/18 (Schrems II), paragraph 96.
[62] Recital 109 of the GDPR and C-311/18 (Schrems II), paragraph 133.

52. In principle, supplementary measures may have a contractual, technical or organisational nature. Combining diverse measures in a way that they support and build on each other may enhance the level of protection and may therefore contribute to reaching EU standards.

53. Contractual and organisational measures alone will generally not overcome access to personal data by public authorities of the third country based on problematic legislation and/or practices.[63] Indeed there will be situations where only appropriately implemented technical measures might impede or render ineffective access by public authorities in third countries to personal data, in particular for surveillance purposes.[64] In such situations, contractual or organisational measures may complement technical measures and strengthen the overall level of protection of data (e.g. by introducing checks and eliminating automatisms for attempts from public authorities to access data in a manner not compliant with EU standards).

54. You may, in collaboration with the data importer where appropriate, look at the following (non-exhaustive) list of factors to identify which supplementary measures would be most effective in protecting the data transferred from public authorities' requests for access to data based on problematic legislation applied in practice:

    - 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 9 and 10 GDPR);[65]
    - 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-);[66]
    - Technique or parameters of practical application of the third country law concluded in Step 3;
    - 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[67]).

[63] 'Problematic legislation' is understood as legislation that 1) imposes on the recipient of personal data from the European Union obligations and/or affect the data transferred in a manner that may impinge on the transfer tools' contractual guarantee of an essentially equivalent level of protection and 2) does not respect the essence of the fundamental rights and freedoms recognised by the EU Charter of Fundamental Rights or exceeds what is necessary and proportionate in a democratic society to safeguard one of the important objectives as also recognised in Union or EU Member States' law, such as those listed in Article 23 (1) GDPR.

[64] Where such access goes beyond what is necessary and proportionate in a democratic society; see Articles 47 and 52 of the EU Charter of Fundamental Rights, Article 23.1 GDPR, and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en.

[65] See footnote 42.

[66] The GDPR assigns distinct obligations to controllers and processors. Transfers can be controller-to-controller, between joint controllers, controller-to-processor, and, subject to the authorisation of the controller, processor-to-controller or processor-to-processor.

[67] See footnote 26.

Examples of supplementary measures

55. Some examples of technical, contractual and organisational measures that could be considered, where not already included in the used Article 46 GDPR transfer tool, may be found in the non-exhaustive lists described in the Annex 2.

***

56. If you have put in place effective supplementary measures, which combined with your chosen Article 46 GDPR transfer tool reach a level of protection that is now essentially equivalent to the level of protection guaranteed within the EEA: you may proceed with your transfers.

57. Where you are not able to find or implement effective supplementary measures that ensure that the transferred personal data enjoys an essentially equivalent level of protection,[68] you must not start transferring personal data to the third country concerned on the basis of the Article 46 GDPR transfer tool you are relying on. If you are already conducting transfers, you are required to suspend or end the transfer of personal data.[69] Pursuant to the safeguards contained in the Article 46 GDPR transfer tool you are relying on, the data that you have already transferred to that third country and the copies thereof should be returned to you or destroyed in their entirety by the importer.[70]

Example:

The law of the third country prohibits the supplementary measures you have identified (e.g. prohibits the use of encryption) or otherwise prevents their effectiveness. You must not start transferring personal data to this country, or you must stop ongoing existing transfers to this country.

58. The competent supervisory authority may impose any other corrective measure (e.g. a fine) if, despite the fact that you cannot demonstrate an essentially equivalent level of protection in the third country, you start or continue the transfer.

2.5 Step 5: Procedural steps if you have identified effective supplementary measures

59. The procedural steps you may have to take in case you have identified effective supplementary measures to be put in place may differ depending on the Article 46 GDPR transfer tool you are using or you envisage to use.

2.5.1 Standard data protection clauses ("SCCs") (Art. 46(2)(c) and (d) GDPR)

60. When you intend to put in place supplementary measures in addition to SCCs, there is no need for you to request an authorisation from the competent SA to add these kind of clauses or

[68] Where such access goes beyond what is necessary and proportionate in a democratic society; see Articles 47 and 52 of the EU Charter of Fundamental Rights, Article 23.1 GDPR, and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en .
[69] C-311/18 (Schrems II), paragraph 135.
[70] E.g. see Clause 12 in the annex to the SCC Decision 87/2010; see the (optional) Extra termination clause in Annex B SCC 2004/915/EC.

additional safeguards as long as the identified supplementary measures do not contradict, directly or indirectly, the SCCs and are sufficient to ensure that the level of protection guaranteed by the GDPR is not undermined.[71] The data exporter and importer need to ensure that additional clauses cannot be construed in any way to restrict the rights and obligations in the SCCs or in any other way to lower the level of data protection. You should be able to demonstrate this, including the unambiguity of all clauses, according to the accountability principle and your obligation to provide for a sufficient level of data protection. The competent supervisory authorities have the power to review these supplementary clauses where required (e.g. in case of complaint or own-volition inquiry).

61. Where you intend to modify the standard data protection clauses themselves or where the supplementary measures added 'contradict' directly or indirectly the SCCs, you are no longer deemed to be relying on standard contractual clauses[72] and must seek an authorisation with the competent supervisory authority in accordance with Article 46(3)(a) GDPR.

2.5.2 BCRs (Art. 46(2)(b) GDPR)

62. The reasoning put forward by the Schrems II judgment also applies to other transfer instruments pursuant to Article 46(2) GDPR since all of these instruments are basically of contractual nature, so the guarantees foreseen and the commitments taken by the parties therein cannot bind third country public authorities.[73]

63. The Schrems II judgement is relevant for transfers of personal data on the basis of BCRs, since third countries laws may affect the protection provided by such instruments.

64. All commitments that need to be included will be referred to in the updated WP256/257 referentials[74] to which all groups relying on BCRs as transfer tools will have to align their existing and future BCRs.

65. The Court highlighted that it is the responsibility of the data exporter and the data importer to assess whether the level of protection required by EU law is respected in the third country concerned in order to determine if the guarantees provided by the SCCs or the BCRs can be

[71] Recital 109 of the GDPR states: "The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects." Similar provisions are provided in sets of SCCs adopted by the European Commission under Directive 95/45/EC.

[72] See by analogy, the EDPB Opinion 17/2020 on the draft Standard Contractual Clauses submitted by the Slovenian SA (Article 28(8) GDPR) on Art. 28 SCC already adopted which contains a similar provision ("In addition, the Board recalls that the possibility to use Standard Contractual Clauses adopted by a supervisory authority does not prevent the parties from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the adopted standard contractual clauses or prejudice the fundamental rights or freedoms of the data subjects. Furthermore, where the standard data protection clauses are modified, the parties will no longer be deemed to have implemented adopted standard contractual clauses"), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinion_202017_art28sccs_si_en.pdf .

[73] CJEU, C-311/18 (Schrems II), paragraph 132.

[74] Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 256 rev.01; Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, as last revised and adopted on 6 February 2018, WP 257 rev.01.

complied with in practice. If this is not the case, you should assess whether you can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EEA, and if the law or practice of the third country will not impinge on these supplementary measures so as to prevent their effectiveness.

2.5.3 Ad hoc contractual clauses (Art. 46.3(a) GDPR)

66. The reasoning put forward by the Schrems II judgment also applies to other transfer instruments pursuant to Article 46 (2) GDPR since all of these instruments are basically of contractual nature, so the guarantees foreseen and the commitments taken by the parties therein cannot bind third country public authorities.[75] The Schrems II judgement is therefore relevant for transfers of personal data on the basis of ad hoc contractual clauses, since third countries laws may affect the protection provided by such instruments.

2.6 Step 6: Re-evaluate at appropriate intervals

67. You must monitor, on an ongoing basis, and where appropriate in collaboration with data importers, developments in the third country to which you have transferred personal data that could affect your initial assessment of the level of protection and the decisions you may have taken accordingly on your transfers. Accountability is a continuing obligation (Article 5(2) GDPR).

68. You should put sufficiently sound mechanisms in place to ensure that you promptly suspend or end transfers where:

- the importer has breached or is unable to honour the commitments it has taken in the Article 46 GDPR transfer tool; or
- the supplementary measures are no longer effective in that third country.

3 CONCLUSION

69. The GDPR lays down rules on processing personal data in the EEA and in doing so allows for free movement of personal data within the EEA. Chapter V of the GDPR governs transfers of personal data to third countries and sets a high bar: the transfer must not undermine the level of protection of natural persons guaranteed by the GDPR (Article 44 GDPR). The CJEU C-311/18 (Schrems II) judgement underscores the need to ensure the continuity of the level of protection afforded under the GDPR to personal data transferred to a third country.[76]

70. To ensure an essentially equivalent level of protection of your data, you must first and foremost know thoroughly your transfers. You must also check that the data you transfer is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

71. You must also identify the transfer tool you are relying on for your transfers. If the transfer tool is not an adequacy decision, you must verify on a case-by-case basis whether (or not) the law or practice of the third country of destination undermines the safeguards contained in the Article 46 GDPR transfer tool in the context of your transfers. Where the Article 46 GDPR transfer tool alone

[75] CJEU, C-311/18 (Schrems II), paragraph 132.
[76] C-311/18 (Schrems II), paragraph 93.

fails to achieve for the personal data you transfer a level of protection essentially equivalent, supplementary measures may fill the gap.

72. Where you are not able to find or implement effective supplementary measures that ensure that the transferred personal data enjoys an essentially equivalent level of protection, you must not start transferring personal data to the third country concerned on the basis of your chosen transfer tool. If you are already conducting transfers, you are required to promptly suspend or end the transfer of personal data.

73. The competent supervisory authority has the power to suspend or end transfers of personal data to the third country if the protection of the data transferred that EU law requires, in particular Articles 45 and 46 GDPR and the Charter of Fundamental Rights, is not ensured.

For the European Data Protection Board

The Chair

(Andrea Jelinek)

ANNEX 1: DEFINITIONS

- "Third country" means any country that is not a Member State of the EEA.
- "EEA" means the European Economic Area and it includes the Member States of the European Union and Iceland, Norway and Liechtenstein. The GDPR applies to the latter by virtue of the EEA Agreement, in particular its Annex XI and Protocol 37.
- "GDPR" refers to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
- "The Charter" refers to the Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407.
- "CJEU" or "the Court" refer to the Court of Justice of the European Union. It constitutes the judicial authority of the European Union and, in cooperation with the courts and tribunals of the Member States, it ensures the uniform application and interpretation of EU law.
- "Data exporter" means the controller or processor within the EEA who transfers personal data to a controller or processor in a third country.
- "Data importer" means the controller or processor in a third country who receives or gets access to personal data transferred from the EEA.
- "Article 46 GDPR transfer tool": refers to the appropriate safeguards under Article 46 GDPR that data exporters shall put in place when transferring personal data to a third country, in the absence of an adequacy decision pursuant to Article 45(3) GDPR. Article 46(2) and (3) of the GDPR contains the list of Article 46 GDPR transfer tools that controllers and processors may use.
- "SCCs" means standard data protection clauses (or "standard contractual clauses") adopted by the European Commission for personal data transfers between controllers or processors in the EEA and controllers or processors outside the EEA. Standard contractual clauses adopted by the European Commission are a transfer tool under the GDPR, as per Article 46(2)(c) and (5) GDPR.

ANNEX 2: EXAMPLES OF SUPPLEMENTARY MEASURES

74. The following measures are examples of supplementary measures you could consider when you reach Step 4 “Adopt supplementary measures”. This list is not exhaustive. You may explore other supplementary measures. Future technological, legal or organisational developments may lead to the emergence of new supplementary measures for you to consider. 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.

75. Any supplementary measure may only be deemed effective in the meaning of the CJEU judgment “Schrems II” if and to the extent that it - by itself or in combination with others - addresses the specific deficiencies identified in your assessment of the situation in the third country as regards its laws and practices applicable to your transfer. If, ultimately, you cannot ensure an essentially equivalent level of protection, you must not transfer the personal data.

76. As a controller or processor, you may already be required to implement some of the measures described in this annex in order to be compliant with the GDPR. This means similar measures might need to be put in place for personal data processed in the EEA, transferred to a data importer covered by an adequacy decision, or to other third countries.[77]

2.1 Technical measures

77. 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.[78]

78. For further clarity, this section describes first some examples of scenarios for which some technical measures could potentially be effective to ensure an essentially equivalent level of protection. The section continues with some scenarios for which the technical measures to ensure this level of protection are not identified.

[77] Article 5.2 GDPR, Article 32 GDPR.
[78] C-311/18 (Schrems II), paragraph 135.

Examples of scenarios referring to cases in which *effective* measures are identified

79. 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 would be necessary to guarantee an essentially equivalent level of protection to that guaranteed in the EEA, even if the public authorities' access complies with the law of the importer's country, where, in practice, such access goes beyond what is necessary and proportionate in a democratic society.[79] 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 datasets that may contain, among other data, online identifiers provided by the devices, applications, tools and protocols used by data subjects in other contexts.

80. 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.

81. 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, U.S. 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.

82. The scenarios describe specific circumstances, and measures taken to serve as an example. Any changes to the scenarios may give rise to different conclusions. The scenarios refer to situations where it has been concluded that supplementary measures are needed in the first place, i.e. where in practice problematic legislation of the third country is applied to the transfer in question.

83. 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

[79] See Articles 47 and 52 of the EU Charter of Fundamental Rights, Article 23.1 GDPR, and EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020.

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

84. 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, and the identity of the importer is verified,
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,[80]
3. the strength of the encryption and key length takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,[81]
4. the encryption algorithm is implemented correctly and by properly maintained software without known vulnerabilities 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),[82] and
6. the keys are retained solely under the control of the data exporter, or by an entity trusted by the exporter in the EEA or under a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA,

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

---

[80] For the assessment of the strength of encryption algorithms, their conformity with the state-of-the-art, and their robustness against cryptanalysis over time, data exporters can rely on technical guidance published by official cybersecurity authorities of the EU and its member states. See e.g. ENISA Report « What is "state of the art" in IT security? », 2019, https://www.enisa.europa.eu/news/enisa-news/what-is-state-of-the-art-in-it-security; guidance given by the German Federal Office for Information Security in its Technical Guidelines of the TR-02102 series and "Algorithms, Key Size and Protocols Report (2018), H2020-ICT-2014 – Project 645421, D5.4, ECRYPT-CSA, 02/2018" at https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[81] The protective capacity of cryptographic algorithms is subject to decline over time due to the discovery of new cryptanalytic techniques, the emergence of new computing paradigms like quantum computing, and the general increase of available computing power, unless the applied algorithms are proven to be information theoretically secure. This concern applies in particular to public key algorithms that are at the time of writing in common use. In consequence, the data exporter has to consider that public authorities may undertake to access encrypted data in the circumstances described in paragraph No. 80, and store it until their resources are sufficient for decryption. The supplementary measure can only be considered effective if such decryption and subsequent further processing at that time would no longer constitute an infringement of the rights of data subjects, e.g., because the data can no longer be used to directly or indirectly identify them.

[82] NIST Special Publication 800-57, Recommendation for Key Management https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final

Use Case 2: Transfer of pseudonymised Data

85. 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,[83]
2. that additional information is held exclusively by the data exporter and kept separately in a Member State or in a third country, by an entity trusted by the exporter in the EEA or under a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA,
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 be expected to possess and use - 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.

86. 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 based service at specific points in time[84] may allow the identification of that person even if their name, address or other plain identifiers are omitted.

87. This is particularly true whenever the data concern the use of information services (time of access, sequence of features accessed, characteristics 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.

88. 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

[83] 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;" Additional data may consist of tables juxtaposing pseudonyms with the identifying attributes they replace, cryptographic keys or other parameters for the transformation of attributes, or other data permitting the attribution of the pseudonymised data to identified or identifiable natural persons.

[84] 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;".

public authorities in their jurisdiction likely possess data about the use of information services by a person they target.

89. If, in the course of performing pseudonymisation, attributes contained in the personal data are transformed using a cryptographic algorithm, then the guidance in footnotes 80 and 81 applies. Henceforth it is recommended to forego the exclusive use of cryptography, and apply transformations based on table look-up mechanisms.

Use Case 3: Encryption of data to protect it from access by the public authorities of the third country of the importer when it transits between the exporter and its importer

90. A data exporter wishes to transfer data to a destination where the law and/or practices allow for access by public authorities to data while it is transiting between the country of the exporter and the country of destination.

If

1. a data exporter transfers personal data to a data importer in a jurisdiction where the law and/or practice allow the public authorities to access data while they are being transported via the internet to this third country without the European essential guarantees concerning these access, 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 this third country,
2. the parties involved in the communication agree on a trustworthy public-key certification authority or infrastructure,
3. specific protective and state-of-the-art measures are used against active and passive attacks on the sending and receiving systems providing transport encryption, including tests for software vulnerabilities and possible backdoors,
4. 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,
5. 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 when data is transiting to this third country taking into account the resources and technical capabilities (e.g., computing power for brute-force attacks) available to them (see footnote 80 above),[85]
6. the strength of the encryption takes into account the specific time period during which the confidentiality of the encrypted personal data must be preserved,
7. the encryption algorithm is implemented correctly and by properly maintained software without known vulnerabilities the conformity of which to the specification of the algorithm chosen has been verified, e.g., by certification,
8. 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,

[85] See footnote 80 for some references to technical guidance published by official cybersecurity authorities of the EU and its Member States.

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

91. 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, possibly, the exporter itself or another entity trusted by the exporter that is located in the EEA or a jurisdiction offering an essentially equivalent level of protection to that guaranteed within the EEA, 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

92. 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. the controller has established by means of a thorough analysis of the data in question, taking into account the missing pieces of information that the public authorities of the recipient countries may be expected to possess and use, 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,
6. 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.

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

Examples of scenarios referring to cases in which *effective* measures are not identified

93. 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 adequate supplementary measures.

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

94. A data exporter transfers personal data, whether by electronic transmission or by making it available to a cloud service provider or other processor to have personal data processed according to its instructions in a third country (e.g., for the provision of technical support or any type of cloud processing), and this data is not - or cannot- be pseudonymised as described in Use Case 2 or encrypted as described in Use Case 1 because the processing requires accessing data in the clear.

If

1. a controller transfers personal 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 in question goes beyond what is necessary and proportionate in a democratic society, where

in practice problematic legislation of the third country applies to the transfers in question (see Step 3).[86]

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 the data subject's fundamental 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.

95. 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: Transfer of personal data for business purposes including by way of remote access

96. A data exporter transfers personal data to entities - in a third country to be used for shared business purposes —whether by electronic transmission or by making it available to remote access by the data importer—, and this data is not - or cannot- be -pseudonymised as described in Use Case 2 or encrypted as described in Use Case 1 because the processing requires accessing data in the clear. One 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 an information system in a way that allows the importer direct access to data of its own choice, or by transferring it directly, individually or in bulk, through use of a communication service,
2. the importer[87] processes the data in the clear in the third country (including for its own purposes where the importer is a controller),
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, where in practice problematic legislation of the third country applies to the transfers in question (see Step 3),

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

97. 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

[86] See Articles 47 and 52 of the EU Charter of Fundamental Rights, Article 23.1 GDPR, and EDPB Recommendations 02/2020 on the European Essential Guarantees for Surveillance Measures, 10 November 2020.

[87] Whether it is a controller or processor in a third country receiving or getting access to personal data transferred from the EEA.

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.

2.2 Additional contractual measures

98. These measures will generally consist of unilateral, bilateral or multilateral[88] contractual commitments.[89] 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.[90]

99. 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 EEA. 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,[91] these measures may often need to 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.

100. 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.

101. 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.[92]

102. 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

103. Depending on the specific circumstances of the transfers (including the practical application of the third country legislation), the contract may need to provide that for transfers to take place,

[88] E.g. within BCRs which should in any case regulate some of the measures listed below.
[89] 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.
[90] 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.
[91] C-311/18 (Schrems II), paragraph 125.
[92] CJEU judgment C-311/18 (Schrems II), paragraph 132.

specific technical measures would have to be implemented (see supra the technical measures suggested).

104. Conditions for effectiveness:

- 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:

105. The exporter could add annexes to the contract with information that the importer would have provided before the conclusion of the contract, 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. It may also underscore the obligation of the importer to assist the exporter in its assessment and engage its liability in providing it with information that is objective, reliable, relevant, verifiable and publicly available or otherwise accessible information.

106. 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, etc.);

(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,[93] 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;[94]

(5) specify whether and to what extent the importer is legally prohibited to provide the information mentioned under (1) – (5) above.

[93] 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.

[94] 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.

107. 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.

108. 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.
- 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 EEA. 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.

***

109. 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.[95]

110. 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.
- 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 inform promptly the exporter once their existence comes to its knowledge.
- In circumstances where the data importer disclosed personal data transferred in violation of the commitments contained under the chosen transfer tool, the contract may also include compensation from the data importer to a data subject for any material and non-material damage suffered.

[95] This clause is important to guarantee an adequate level of protection of the personal data transferred and should usually be required.

***

111. The exporter could reinforce its power to conduct audits[96] 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.

112. 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.
- Access logs and other similar trails should be tamper proof (e.g. they should be made inalterable using state of the art encryption techniques, such as hashing, and also systematically transmitted to the exporter on a periodic basis) 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.

***

113. 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, in case of a change of the situation, 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".[97.]

114. This inability to comply may result from changes in the third country's legislation or practice.[98] 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.

115. 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

[96] 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.
[97] Clause 5.a and d.i of SCCs Decision 2010/87/EU.
[98] 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."

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

***

116. 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.

117. 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

118. 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

[99] This threshold should ensure that data subjects continue to be afforded a level of protection equivalent to that guaranteed within the EEA.

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.

119. 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 fulfil this commitment.

***

120. In the same situation as described above, 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[100] 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.

121. 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 fulfil this commitment.

[100] 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.

Empowering data subjects to exercise their rights

122. 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 agreement of the exporter and/or the data subject for a specific access to data.

123. 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).[101.]
- 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 plain 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.

***

124. 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), including compensation from the data importer for any material and non-material damage suffered because of the disclosure of his/her personal data transferred under the chosen transfer tool in violation of the commitments it contains.

125. 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 and compensate 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.

[101] Article 4(11) GDPR.

***

126. 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.

127. Conditions for effectiveness

- Some national regulations may not allow the data importer to provide this type of assistance directly to data subjects, although they may allow the data importer to procure this assistance for the data subjects.
- 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 EEA. 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 exists, including against surveillance measures.

2.3 Organisational measures

128. 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 EEA.

129. 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

130. Adoption of adequate internal policies with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for cases of formal or informal 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, composed of experts on IT, data protection and privacy laws, to deal with requests that involve personal data transferred from the EEA; 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.

131. 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.

132. 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.[102] When the request is incompatible, 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

133. 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.

134. 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 the failure to provide an adequate level of protection.

***

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

135. 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.

136. 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

137. 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).

138. 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 so 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 leads to the disclosure of identifiable data.

***

139. 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.

140. 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

141. 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.

Others

142. 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 essentially equivalent level of protection to that guaranteed within the EEA of the personal data transferred is maintained.

***

143. 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 essentially equivalent level of protection of the personal data to that afforded within the EEA cannot be guaranteed in the third country.[103]

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

ANNEX 3: POSSIBLE SOURCES OF INFORMATION TO ASSESS A THIRD COUNTRY

144. Your data importer should be in a position to provide you with relevant sources and information relating to the third country in which it is established, including the laws and the practices applicable to the importer and the data transferred. You and the importer may refer to several sources of information, such as the ones non-exhaustively listed below and presented by order of preference:

- Case-law of the Court of Justice of the European Union (CJEU) and of the European Court of Human Rights (ECtHR)[104] as referred to in the European Essential Guarantees recommendations;[105]
- Adequacy decisions in the country of destination if the transfer relies on a different legal basis;[106]
- Resolutions and reports from intergovernmental organisations, such as the Council of Europe,[107] other regional bodies,[108;] and UN bodies and agencies (e.g. UN Human Rights Council,[109] Human Rights Committee[110]);
- Reports and analysis from competent regulatory networks, such as the Global Privacy Assembly (GPA);[111]
- National case-law or decisions taken by independent judicial or administrative authorities competent on data privacy and data protection of third countries;
- Reports of independent oversight or parliamentary bodies;
- Reports based on practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, from entities active in the same sector as the importer;
- Warrant canaries of other entities processing data in the same field as the importer;
- Reports produced or commissioned by Chambers of commerce, business, professional and trade associations, governmental diplomatic, trade and investment agencies of the exporter or other third countries exporting to the third country to which the transfer is made;
- Reports from academic institutions, and civil society organizations (e.g. NGOs);

---

[104] See factsheet of the ECtHR jurisprudence on mass surveillance: https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf

[105] EDPB Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en

[106] C-311/18 (Schrems II), paragraph 141; see adequacy decisions in https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

[107] https://www.coe.int/en/web/data-protection/reports-studies-and-opinions

[108] See for instance country reports of the Inter-American Commission on Human Rights (IACHR), https://www.oas.org/en/iachr/reports/country.asp.

[109] See https://www.ohchr.org/EN/HRBodies/UPR/Pages/Documentation.aspx

[110] See: https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=5

[111] See e.g. https://globalprivacyassembly.org/wp-content/uploads/2020/10/Day-1-1_2a-Day-3-3_2b-v1_0-Policy-Strategy-Working-Group-WS1-Global-frameworks-and-standards-Report-Final.pdf

- Reports from private providers of business intelligence on financial, regulatory and reputational risks for companies;
- Warrant canaries of the importer itself;[112]
- Transparency reports, on the condition that they expressly mention the fact that no access requests were received. Transparency reports merely silent on this point would not qualify as sufficient evidence as these reports most often focus on access requests received from law enforcement authorities and provide figures only on this aspect while remaining silent on access requests for national security purposes received. This does not mean that no access requests were received but rather that this information cannot be shared;[113]
- Internal statements or records of the importer expressly indicating that no access requests were received for a sufficiently long period; and with a preference for statements and records engaging the liability of the importer and/or issued by internal positions with some autonomy such as internal auditors, DPOs, etc.[114]

[112] See conditions for the consideration of the documented practical experience of the importer with relevant prior instances of requests for access received from public authorities in the third country in paragraph 47.
[113] *Ibid.*
[114] *Ibid.*