International data transfers under GDPR: applicable requirements and practical implementation

Thomas ESPEEL
Avocat (Lexing)

Eléonore COLSON
Avocate (Lexing)

Alexandre CRUQUENAIRE
Avocat (Lexing), Chargé de cours invité à l'Université de Namur (CRIDS)

TABLE OF CONTENT

Introduction

1. With the increasing use of the internet and information technologies, European companies are developing collaborations across the world. Possibly combined with the common practice of outsourcing of IT services outside of the EU[1], this results in lots of international (personal) data flows. The transfer of (personal) data outside of the EU can be considered as a common practice for a huge number of European companies.

2. The Court of Justice of the European Union (CJEU) already addressed specific questions relating to international transfers of personal data.[2]

In its *Schrems II* judgment of 16 July 2020[3], the Court of Justice ruled the compliance with GDPR requirements from data controllers[4] to assess foreign legislations and governmental practices, in order to decide whether the transfer of personal data to the relevant non-EU countries may compromise the level of protection of the transferred data. Specific requirements apply if the assessment shows a risk for the level of protection of the personal data to be transferred.

Scholars noted this decision will have significant implications for many areas of EU law and policy, transatlantic relations and, more generally, global data governance[5], some authors considering the Court of Justice created a kind of Babylonian confusion in the data protection law landscape.[6] Indeed, it is worth noting the practical implementation of the Court decision does not appear to be an easy job.

The aim of the present paper is therefore to present the key elements of the *Schrems II* decision, but also and mainly to address the practical difficulties for European companies to comply with the outcome of this specific case law.

1. References to "EU" made throughout this paper should be understood as references to "EEA" and conversely.
2. See in particular CJEU, 6 October 2015, *Maximillian Schrems v. Data Protection Commissioner*, Case C-362/14 (hereinafter "*Schrems I*") whereby the CJEU invalidated the European Commission's Safe Harbor Decision. For an historical overview of the issue of personal data transfers between the EU and the US, see M. BERNAERTS, "Les transferts de données à caractère personnel entre l'Union européenne et les Etats-Unis: une valse à mille temps?", *RDC-TBH* 2017/2, pp. 161-184.
3. CJEU, 16 July 2020, *Data Protection Commissioner vs Facebook Ireland Ltd and Mr. Schrems,* C-311/18 (hereinafter "*Schrems II*").
4. With the support of the relevant processors.
5. M. ZALNIERIUTE and G. CHURCHES, "Rejecting the Transatlantic Outsourcing of Data Protection in the Face of Unrestrained Surveillance", *Cambridge Law Journal*, 2021, 80(1), p. 8-11, UNSW Law Research Paper No. 21-32, available at: https://ssrn.com/abstract=3805488.
6. For other comments of the decision, see among others F. JACQUES, "'Uncle Sam is watching you' Retour sur les enseignements de l'arrêt Schrems II de la Cour de justice de l'Union européenne", *JT*, 2021/13, p. 246-249; V. LOBATO CERVANTES, "The Schrems II Judgment of the Court of Justice Invalidates the EU – U.S. Privacy Shield and Requires 'Case by Case' Assessment on the application of Standard Contractual Clauses (SCCs)", *EDPL*, 2020/4, p. 602-606; V. VANDER GEETEN, "L'arrêt de la Cour de justice de l'Union européenne Schrems II et ses conséquences pour les transferts internationaux de données", *DPOnews*, 2020/10, p. 6-9; J. SAURON, "Le tohu-bohu de l'arrêt Schrems II: l'Union européenne pourra-t-elle sortir de l'impasse dans laquelle elle s'est elle-même placée?", *DPOnews*, 2021/12, pp. 4-7.

Part I – Background and consequences of the CJEU judgment in the Schrems II case

3. The factual background of *Schrems II* case can be summarised as follows. Max Schrems, an Austrian data protection activist, lodged a complaint before the Irish supervisory authority (Data Protection Commission – DPC) to prohibit transfers of personal data from Facebook Ireland to the US Facebook Inc. company. Following the Snowden revelations on US mass surveillance programmes in 2013[7], Mr Schrems considered that US law and government practices did not sufficiently protect personal data processed in the US against mass surveillance as performed by US public authorities. On the basis of the provisional findings of its investigation, the DPC decided to refer the matter to the High Court. The results of this investigation were such as to call into question the validity of the EU-US Privacy Shield decision and the standard contractual clauses as adopted by the European Commission on which Facebook's data transfers were partly based.[8]

4. In the present section of the paper, we will focus on the main elements of the Court of Justice decision. After a brief overview of the data transfers regime under the GDPR (1), we will highlight the outcome of the landmark *Schrems II* decision: the invalidation of the EU-US Privacy Shield (2) and the confirmation of the Standard Contractual Clauses mechanism subject to specific conditions (3). Finally, we will wrap up the most relevant aspects of the US laws governing surveillance as referred to in the *Schrems II* case (4).

1. General principles for international data transfers

5. Chapter V of the GDPR covers the issue of "international data transfers". First of all, it is important to define the notion of "international data transfers" (1.1. and 1.2.). Then, we will briefly introduce the different legal mechanisms allowing international data transfers under the GDPR (1.3).

1.1. The concept of "data transfer" (material scope)

6. It is first required to properly delineate the concept of "transfer". In the absence of a formal definition of "transfer of personal data", the European Data Protection Supervisor (EDPS) considers that "transfer" would normally imply the following elements: *"communication, disclosure or otherwise making available of personal data, conducted with the knowledge or intention of a sender subject to the Regulation that the recipient(s) will have access to it"*.[9]

The notion of transfer would therefore cover both "deliberate transfers of" and "permitted access to" personal data. The conditions of "knowledge" or alternatively "intention" would clearly exclude cases of access through illegal actions (*e.g.* hacking). However, it is less obvious in the case where data cross the borders of the EU without a clear intention or knowledge of the controller or processor. It may occur, for instance, where data are redirected to servers located in different countries for network configuration reasons.[10]

However, a definition of transfer relying on the controller's or processor's knowledge or intention can be questioned. Indeed, such requirement is likely to raise the risk of arbitrary delineation of the scope of the "transfer" concept. For example, in *Schrems II* (see below), the CJEU has confirmed that transferring personal data even indirectly to non-EU public authorities may interfere with the protection of EU fundamental rights (*i.e.* rights of privacy and personal data protection), "*whatever the subsequent use of the information concerned*".[11] In its ruling, the Court did not take into account the intention or knowledge of the controller or processor, but exclusively focused on whether public authorities outside the EU can access the transferred data (the mere possibility being sufficient).[12] The legal debate on the notion of "transfer" is therefore not closed.

As a consequence, we consider that any act which makes accessible personal data outside the EU should be considered a "transfer" in the meaning of GDPR. It covers two different situations: when the data is physically stored outside the EU and when it is physically stored inside the EU but is accessible to entities

7. J. BALL, *NSA Stores Metadata of Millions of Web Users for up to a Year, Secret Files Show*, *The Guardian*, 2013, available at: https://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents.
8. See F. JACQUES, "'Uncle Sam is watching you' Retour sur les enseignements de l'arrêt Schrems II de la Cour de justice de l'Union européenne", *op. cit.*, p. 246.
9. EDPS, The transfer of personal data to third countries and international organisations by EU institutions and bodies, Position paper, 2014, available at: https://edps.europa.eu/sites/default/files/publication/14-07-14_transfer_third_countries_en.pdf.
10. L. DRECHSLER and I. KAMARA, "Essential Equivalence as a Benchmark for International Data Transfers After Schrems II" in *Research Handbook on EU data protection,* Edward Elgar Publishing Ltd., 2021, p. 5. According to the UK Information Commissioner (ICO), personal data "just electronically routed through a non-EEA country" while being sent from an EEA country to another EEA country are not considered a data transfer. See ICO, 'International transfers after the UK exist from the EU Implementation Period', available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exi.
11. CJEU, Case C-311/18 *Schrems II*, §§ 170-171.
12. CJEU, Case C-311/18 *Schrems II*, §§ 178-185.

located outside the EU.[13] It seems confirmed by the European Data Protection Board (EDPB), following which a "data transfer" includes notably:

– the communication, the copy or the displacement of personal data to third countries; but also
– the provision of access to the personal data;
– the remote access from a third country (*e.g.* for IT support services) and/or hosting (cloud or not) outside the EU; and
– the onward transfers (*e.g.* when a processor outside the EEA transfers personal data entrusted to him to a sub-processor in another third country or in the same third country).[14]

1.2. The concept of "international transfer" (territorial scope)

7. The clarification of the concept of "data transfer" is not enough; it is also necessary to further explain what is meant by "international transfer".
Unfortunately, the GDPR does not provide for a legal definition of the concept of "international transfers" (*i.e.* what constitutes a "*transfer of personal data to third country or to an international organisation*").

8. On 18 November 2021, the EDPB finally published long-awaited guidelines on the interplay between article 3 and Chapter V of the GDPR.[15] The guidelines are subject to public consultation until the end of January 2022.

The aim of these guidelines is to clarify the notion of "international data transfer" in order to assist EU controllers and processors in identifying whether a processing constitutes an international transfer and, consequently, whether they have to comply with the provisions of Chapter V of the GDPR.

According to the EDPB Guidelines, three cumulative criteria must be met to qualify a processing as an international data transfer:

– The data exporter (a controller or processor) is subject to the GDPR for the given processing.[16]
– This data exporter transmits or makes available the personal data to the data importer (another controller, joint controller or processor).[17] Logically, it is not the case if the data are disclosed directly and by the data subject (on his/her own initiative) to the recipient. Furthermore, as anticipated, the EDPB specifies that the situation where a processor in the EU sends data back to its controller in a third country must be understood as an international data transfer. The EDPB also recalled that entities belonging to the same group of companies may qualify as separate controllers or processors. Therefore, disclosures of data between entities belonging to the same group may constitute transfers of personal data.
– The data importer is in a third country or is an international organization, irrespective of whether or not this importer is subject to the GDPR in respect of the given processing in accordance with article 3.[18] Based on this third criterion, the importer shall be geographically in a third country or is an international organization, regardless of whether the processing at hand falls under the scope of the GDPR. This may appear surprising since the Recital 7 of the new Standard Contractual Clauses of the European Commission clearly indicates that the SCCs could not be used for the transfer to non-EU data importers already subject to the GDPR (including based on the extraterritorial application of article 3(2)). EDPB therefore creates new complexity by requiring the adoption of a new transfer tool.[19] In the EDPB's minutes (point 2) of its 54th plenary meeting held in September 2021[20], the EDPB stated that following the adoption of these guidelines, the EU Commission intends to develop a specific set of SCCs regarding transfers to importers subject to article 3(2) GDPR.

1.3. Data transfers mechanism

9. As already mentioned, the transfer of personal data outside the EU is regulated in Chapter V of the GDPR. As a general principle, the GDPR prohibits transfers

13. In this sense, see V. VANDER GEETEN, "L'arrêt de la Cour de justice de l'Union européenne Schrems II et ses conséquences pour les transferts internationaux de données", *DPOnews*, 2020/10, p. 7 and C. DE TERWANGNE and E. DEGRAVE, "Titre 6 – Le RGPD et les transferts internationaux de données à caractère personnel", in *La protection des données à caractère personnel en Belgique*, Bruxelles, *Politeia* 2019, p. 289.
14. EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 18 June 2021, available at: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en, p. 9.
15. EDPB, Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, 18 November 2021, available at: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-052021-interplay-between-application_en.
16. The EDPB recalls that controllers and processors, which are not established in the EU, may be subject to the GDPR pursuant to article 3(2) (and shall thus comply with Chapter V when transferring personal data to a third country or to an international organisation).
17. These concepts have been further developed in the EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR.
18. The EDPB illustrates this criterion with the following clear example: Company A, a controller without an EU establishment, offers goods and services to the EU market. The French company B, is processing personal data on behalf of company A. B re-transmits the data to A. The processing performed by the processor B is covered by the GDPR for processor-specific obligations pursuant to article 3(1), since it takes place in the context of the activities of its establishment in the EU. The processing performed by A is also covered by the GDPR, since article 3(2) applies to A. However, since A is in a third country, the disclosure of data from B to A is regarded as a transfer to a third country and therefore Chapter V applies.
19. On this point see: https://iapp.org/news/a/new-edpb-guidelines-define-international-transfers-dancing-in-place/.
20. Available at: https://edpb.europa.eu/system/files/2021-10/20210914plenfinalminutes_54thplenary_public.pdf.

of personal data outside the EU.[21] [22] The objective of such a transfer's regime is clearly to preserve a high level of fundamental rights for EU data subjects.[23] However, articles 44-49 GDPR provide for a "multi-tiered framework" allowing international data transfers.[24]

The first tier of the regime is based on the concept of 'adequate level of protection', under which the Commission adopts decisions on the adequacy of a non-EU third country ("adequacy decisions").[25]

The second ground for transfers to third countries and international organizations relies on the concept of 'appropriate safeguards', whereby controllers and processors exporting personal data provide safeguards for the processing carried out by controllers or processors in third countries.[26]

Thirdly, the GDPR provides for a list of 'derogations' qualifying transfers as lawful, subject to the fulfillment of specific conditions.[27]

10. Adequate level of protection – The GDPR stipulates that the transfer of personal data to a third country (*i.e.* outside the European Economic Area – "EEA"[28]) or an international organization may, in principle, only take place if the non-EU third country ensures an adequate level of protection for personal data (so-called 'whitelisted countries').

The European Commission may decide that a third country, a territory or one or more specified sectors within that third country, or an international organization ensures an adequate level of protection.[29]

The list of countries recognized as such are[30]: Andorra, Argentina, Canada (commercial organizations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, South Korea, Switzerland, United Kingdom and Uruguay.

According to the European Commission: "*The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to that third country without any further safeguard being necessary. In other words, transfers to the country in question will be assimilated to intra-EU transmissions of data*".[31]

11. Appropriate safeguards – In the absence of an adequacy decision, international data transfers can only take place if the EU-data exporter implements appropriate safeguards, and insofar as enforceable rights and effective legal remedies are available to data subjects.[32]

The appropriate safeguards may be provided for by:
- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules (BCR) in accordance with article 47 GDPR;
- standard contractual data protection clauses (SCCs);
- an approved code of conduct (pursuant to article 40 GDPR) or an approved certification mechanism (pursuant to article 42 GDPR).

12. Specific derogations – Finally, in the absence of an adequacy decision or of appropriate safeguards, a transfer of personal data to a third country or an international organization may take place only if one of the following conditions are met (*i.e.* derogations for specific situations)[33]:
- The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards.
- The transfer is necessary for the performance of a contract between the data subject and the controller, or the implementation of pre-contractual measures taken at the data subject's request.
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary for the establishment, exercise or defence of legal claims.
- The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

21. GDPR, article 44.
22. Regarding the debate on the regulatory approach of the GDPR towards data transfers (prohibitive versus permissive), see notably: L. DRECHSLER and I. KAMARA, "Essential Equivalence as a Benchmark for International Data Transfers After Schrems II" in *Research Handbook on EU data protection*, Edward Elgar Publishing Ltd., 2021, pp. 3-5, available at SSRN: https://ssrn.com/abstract=3881875 or http://dx.doi.org/10.2139/ssrn.3881875.
23. Article 44 and recital 101 GDPR.
24. C. KUNER, 'Article 45', in Kuner/Bygrave/Docksey (eds.), *The General Data Protection Regulation (GDPR): A commentary* (OUP 2020), p. 774.
25. GDPR, article 45.
26. GDPR, article 46.
27. GDPR, article 49.
28. The EEA includes the member states of the European Union, Iceland, Norway and Liechtenstein.
29. GDPR, article 45.
30. As published by the European Commission on 31 December 2021.
31. See: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
32. GDPR, article 46.
33. GDPR, article 49. Theses derogations must be interpreted restrictively.

– The transfer is made from a register which according to Union or member state law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or member state law for consultation are fulfilled in the particular case.

2. Main elements of Schrems II decision

2.1. The invalidation of the EU-US Privacy Shield decision

13. In its long-awaited judgement, the Grand Chamber of the Court of Justice of the European Union invalidated the key mechanism for EU-United States data transfers (*i.e.* the EU-US Privacy Shield) on the basis that the US laws, and in particular certain surveillance programmes (*i.e.* Section 702 FISA and E.O. 12333 – for more details see below) authorising the access and use by US public authorities of personal data transferred from the EU to the US for national security purposes, do not guarantee to the transferred personal data a level of protection that is "essentially equivalent" to that required under EU law.[34] Furthermore, the Court emphasised that US legislation did not grant data subjects enforceable rights against the US authorities, as a result of which the data subjects have no right to an effective remedy.

As a consequence, the Court considered that the United States did not provide a level of protection to the personal data transferred that is substantially equivalent to that required under EU privacy law and therefore declared the Privacy Shield adequacy decision invalid.[35]

2.2. The confirmation of the standard contractual clause mechanism

14. In its request for a preliminary ruling, the referring Irish court asked whether the European Commission's Decision 2010/87/EC on Standard Contractual Clauses (SCCs) was capable of ensuring an adequate level of protection of the personal data transferred to third countries given that the standard data protection clauses provided for in that decision do not bind the supervisory authorities of those third countries. Indeed, although those clauses are binding on a controller established in the EU ("data exporter") and the recipient of the transfer of personal data established in a third country ("data importer") insofar as they have concluded together a contract incorporating those clauses, it is obvious that the SCCs are not binding for the authorities of that third country, since they are not party to the signed agreement.[36]

15. In its judgment, the CJEU therefore examined the SCC Decision 2010/87/EC and declared it valid.

However, the Court ruled that such validity is subject to the ability of the SCCs to ensure the effectiveness of the granted protection which has to be substantially equivalent to the level of protection guaranteed within the EU by the GDPR.

More specifically, the Court further specified that the 2010/87/EC decision imposes to the data exporter and the recipient of the data the duty to verify (on a "case-by-case analysis"), prior to any transfer, the compliance of the third country with the level of protection granted by EU law. If it is not the case, adequate additional measures must be implemented to align with such an EU protection level.[37] The data importer is also committed to inform the data exporter of any inability to comply with the standard data protection clauses.

The transfer of personal data based on SCCs is therefore subject to the outcome of a prior assessment of the level of protection of personal data within the relevant third country, taking into account the circumstances of the transfers and the so-called "supplementary measures" if need be. If the assessment shows the controller or the processor established in the European Union is not able to take adequate additional measures to guarantee such a level of protection, the controller or processor is required to suspend ("freeze") or stop the transfer of personal data to the concerned third country.[38]

2.3. US surveillance regime

As already mentioned, the *Schrems II* case involved different US surveillance legislations, and in particular Section 702 of the Foreign Intelligence Surveillance Act (FISA) (section 3.1 below) and the Executive Order 12333 (E.O. 12333) (section 3.2. below). An overview of these US pieces of legislation is necessary to properly understand the Court of Justice reasoning.

In the following section of the paper, we will therefore present these legal provisions which played a major role in the Court of Justice decision.

34. Regarding the standard of 'essential equivalence' as the benchmark for the GDPR transfers regime see L. DRECHSLER and I. KAMARA, "Essential Equivalence as a Benchmark for International Data Transfers After Schrems II" in *Research Handbook on EU data protection, op. cit.*
35. See in particular §§ 150-202.
36. §§ 123-125.
37. § 133.
38. § 135.

3. Overview of the most relevant US laws governing surveillance

3.1. Foreign Intelligence Surveillance Act (FISA) and Foreign Intelligence Surveillance Amendments Act (FAA)

3.1.1. Historical background and aim of the act

16. Initially, the US law applicable to surveillance activities was mainly based on the balance between the Fourth Amendment of the Constitution, protecting the American citizens against "*unreasonable searches and seizures*"[39], and the power of the president to authorize warrantless electronic surveillance for national security purposes.[40]

The US case law progressively imposed some limitations to the surveillance power of the government, based on the preservation of the Fourth Amendment and the protection of US citizens.[41]

17. The situation changed with the investigations carried out by the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (*Church Committee*), which publicly revealed large-scale abuse of the foreign intelligence surveillance purpose to conduct domestic surveillance.[42] The US Congress therefore decided to adopt, in 1978, the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq* (FISA), in order to impose a legal regime to ringfence the domestic surveillance activities.[43]

The FISA aims at reaching a balance between the desire to facilitate the acquisition of foreign intelligence information in the interests of US national security and, on the contrary, the intent to safeguard constitutional protection where the scope of foreign intelligence activities encompasses communications of US citizens.[44]

The FISA of 1978 established a special secret court – named the US Foreign Intelligence Surveillance Court (FISC)[45] – to review US government applications for approval of electronic surveillance, physical searches, and certain other forms of investigative actions for foreign intelligence purposes.

Following 9/11, the USA PATRIOT Act[46] extended the government power to conduct surveillance activities towards foreign powers, in order to deter and punish terrorist acts in the United States and around the world. FISA's initial requirements were softened, and government powers enlarged accordingly.[47]

The Protect America Act (PAA) in 2007 and the Foreign Intelligence Surveillance Amendments Act (FAA) in 2008 (replacing the PAA which expired earlier in 2008) brought amendments to the FISA, in order to soften the legal requirements for conducting surveillance activities. More specifically, the FAA replaced the individual warrant requirement (based on pre-identified targets) with a generic authorization (based on the review of rules proposed by the government).[48] The FAA also imposed on electronic communication service providers a duty to cooperate, with a right to challenge orders (called 'directives') to provide access to information of their clients.

3.1.2. Scope and conditions of the act

18. The scope of the FISA is interesting in the framework of the issues raised by the *Schrems II* case.[49]

Title VII of FISA includes Section 702, which concerns the surveillance of non-US persons outside the US.

19. Section 702 of FISA allows the (*i*) targeting of persons who are not US persons (*ii*) who are reasonably believed to be located outside the United States (*iii*) with the compelled assistance of an electronic communication service provider, and (*iv*) in order to acquire foreign intelligence information.[50]

20. Within the meaning of the FISA, "person" means "*any individual, including any officer or employee of the Federal Government, or any group, entity,*

39. US Const., Amendment IV: "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized*".
40. K. POORBAUGH, "Security Protocol: A Procedural Analysis of the Foreign Intelligence Surveillance Courts", *U. Ill. L. Rev.* 1363, 2015, p. 1366.
41. See for instance the Supreme Court decision in the *Keith* case, where the Court found a Fourth Amendment breach, but only regarding the warrantless wiretaps in a case involving domestic threats to national security: *United States v. United States District Court*, 407 US 297 (1972).
42. K. POORBAUGH, "Security Protocol: A Procedural Analysis of the Foreign Intelligence Surveillance Courts", *op. cit.*, p. 1369.
43. See E.B. BAZAN, The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions (CRS Report for Congress), updated 22 September 2004, available at: https://irp.fas.org/crs/RL30465.pdf.
44. W.C. BANKS, "The Death of FISA", *Minnesota Law Review* 641, 2007, pp. 1216-1233.
45. The FISC consists of 11 federal trial judges appointed by the Chief Justice of the United States for a single-year term spending alternately one week out of every 11 on the FISC in Washington, D.C. (50 U.S.C. § 1803(a)(1), 1803(d)). If the government application is rejected, an appeal is possible for the government before the Foreign Intelligence Court of Review (FISA Appeals Court – see 50 U.S.C. § 1803(b)).
46. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001.
47. K. POORBAUGH, "Security Protocol: A Procedural Analysis of the Foreign Intelligence Surveillance Courts", *op. cit.*, p. 1374.
48. E. BERMAN, "The Two Faces of the Foreign Intelligence Surveillance Court", *Indiana Law Journal*, vol. 91: Iss. 4, 2016, p. 1200.
49. For an in-depth analysis of the FISA 702, see also the Expert Opinion from Prof. Stephen I. Vladeck (University of Texas School of Law) on the Current State of U.S. Surveillance Law and Authorities, 15 November 2021. Available at: https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/Vladek_Rechtsgutachten_DSK_en.pdf.
50. 50 US Code § 1881 a.

association, corporation, or foreign power".[51] According to the Privacy and Civil Liberties Oversight Board, "*the definition of 'person' is therefore broad, but not limitless: a foreign government or international terrorist group could qualify as a 'person' but an entire foreign country cannot be a 'person' targeted under Section 702*".[52]

21. Electronic surveillance targeting persons believed to be located in the US is not allowed by Section 702, whether such persons are US persons or not.[53]

22. The concept of "*electronic communication service provider*" is defined by the FISA as including a variety of telephone, Internet service, and other communication providers (including cloud service providers such as Microsoft or Amazon).

23. A significant purpose of the acquisition must be to obtain foreign intelligence information. The acquisition of foreign intelligence information does not need to be the sole or primary purpose of surveillance.[54]

The concept of "foreign intelligence information" is broadly defined as:

"*(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against –*

(a) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(b) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(c) clandestine intelligence activities by an intelligence service or network of a foreign and power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to –

(a) the national defence or the security of the United States; or

(b) the conduct of the foreign affairs of the United States.".[55]

The FISA does not contain any definition of the "foreign affairs" and the lack of publicity of the FISA Court's decisions does not favour clarity. The broad nature of the concept seems undisputable.[56] Some scholars are trying to ringfence the scope of allowed surveillance activities under this requirement[57], but the applicable standard remains vague.

24. Acquisition under 50 U.S.C. § 1881a(a) (*i.e.* FISA Section 702) is subject to several procedural safeguards aiming to ensure the constitutional protection of US persons and others located in the United States.[58]

To mitigate the risk, the FISA surveillance may interfere with the constitutional rights of US persons, the attorney general (AG) (in consultation with the director of national intelligence – DNI) must adopt targeting procedures[59] and minimization procedures.[60] These procedures aim at limiting the acquisition, retention and dissemination of non-public information about US persons.[61] More specifically, the targeting procedures are designed to ensure that an acquisition only targets persons outside the US, while minimization procedures protect the identities of US persons and any non-public information concerning them that may be incidentally acquired.[62]

Furthermore, the AG and the DNI must certify that a significant purpose of the acquisition is to obtain foreign intelligence information.[63] The aim of such a limitation is to secure the sharing of information

51. 50 US Code § 1801(m).
52. *See* Privacy and Civil Liberties Oversight Board, Transcript of Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, at 71 (19 March 2014) ("PCLOB March 2014 Hearing Transcript") (statement of Rajesh De, General Counsel, NSA, in response to questions by James Dempsey, Board Member, PCLOB), available at: https://www.pclob.gov/library/20140319-Transcript.pdf, cited in Privacy and Civil Liberties Oversight Board, Report on the Surveillance program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance, 2 July 2014, p. 6. Available on the official web site of the PCLOB: https://www.pclob.gov/reports/report-702/.
53. 50 U.S.C. §§ 1881.a(b)(1).
54. Indeed, the USA PATRIOT Act amended the original FISA's purpose provision by requiring the government to certify only that a "significant purpose" of the requested surveillance is the acquisition of foreign intelligence information. This amendment thus replaced the "primary purpose" test by a lighter "significant purpose" test. For further information on the practical impact of this amendment, see K. POORBAUGH, "Security Protocol: A Procedural Analysis of the Foreign Intelligence Surveillance Courts", *op. cit.*, p. 1374. About the historical background of this specific requirement, see S.J. GLICK, "FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security", *Harvard National Security Journal*, vol. 1, 2010, pp. 88-143.
55. 50 U.S.C. § 1801(e).
56. There is a kind of consensus on the broad scope of the concept of "foreign affairs". See for instance: Privacy International, "A guide to FISA § 1881 a: the law behind it all", 9 February 2018, https://privacyinternational.org/blog/1439/guide-fisa-ss1881a-law-behind-it-all.
57. See in particular P. MARGULIES, "Defining 'Foreign Affairs' in Section 702 of the FISA Amendments Act: The Virtues and deficits of Post-Snowden Dialogue on US Surveillance Policy", *Washington and Lee Law Review*, vol. 72, Issue 3, 2015, pp. 1301-1302 (referring to the allowed collection of data about the "*intent of foreign governments*", based on the assumption that reciprocity in espionage makes the process acceptable under international law standards – also highlighting that *"foreign governments also constantly seek to learn 'what their adversaries are doing"*, which would make unwise unilateral restraint by the USA).
58. 50 U.S.C. § 1881a(b).
59. 50 U.S.C. § 1881a(d).
60. 50 U.S.C. § 1881a(e).
61. 50 U.S.C. § 1881a(d) and 50 U.S.C. § 1881a(e).
62. 'Letter to (US Congress) John BOEMER, Harry REID, Nancy PELOSI and Mitch MCCONNELL about the re-authorization of Title VII of the Foreign Intelligence Surveillance Act (FIS) enacted by the FISA Amendments Act of 2008 (FAA)', 8 February 2012, p. 2. Available at: https://www.justice.gov/sites/default/files/ola/legacy/2012/11/08/02-08-12-fisa-reauthorisation.pdf.
63. 50 U.S.C. 1881a(h)(2)(A)(v).

initially collected for foreign intelligence purposes with the authorities in charge of law enforcement.[64]

The limitations to the US government's ability to carry out surveillance activities are therefore based on the nationality (non-US person) of the target and its location (outside of the USA), which means that the US government is allowed to monitor billions of communications, "*into a warrantless foreign intelligence collection framework, as long as there is a chance that the net will pull in some information relating to security or foreign affairs*".[65] In addition, the FISC found it unnecessary to limit foreign intelligence to foreign powers or their agents when the target is a non-citizen overseas.[66]

3.1.3. Procedural aspects

25. From a procedural point of view, the FISA surveillance mainly covers two types of procedures: validation of surveillance plan as proposed by the US government, and validation/challenge of government's directives by the electronic communication service providers (ECSPs).

26. It is worth noting the amendments to the FISA resulted in a reduced control on surveillance activities. Indeed, since the FISA Amendments Act (FISAA), 50 U.S.C. § 1881 a surveillance does no longer require individualized authorization by FISC judges and has been replaced by so-called programmatic authorization.[67] The role of FISC is therefore not to determine that a specifically targeted individual person or facility meets the legal requirements, but rather to review, *in abstracto*, the general rules proposed by the government on permissible targets to conduct its surveillance activities (based on its own decisions to implement such general rules).[68]

The procedure before the FISC is non-adversarial and exclusively conducted *ex parte*.[69] The lack of adversarial debate does not help the FISC in its auditor role and favours the government's position.[70]

27. As already stated, § 1881 a surveillance can take place with the compelled assistance of electronic communication service providers. The "*electronic communication service providers*" definition includes telecommunications carriers, providers of electronic communication services and providers of remote computing services (*i.e.* cloud providers). Is such a provider located outside of the USA (*e.g.* in Europe) subject to § 1881 a surveillance? Without any specific provision addressing the point within the FAA 2008, the question is answered by the case law.[71] The location where the data are stored is not decisive to determine whether a cloud service provider is subject to the FISA jurisdiction.[72]

Authorizations under Section 702 may require the assistance of electronic communication service providers which can be requested to immediately provide the government with all information, facilities, or assistance necessary to accomplish the acquisition in a manner that will protect the secrecy of the acquisition and produce a minimum of interference with the services that such an electronic communication service provider is providing to the target of the acquisition. The service provider is therefore not allowed to inform its customers about the request to get access to their data. Furthermore, the service providers may also be requested to maintain under security procedures any records concerning the acquisition.[73] As an incentive to the service providers to cooperate with government orders, no action may be brought in any US court against them for providing assistance in accordance with 50 U.S.C. § 1881a(i)(1).[74] The assistance may be imposed in case of refusal to cooperate with the issued directive, the FISC being entitled to issue an order to compel.[75]

To challenge a directive, a service provider has to file a petition before the FISC either to modify or to set aside the received directive. The decision of the FISC on the challenge of the directive may be appealed before the FISA Court of Review by either the government or the service provider. A petition before the

64. S.J. GLICK, "FISA's Significant Purpose Requirement and the Government's Ability to Protect National Security", *op. cit.*, pp. 110-115.
65. E. GOITEN and F. PATEL, "*What went wrong with the FISA Court*", Brennan Center for Justice at New-York University School of Law, 2015, available at: https://www.brennancenter.org/sites/default/files/2019-08/Report_What_Went_%20Wrong_With_The_FISA_Court.pdf, p. 41.
66. See FISC decision available on the EFF website: https://www.eff.org/files/2015/03/02/fisc_opinion_and_order_september_4_2008.pdf.
67. NSA Director of Civil Liberties and Privacy Office Report: NSA's implementation of Foreign Intelligence Surveillance Act Section 702, 16 April 2014, p. 2 ("NSA DCLPO REPORT"), *available at* http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf (noting that Section 702 certifications do not require "individualized determination" by the FISC).
68. E. BERMAN, "The Two Faces of the Foreign Intelligence Surveillance Court", *op. cit.*, p. 1200 (considering that the FISC becomes a kind of rule maker approving the set of rules proposed by the government).
69. US Foreign Intelligence Surveillance Court, Rules of procedure, Effective 1 November 2010, Rule 17 (b) and Rule 30, available on the official website of the FISA Court: https://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.
70. E. BERMAN, "The Two Faces of the Foreign Intelligence Surveillance Court", *op. cit.*, p. 1240 (arguing that adversarial debate may lead to a more balanced FISC case law, compared with the fact that the bulk collection program had been approved by the FISC over thirty times before the Snowden leaks).
71. J. VAN HOBOKEN, A. ARNBAK and N. VAN EIJK, "Obscured by Clouds or How to Address Governmental Access to Cloud Data From Abroad", *op. cit.*, p. 9. Regarding § 1881 a, the US Supreme Court ruled that the Fourth Amendment does not protect non-US persons (*United States v. Verdugo--Urquidez*, 494 U.S. 259, 267 (1990)).
72. See W. MAXWELL and C. WOLF, "A Global Reality: Governmental Access to Data in the Cloud", 23 May 2012, available at: https://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf; J. VAN HOBOKEN, A. ARNBAK and N. VAN EIJK, "Obscured by Clouds or How to Address Governmental Access to Cloud Data From Abroad", *op. cit.*, p. 10.
73. 50 U.S.C. § 1881a(i)(1).
74. 50 U.S.C. § 1881a(i)(3).
75. 50 U.S.C. § 1881a(i)(5)(A). The non-compliance with such an order may be qualified as a contempt of court (D).

Supreme Court is similarly available to both parties against the FISA Court of Review's determination.

3.1.4. Acquisition process

28. As explained above, once foreign intelligence acquisition has been authorized under Section 702, the US government sends written directives to ECSPs compelling their assistance in the acquisition of communications.

Practically, the US government identifies (or "tasks") certain "selectors" (such as email addresses or telephone numbers) that are associated with targeted persons and sends these selectors to ECSPs to process the acquisition.[76]

29. Following amendments implemented with the FISAA 2008, FISA is claimed to be technology-neutral.[77] Indeed, the technology used to transmit the intercepted data does not make any difference: both open transmission over the airwaves via satellite and closed transmission via optical cable fall within the scope of FISAA.[78]

From a technical point of view, there are two main types of Section 702 acquisitions: "Downstream collection" (previously referred to as 'PRISM collection') and "Upstream collection".[79]

Under "downstream collection", the US government sends selectors (*e.g.* an email address) to a US-based ECSP (such as an Internet Service Provider – 'ISP') that has received a directive. Under such a directive, the service provider is obliged to give the US government the communications sent 'to or from' that selector (at the exclusion of the communications that are only 'about' the selector).

Then, NSA receives all downstream collection acquired under Section 702 and a copy of the raw data acquired may also be sent to the CIA and/or FBI.[80]

Upstream collection is different since it does not occur with the compelled assistance of US-ISPs, but instead with the compelled assistance (through a Section 702 directive) of the providers that control the telecommunications "backbone" over which – telephone and Internet[81] – communications transit.[82]

Therefore, the collection "*does not occur at the local telephone company or email provider with whom the targeted person interacts (which may be foreign telephone or Internet companies, which the government cannot compel to comply with a Section 702 directive), but instead occurs 'upstream' in the flow of communications between communication service providers*".[83]

Finally, the upstream collection of Internet communications includes the acquisition of so-called about communications and the acquisition of so-called multiple communications transactions ('MCTs').[84]

3.2. Executive Order 12333

30. Beyond the FISA, surveillance activities of the US government may also rely on the Executive Order 12333[85], which is an executive order signed on 4 December 1981 by US President Ronald Reagan which establishes an overarching policy framework for the Executive Branch's spying powers.[86] The EO 12333 is a legal authority used by the NSA for the majority of its foreign intelligence surveillance activities.[87] EO 12333 provides for both authorizations and restrictions for the collection of foreign intelligence information from non-US persons (even if it also allows in

76. Privacy and Civil Liberties Oversight Board, Report on the Surveillance program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance, 2 July 2014, p. 6. Available on the official website of the PCLOB: https://www.pclob.gov/reports/report-702/.
77. J. VAN HOBOKEN, A. ARNBAK and N. VAN EIJK, "Obscured by Clouds or How to Address Governmental Access to Cloud Data From Abroad", *op. cit.*, p. 10.
78. *Ibidem*.
79. For more details about "downstream collection" and "upstream collection", see Privacy and Civil Liberties Oversight Board, Report on the Surveillance program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance, 2 July 2014, pp. 33-41.
80. Privacy and Civil Liberties Oversight Board, Report on the Surveillance program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance, 2 July 2014, p. 34.
81. Contrary to downstream collection, upstream collection thus also includes telephone calls in addition to Internet communications.
82. See Privacy and Civil Liberties Oversight Board, Transcript of Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, at 26 (March 19, 2014) ("PCLOB March 2014 Hearing Transcript") (statement of Rajesh De, General Counsel, NSA, in response to questions by James Dempsey, Board Member, PCLOB).
83. Privacy and Civil Liberties Oversight Board, Report on the Surveillance program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance, 2 July 2014, p. 35. See also PCLOB March 2014 Hearing Transcript, supra, at 26 (statement of Rajesh De, General Counsel, NSA) (stating that "*This type of collection upstream fills a particular gap of allowing us to collect communications that are not available under PRISM collection.*").
84. An "about" communication is "*one in which the selector of a targeted person (such as that person's email address) is contained within the communication but the targeted person is not necessarily a participant in the communication. Rather than being 'to' or 'from' the selector that has been tasked, the communication may contain the selector in the body of the communication, and thus be 'about' the selector*". An "MCT" is "*an Internet 'transaction' that contains more than one discrete communication within it. If one of the communications within an MCT is to, from, or 'about' a tasked selector, and if one end of the transaction is foreign, the NSA will acquire the entire MCT through upstream collection, including other discrete communications within the MCT that do not contain the selector*" (See Privacy and Civil Liberties Oversight Board, Report on the Surveillance program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance, 2 July 2014, pp. 7). In April 2017, the NSA declared that it has decided that its Section 702 foreign intelligence surveillance activities will no longer include any upstream internet communications that are solely "about" a foreign intelligence target. See official press release of the NSA: https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/).
85. Exec. Order ("EO") No. 12333, 46 Fed. Reg. 59,941 (December 4, 1981).
86. M.M. JAYCOX, "No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333", *Harvard National Security Journal*, vol. 12:1 (Forthcoming 2020), p. 3.
87. Nat'l Sec. Agency, Legal Fact Sheet: Executive Order 12333 (19 June 2013), available at: https://www.aclu.org/files/assets/eo12333/NSA/Legal%20Fact%20Sheet%20Executive%20Order%2012333.pdf.

practice to collect data of US persons).[88] The policy regime created by EO 12333 is described by authors as immense, complex and opaque since most of it is classified. Much of the information is therefore difficult to decipher.[89]

EO 12333 is structured as follows:
- Section 1 provides a general introduction in order to understand core concepts of signals intelligence and explain the roles of the individual components of the Intelligence Community.[90]
- Section 2 governs the conduct of intelligence activities, defines the scope of the intelligence and provides for certain restrictions[91] on the intelligence components. It also defines in general terms the information that intelligence agencies may collect, retain and share.[92]
- Section 3 defines key terms.

Since FISA only regulates a subset of NSA's signals intelligence activities, NSA conducts the majority of its signals intelligence (SIGINT) activities solely pursuant to the authority provided by Executive Order (EO) 12333.[93]

The permissive targeting standards are intended to target non-US persons outside the US for foreign intelligence information purposes.[94] It is sometimes argued that "*permissive targeting standards allow for EO 12333 surveillance across the entire spectrum of bulk acquisitions*" and different techniques of surveillance exist: "*One type of EO 12333 surveillance analyzes all phone calls and metadata exiting a country. A second type includes surveillance similar to Section 702's upstream collection techniques. A third type, called XKEYSCORE, collects information from multiple authorities, including EO 12333, and is a 'front end search engine' akin to a search engine for intelligence analysts; however, it can also send commands to servers connected to the telecommunications backbone to prioritize, analyze, and store information into NSA databases as certain data transits the global telecommunications backbone*".[95]

Part II – International data transfers after Schrems II

Although their revision was already pending, the SCCs have been reviewed notably in the light of the *Schrems II* decision. The decision also introduced the obligation to implement "supplementary measures" where the level of protection in the third country is not "essentially equivalent". These notions deserved clarifications, which were provided by the EDPB in several recommendations.

This second part of the paper explains the structure and functioning of the new SCCs (1) and reviews the different types of supplementary measures (2), having in mind the EDPB's recommendations. However, the required assessment to be performed prior to any transfer is quite complex in practice. We will therefore also address the first emerging tools designed to help data importers and data exporters to carry out the transfer impact assessment (3).

1. The new standard contractual clauses (SCCs)

1.1. New structure and … new issues

31. After the release of a first draft for public consultation, the European Commission adopted the final version of the new standard contractual clauses on 4 June 2021.[96]

32. The new SCCs are structured following a modular approach taking into account different transfer scenarios depending on the respective roles of the importer and exporter in the relevant transfer. There are four possible data transfer scenarios: (i) controller-to-controller transfer (C2C), (ii) controller-to-processor transfer (C2P), (iii) processor-to-processor transfer (P2P), and (iv) processor-to-controller transfer (P2C).

SCCs can be included in a wider contract provided that other clauses of the contract do not contradict the provisions of the SCCs.[97]

88. *Ibidem,* p. 42.
89. *Ibidem*, p. 4.
90. As a reminder, the IC includes seventeen different agencies (including notably NSA, CIA and FBI). See members of the IC: https://www.dni.gov/index.php/what-we-do/members-of-the-ic.
91. Such restrictions mainly concern the collection of information related to US citizens or people present on the US soil. In that sense, see notably EO 12333, at § 2.3 (*e.g.* collection, retention, and dissemination of certain information concerning US persons is authorized only pursuant to attorney general-approved procedures), § 2.4 (*e.g.* agencies of the IC shall use the least intrusive collection techniques feasible for collection within the US or directed against US persons abroad) and § 2.5 (*e.g.* the attorney general has the power to approve surveillance within the US or against a US person abroad using any technique for which a warrant would be required if it was undertaken by law enforcement).
92. EO 12333, § 2.3.
93. Nat'l Sec. Agency, Legal Fact Sheet: Executive Order 12333 (19 June 2013). See also EO 12333, § 3.5(h).
94. M.M. JAYCOX, "No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333", *op. cit.*, p. 69.
95. For further details on the different types of surveillance, please refer to M. JAYCOX, "No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333", *op. cit.*, pp. 42-70.
96. Commission implementing decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021D0914&from=FR.
97. Commission implementing decision (EU) 2021/914 of 4 June 2021, *op. cit.*, Recital 3.

Data subjects must be informed about the use of SCCs and how to obtain a copy/where they are made available (transparency principle).

SCCs enable multiparty schemes: it is indeed possible to encompass more than two contracting parties, and after signing, the SCCs do not prevent additional parties to adhere to pre-existing agreements based on the SCCs.

33. Regarding the application of the SCCs, a transitional regime is organised. First, the new SCCs entered into force on 21 June 2021. The former SCCs have been repealed as of 27 September 2021 and therefore can no longer be signed for new agreements. In addition, currently in force agreements previously signed on the basis of the previous version of the SCCs must be replaced by new agreements based on the new SCCs by 27 December 2022.

1.2. Are the new SCCs sufficient after *Schrems* II?

34. The transfer of data to a third country must be based on an appropriate data transfer mechanism amongst those listed in Chapter V of the GDPR, such as SCCs.
However, the data exporter shall first, following the EDPB's six steps roadmap (see below), assess whether the third country's laws and practices provide an essentially equivalent level of protection of personal data compared with the level of protection granted in the EU.

The data exporter can therefore transfer personal data on the basis of SCCs only insofar as this prior assessment is positive, taking into account the circumstances of the planned transfer, and the supplementary measures which could be implemented (if need be).

35. The new SCCs do not include all the contractual measures suggested by the EDPB. Moreover, contractual requirements alone may be weak to guarantee the transferred data a level of protection essentially equivalent to that guaranteed within the EU by the GDPR. Indeed, foreign surveillance laws will probably supersede contractual provisions imposing specific obligations to the data importer. For instance, surveillance programmes based on Section 702 of the FISA are secret and the US data importers are subject to a secrecy obligation regarding the acquisition requested by the US government, which prohibits the sending of a notification to their customers (*i.e.* the data exporters). However, data protection practitioners try to design a circumvention mechanism which can contribute to improve the effectiveness of the protection of the personal data processed in the USA. The warrant canary clause is a good illustration of contractual tools which can contribute to the protection of personal data. The warrant canary clause provides for that the data exporter has the duty to issue, on a regular basis, an information notice confirming it did not receive any government or court order to disclose data of its client. Without infringing the prohibition to disclose to its clients such an order, the lack of such a notice will implicitly confirm to the data exporter that the data importer has been subject to such an order and therefore that its personal data may be accessed by the third country government.

However, the implementation of technical measures (such as strong encryption) appears to be a more effective instrument to improve the effectiveness of the protection of the transferred personal data in such a case. Nevertheless, such a finding is problematic since it is sometimes necessary for the importer to access the data in the clear (*e.g.* to be able to provide the services requested by the exporter). The direct consequence could therefore be that in some cases the transfer of data to a country that does not provide for an equivalent level of protection would become "legally" impossible.

2. The EDPB recommendations on supplementary measures

38. Following the *Schrems II* judgement, the EDPB issued a set of recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data[98] and Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.[99]

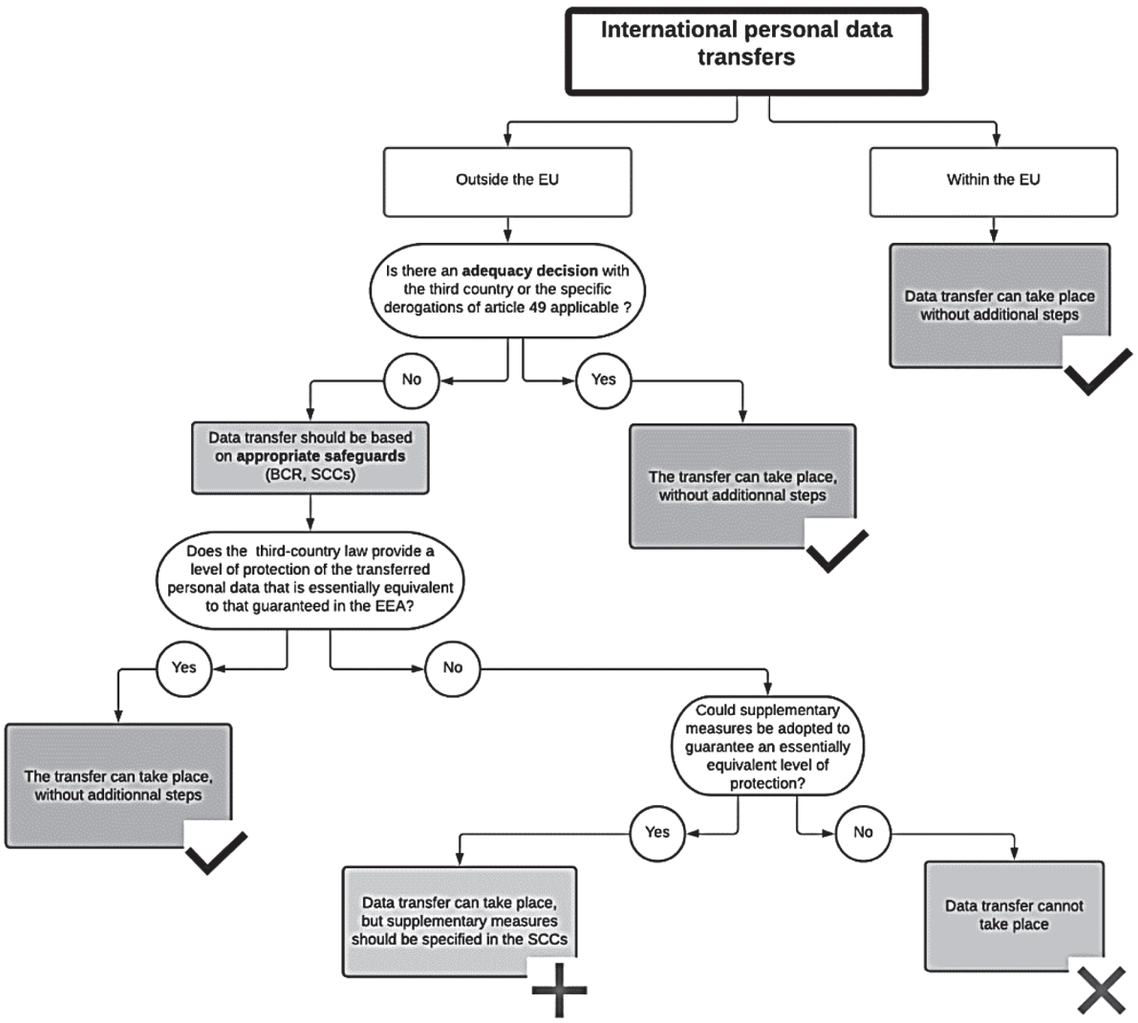
2.1. Recommendations on supplementary measures

2.1.1. Six-steps roadmap

39. The EDPB Recommendations provide a six-step roadmap to help data exporters with the complex task of assessing data transfers to third countries (*i.e.* non-EU countries) and identifying appropriate supplementary measures where needed.

98. See *infra*, point 3.1.
99. See *infra*, point 3.2.

The following decision tree summarises the EDPB roadmap:



EDPB six-steps roadmap could be summarised as follows:

40. Step 1 – Know your data transfers – The organization must identify and map all personal data transfers to third countries (including any onward transfers) and ensure such transfers comply with the GDPR principle of data minimisation.[100] Practically, the idea is to have a full picture of the data flows.

41. Step 2 – Identify the transfer tools you are relying on – The organization must identify the appropriate data transfer mechanism to rely on, amongst those listed in Chapter V of the GDPR (*i.e.* adequacy decision, appropriate safeguards, such as SCCs, BCRs, codes of conduct, etc., or specific derogations).

If the transfer is based on an adequacy decision or meets the strict conditions for a derogation, no further requirements are needed.

If the data transfer is based on appropriate safeguards, continue to step 3.

42. Step 3 – Assess the effectiveness of the article 46 GDPR transfer tool you are relying on the context of your specific data transfer – The organization must assess (with the support of the importer where appropriate) whether the laws or practices of the third country may prevent the personal data transferred from being afforded an essentially equivalent level of protection as under the GDPR.

Particular attention should be paid to local legal requirements to disclose personal data to public

100. As explained *supra* in point 1.1. (Part II), remote access from a third country (*e.g.* for support services) and/or use of cloud-based solutions located outside the EEA are also considered to be a transfer.

authorities or granting such public authorities powers to request access to personal data (*e.g.* under US law, not. with Section 702 of FISA and EO 12333).

43. Step 4 – Identify and adopt supplementary measures – If the third country's laws or practices do not provide an essentially equivalent level of protection to the EU (*e.g.* if Section 702 of FISA and/or EO 12333 applies, for EU-US transfers), the organization must identify and adopt effective supplementary measures (to the safeguards already provided for by article 46) in order to ensure an appropriate level of protection.

Annex 2 of the EDPB Recommendations 01/2020 provides for a non-exhaustive list of technical (*e.g.* pseudonymization or encryption), contractual (*e.g.* transparency obligations) and organizational (*e.g.* internal policies) supplementary measures. It also provides for scenarios for which effective measures could be found, or not.

If no appropriate supplementary measure can be adopted, the organization must avoid, suspend or terminate the data transfer.

44. Step 5 – Procedural steps if you have identified effective supplementary measures – The organization must take the necessary procedural steps for the implementation of the identified supplementary measures. Specific consultation with the relevant data protection supervisory authority may be required depending on the appropriate safeguards the organization is relying on.

45. Step 6 – Re-evaluate at appropriate intervals – Last but not least, the organization must periodically re-evaluate whether the protection granted to transferred personal data has changed due to the adoption of new legislation in the third country. The EDPB does not give a precise indication about the frequency of reassessment.

2.1.2. Supplementary measures

46. The obligation to adopt supplementary measures has been formulated by the CJEU in the *Schrems II* case. Previously, standard contractual clauses were signed by the parties as a kind of "formality", like general terms and conditions. However, the Court reminded us that such clauses are not binding for the public authorities of third countries. For this reason, data exporters may need to implement supplementary measures, to secure the efficiency of the SCCs, as mentioned in article 109 of the GDPR.[101]

Unfortunately, neither the Court, nor the GDPR itself are very specific about the nature of the possible supplementary measures. Therefore, the EDPB has decided to issue guidelines to help data exporters. In particular, the Recommendations 01/2020 provide for a "*methodology for the exporters to determine whether and which additional measures would need to be put in place for their transfers*".[102]

Regarding the supplementary measures which should be adopted, it is important to note that there is no "one-size-fits-all solution". While some supplementary measures may be effective in some countries or for certain types of processing activities, the same measures might be ineffective in other countries or for other processing activities. In addition, depending on the practical elements of the relevant processing activities, it may be interesting/necessary to combine several supplementary measures to reach the required standard of essential equivalence to the EU level of protection.

The assessment of the effectiveness of the supplementary measures is to be performed by the data exporter and has to take into account the context of the transfer, the third country law and practices and the chosen transfer tool.

47. To determine the type of adequate supplementary measures, the following factors should be considered[103]:

- format of the data to be transferred (*i.e.* in plain text/pseudonymized or encrypted);
- nature of the data (*e.g.* sensitive data as covered by articles 9 and 10 of the GDPR);
- length and complexity of data processing workflow, number of actors involved in the processing, and the relationship between them;
- technique or parameters of practical application of the third country law;
- possibility that the data may be subject to onwards transfers, within the same country or even to other third countries (*e.g.* involvement of sub-processors of the data importer).

In practice contractual and organizational measures alone may not be able to provide sufficient protection, while technical measures (can) do. However, contractual and organizational measures may supplement the technical measures and strengthen the overall level of protection of data. To find the right balance between the possible measures is a challenge for data exporters.

101. See also CJEU, Case C-311/18, *Schrems II*, §§ 132-133.
102. EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 18 June 2021, available at: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en, p. 8.
103. EDPB, Recommendations 01/2020, *op. cit.*, p. 22.

This assessment of supplementary measures must be carried out with due diligence and must be documented, to comply with the accountability principle (articles 5.2 and 28.3 (h) of the GDPR).

If no appropriate supplementary measure can be adopted, the data transfer must be avoided in order not to compromise the level of protection of personal data as guaranteed within the EU by the GDPR. If the transfer is already conducted, it must be suspended or terminated.[104]

2.1.3. Contractual measures

48. Contractual measures mostly consist in unilateral, bilateral or multilateral contractual commitments of a private nature. If standard contractual clauses already contain mechanisms making it possible, in practice, to ensure compliance with the adequate level of protection, public authorities may override them. Additional contractual measures may be helpful to consolidate the supplementary organizational and technical measures implemented to prevent the public authorities to interfere.

49. EDPB gives a few examples of contractual measures that could be adopted. They can be classified into the following four categories:

– **Providing for the contractual obligation to use specific technical measures**. The technical measures that would be identified as necessary by the exporter would be described in the contract.

– **Transparency obligations**. Different provisions can be introduced to ensure the importer is transparent towards the exporter. For instance, specific annexes could be added to the contract, giving some information about the access by public authorities to personal data (*e.g.* enumeration of the laws and regulations of the third country that could permit it or, in the absence of such laws and regulation, information and statistics based on the importer's experience or reports from various sources; indication of the measures taken to prevent the access to transferred data; a complete report on all requests of access to personal data formulated by public authorities). This transparency would help both the exporter, with its obligation to document its assessment of the level of protection, and the importer, with its obligation to assist the exporter.
  The EDPB also provides for the possibility for the exporter to insert 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"*.[105] But of course, third-country law or practices could prevent the importer to comply with such an obligation. In this case, the importer should notify the exporter of this obstacle.
  Contractual commitments could also provide the possibility for the exporter to conduct audits or inspections of the data processing facilities of the importer.[106] To be effective, access logs and other similar trails should be tamper-proof so that the inspectors/auditors could find out evidence of disclosure.
  There could also be an obligation for the importer to notify the exporter if it can no longer comply with its contractual obligations and cannot guarantee an adequate level of protection anymore. This notification should take place before the access is granted to the data, and quick mechanisms should be implemented to guarantee the level of protection (*i.e.*, promptly secure the data or return it to the exporter).
  Finally, the so-called "warrant canary" clauses could be adopted by the parties. This guarantee obliges the importer to regularly publish a cryptographically signed message informing the exporter that as of a certain date and time it did not receive any order to disclose personal data to the local public authorities. The exporter automatically monitors this notification. The encryption key for signing the warrant canary must be kept safe. The lack of such notification implicitly reveals the receipt of a disclosure order by the data importer, without infringing a possible prohibition to (positively) inform the data exporter as it may exist under the third country law.

– **Obligations to take specific actions**. The exporter could impose the importer to review and challenge the legality of any order addressed to it by public authorities, provided that third country law offers effective legal possibilities to challenge such orders.

– **Empowering data subjects to exercise their rights**. Another means to reinforce the conditions of transfer is to empower the data subject in the exercise of his rights. For instance, the *"contract could provide that personal data transmitted in plain text in the normal course of business may only be*

104. CJEU, Case C-311/18, *Schrems II*, § 135.
105. EDPB, Recommendations 01/2020, *op. cit.*, p. 38.
106. On-site and/or remotely.

accessed with the express or implied agreement of the exporter and/or the data subject for a specific access to data".[107] The effectiveness of this measure is limited to cases where consent can be validly given. In addition, in some cases, access to the data would not be known to the importer, so this measure will not be effective either.

The contract could also provide the prompt notification of the data subject in case of request or order received from the public authorities of the third country or if the importer is not able to comply with contractual commitments anymore. However, national regulations and policies may prohibit this notification to the data subject.

In addition, parties could insert clauses that 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.

2.1.4. Organizational measures

50. Organizational measures may be needed to complete technical and contractual measures, in order to meet the EU standards of data protection. Again, the choice of the measure will depend on the specific circumstances of the transfer. Below, we provide a list of the different types of organizational measures listed by the EDPB:

– **Internal policies for governance of transfers especially with groups of enterprises**. They could include, among others:
- the appointment of a specific team, which should be based within the EEA, composed by experts on IT, data protection and privacy laws, to deal with requests that involve personal data transferred from the EU;
- the notification to the senior legal and corporate management and to the data exporter upon receipt of such requests;
- the procedural steps to challenge disproportionate or unlawful requests and the provision of transparent information to data subjects.

– **Transparency and accountability measures**. The following transparency and accountability documents could be held by the parties:
- records of the requests for access received from public authorities and the response provided, alongside the legal reasoning and the actors involved. These records should be made available to the data exporter, who should in turn provide them to the data subjects concerned where required;
- regularly, transparency reports or summaries regarding governmental requests for access to data and the kind of reply provided, insofar publication is allowed by local law.

– **Organization methods and data minimization measures**. Such as the adoption of strict and granular data access and confidentiality policies and best practices, based on a strict "need-to-know" principle. Also, unnecessary personal data should not be transferred (a preliminary sorting of the data or a separation of the accessible data, in case of remote access, should be carried out). This could be monitored with regular audits and enforced through disciplinary measures.

– **Adoption of standards and best practices**. Strict data security and data privacy policies should be adopted, based on EU certification or codes of conducts or on international standards (*e.g.* ISO norms) and best practices (*e.g.* ENISA), having regard to the state of the art, in accordance with the risk of the categories of data processed.

2.1.5. Technical measures

51. The recommendations of the EDPB develop, in more details, the different technical measures that can be considered. Through different use cases, the measures and their conditions of effectiveness are scrutinised. But, once again, the efficiency of each technical measure has to be assessed on a case-by-case basis. If the circumstances of the transfer differ from the use case described by the EDPB, the results of the effectiveness analysis could lead to different conclusions.

Since technical measures are always necessary in case of a non-equivalent level of protection, we reproduce below, in details, a table containing the technical measures foreseen by the EDPB.

The table below lists the measures that the EDPB calls "technical" in its recommendations 01/2020. However, in our opinion, "technical" measures *sensu stricto* should not include, for instance, professional secrecy or the division of data among several providers.[108]

107. EDPB, Recommendations 01/2020, *op. cit.*, p. 42.
108. We would rather qualify them as "organizational" measures.

Measure:	*For example:*	*Effective, as long as:*
Encryption	– Storage of data (*e.g.* backup) in the third country where the data is not accessible in clear text.	– *Strong encryption* is used taking into account (1) the state-of-the-art, (2) resources available to foreign authorities, (3) the period of time during which confidentiality must be preserved; – *it is before* transmission; – *the encryption is well implemented* (certified and properly maintained software); – *keys are reliably managed inside EU*, EEA or in a country which has been the subject of an adequacy decision; – *measures* are taken against attacks, vulnerabilities and backdoors.
	– Encryption to protect data from access by public authorities in the receiving country during transit.	– Exporter and importer *agree* on an *encryption key;* – specific protective and state-of-the-art *measures* are taken against active and passive attacks, vulnerabilities and backdoors; – *transport encryption and possibly also end-to-end encryption of the personal data* on the application layer; – – the encryption keys are entrusted to the exporter established in a country offering an equivalent level of protection.
Pseudonymization	– The importer pseudonymizes the data before sending it to the third country (*e.g.* data used in research).	– A thorough analysis of the data in question demonstrates that it *cannot be cross-referenced* with any information that the public authorities of the recipient country may possess to be attributed to an identified or identifiable natural person; – … and that *additional information needed to reidentify* data are: • *kept separately;* • *inside EU*, EEA or in a country which has been the subject of an adequacy decision; • *by the data exporter;* • *protected* by appropriate technical and organizational safeguards.
Protected recipient (*e.g.* professional secrecy)	– The data importer in the third country is specially protected by the laws of his country against disclosure of the data he holds.	– The law of the third country *specifically exempts* that recipient from providing access to data in its possession; – includes *all* data in its possession; – the recipient *does not transmit* the data to another entity that does not have the same protection; – the data is *encrypted before* it is sent and only the person holding the confidentiality agreement has the decryption key.

Measure:	*For example:*	*Effective, as long as:*
Division of data	– Processing of data involving several actors: the data exporters wish 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.	– Each actor is given a portion of the data that does not allow them to identify the person to whom their data relates; – the exporter then receives the result obtained by each entity after it has done its processing to return the final result/aggregate data.

Finally, from a general point of view, a review of all the supplementary measures put in place should be held regularly by the contractors, in order to verify the level of protection is still guaranteed.

2.1.6. Assessment of the effectiveness of the measures

52. In our description of the measures that the EDPB advocates, we have briefly specified the conditions for the effectiveness of each measure.

53. The EDPB's recommendations also identify scenarios in which effective measures are not identified:
– transfer to cloud services providers or other processors which require access to data in the clear. *E.g.* provision of technical support or any type of cloud processing;
– transfer of personal data for business purposes including by way of remote access. *E.g.* SharePoint, shared services inside a group of enterprises, …

54. Ultimately, it will be up to the courts to assess the effectiveness of the measures put in place to secure the transfer. Surprisingly, the Belgian Council of State was the first to decide on the topic.

The Flemish Region of Belgium had awarded a public procurement to a company, which was a subsidiary of a US entity, for the implementation of a new platform aimed at facilitating the mobility of disabled people. As this platform was to process a certain amount of personal data (some of which being special categories of data), the contract specifications provided for certain reinforced obligations in terms of compliance with the GDPR. In view of the *Schrems II* ruling, in order to verify the tenderers' ability to comply with the provisions of the GDPR, the contracting authority also required to fulfil a questionnaire relating to the data transfers and to attach it to the tender.

The award decision was appealed to the Council of State. The competitors of the selected company argued that no additional measures could be taken to remedy the inadequate level of data protection in the United States. In this case, however, a data transfer was still possible.

In a first decision[109], the Council of State decided to suspend the award of the contract in question, on the grounds that the decision taken by the contracting authority did not allow for a real examination of the compliance of the tender with the provisions of the GDPR and the contract documents.

The contracting authority then withdrew the initial award decision and took a new award decision ... to the same tenderer. A cancellation action was then lodged, alleging a violation of articles 28, 44 and 45 to 50 of the GDPR since the successful tenderer mentioned in its tender the possibility of transferring the data to the United States.

During this new examination of the legality of the tenders submitted[110], the Council of State noted this time the particular care that had been taken to verify the respect of data protection regulation. For that purpose, the contracting authority asked the data protection officer of the Mobility and Public Works Department to carefully examine the tenders. The DPO confirmed that the tender complied with the requirements of the contract documents, although a transfer of data to the United States was still possible.

The State Council recalled that a transfer of data to the United States was still permitted, even after the *Schrems II* ruling, provided that additional measures were adopted. Unfortunately, the Council did not include in its decision the specific measures adopted by the successful tenderer. However, it suggests that the measures called for by EDPB recommendation 01/2020 are implemented:
"Petitioners' assertion that no additional measures are conceivable that would remedy the inadequate level of data protection in the United States, even through encryption or pseudonymization, appears to misunderstand, in a general way, how such measures could be implemented. From the file, it appears that neither the VTC [for 'Vlaamse toezichtcommissie voor de verwerking van persoonsgegevens', i.e. 'Flemish Commission for the Supervision of the Processing

109. Belgian Council of State, 12 May 2021, no. 250.599.
110. Belgian Council of State, 19 August 2021, no. 251.378.

of Personal Data'] nor the European Data Protection Board object to full encryption of the data before it is handed over to the service provider, with the encryption keys being kept entirely under the control of the Flemish appeal body. The file shows that the selected tenderer offers a complete set of guarantees".[111]

With this decision, the Belgian Council of State has therefore implemented the *Schrems II* case law at the Belgian level and also relied on the EDPB's recommendation. For the sake of clarity, it is however unfortune the Council did not elaborate on the exact measures implemented by the successful tenderer. It is therefore difficult to fully benefit the Council ruling for other similar Belgian cases.

3. Transfer impact assessment (TIA)

55. We will now focus on the assessment process itself, i.e. how a company or organization – as a data controller – should perform such an assessment in practice.

3.1. EDPB European Essential Guarantees Recommendations

56. The EDPB Recommendations[112] update the European Essential Guarantees (EEGs) drafted by the article 29 Working Party in response to the *Schrems I* judgment. Their aim is to provide further guidance for the required assessment of the possible interference of the third country laws and practices on the level of protection of transferred personal data. It provides elements to determine if this interference can be regarded as justifiable or not. Recommendations "*do not aim on their own at defining all the elements that might be necessary to consider when assessing whether the legal regime of a third country prevents the data exporter and data importer from ensuring appropriate safeguards in accordance with Article 46 of the GDPR*". They provide the essential guarantees that should be found in the third-country law and practices, which is a key part of the assessment.

57. Within the framework of this interference assessment, four EEGs should be addressed: (i) processing should be based on clear, precise and accessible rules, (ii) necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated, (iii) an independent oversight mechanism should exist and (iv) effective remedies need to be available to the individual.

3.2. EDPB recommendations on supplementary measures

58. When conducting the assessment of the third-country national law and "practices", the importer should provide the exporter with the relevant sources and information relating to the third country where it is established. The EDPB lists several sources of information, by order of preference[113]:

- case-law of the Court of Justice of the European Union (CJEU) and of the European Court of Human Rights (ECtHR) as referred to in the European Essential Guarantees recommendations;
- adequacy decisions in the country of destination if the transfer relies on a different legal basis;
- resolutions and reports from intergovernmental organizations, such as the Council of Europe, other regional bodies, and UN bodies and agencies (e.g. UN Human Rights Council, Human Rights Committee);
- reports and analysis from competent regulatory networks, such as the Global Privacy Assembly (GPA);
- 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);
- reports from private providers of business intelligence on financial, regulatory and reputational risks for companies;
- warrant canaries of the importer itself[114];
- 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

111. Paragraph 16 of the aforementioned Belgian Council of State decision of 19 August 2021 (free translation).
112. EDPB, Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10 November 2020, available at: https://edpb.europa.eu/sites/default/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf.
113. EDPB, Recommendations 01/2020, *op. cit.*, p. 47-48.
114. The reference to the warrant canary clauses as a tool to assess the level of interference on data protection could be viewed as an implicit recognition of the efficiency of this tool as a "supplementary measure" to improve the level of protection of the transferred personal data.

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;
– 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.

59. By listing all of these sources, the EDPB attempts to clarify what is meant by "practices." By not considering only case law or official reports in the list, the EDPB perhaps leaves a door open to some "self-regulation" of the sectors.

60. The proposal is interesting and could be carried by the actors of certain sectors. But this would require a pooling of resources and knowledge by the different actors of the sector concerned. And a significant degree of cooperation...

Moreover, it is difficult to assess the level of seriousness to be given to some of the sources quoted at the very bottom of the list... How important would a supervisory authority consider them?

3.3. Practical recommendations

61. The Transfer Impact Assessment (TIA) aims to identify and describe the risks associated with data transfers to third countries, as well as any supplementary measures to be taken.

Such TIA is based on the regulatory concept of the "risk-based approach" according to which data protection obligations are adapted to the concrete risk situation for the rights and freedoms of the data subject.

62. The International Association of Privacy Professionals (IAPP) published Transfer Impact Assessment Templates as resource to assist privacy professionals in conducting TIAs.[115]

In brief, the IAPP recommends different steps to conduct a TIA, *i.e.*:
– Describe the intended transfer, *e.g.* identity and country of the data exporter/data importer, context and purpose of the transfer, categories of data subjects concerned, categories of personal data transferred, sensitive personal data, technical implementation of the transfer, technical and organizational measures in place, relevant onward transfer(s) of personal data (if any) and countries of recipients of relevant onward transfer(s).
– Define the TIA parameters, *e.g.* starting date of the transfer, assessment period in years, determining the acceptable residual risk of foreign lawful access, target jurisdiction for which the TIA is made and the relevant local laws taken into consideration.
– Define the safeguards in place. Different questions need to be asked, such as: Would it be feasible, from a practical, technical and economical point of view, for the data exporter to transfer the personal data in question to a location in a whitelisted country instead? Is the personal data at issue transmitted to the target jurisdiction in clear?
– Assess the risk of prohibited lawful access in the target legislation, *i.e.* despite the safeguards put in place, does foreign lawful access remain (at least) technically possible? The EDPB published a non-exhaustive list of sources of information to help the data exporter (and the data importer where relevant) to identify the relevant sources and information relating to the third country as well as the laws and practices applicable in the third country.
– Conclude that in view of the above-mentioned elements and the application data protection laws, the transfer is to be considered permitted or prohibited.

63. From the supervisory authorities' side, the UK Information Commissioner's Office (ICO) has published an "International transfer risk assessment tool"[116] in order to help organizations transferring data outside the UK to comply with the law and continue to enable data flows.[117] In this guidance, ICO proposes its own UK-specific standard contractual clauses for restricted transfers (the so-called "IDTA"). But the ICO also proposes an International Transfer Risk Assessment (TRA) Tool. It enables organizations to ensure that the article 46 transfer tool provides appropriate safeguards in the particular circumstances of the restricted transfer.

ICO's TRA lists some of the factors which impact the extent to which the legal regime in the destination country provides enforceable rights and effective legal remedies for the exporter and for data subjects[118]:
– The country recognises the rule of law (*i.e.* there is an established and respected legal and court system).
– You can enforce foreign judgments or arbitration awards.
– The jurisdiction is party to a convention for recognition of enforcement of foreign judgments or

115. Available here: https://iapp.org/resources/article/transfer-impact-assessment-templates/.
116. ICO, Draft International Transfer Risk Assessment and Tool, August 2021, available at: https://ico.org.uk/media/about-the-ico/consultations/2620397/intl-transfer-risk-assessment-tool-20210804.pdf.
117. ICO, Draft International Transfer Risk Assessment and Tool, *op. cit.*, p. 4.
118. ICO, Draft International Transfer Risk Assessment and Tool, *op. cit.*, p. 17.

arbitration awards (namely, if you consider the key conventions: the Brussels Convention or the Hague Choice of Court Convention.
– There is ready access to justice through the court system which provides a means for redress and effective remedies.
– The rights of third-party beneficiaries under contracts are recognised and enforced.
– There are high levels of integrity and independence in the judicial process.
– There are partial adequacy regulations in relation to the country (which do not cover your transfer).

If the above criteria are not met (*e.g.* foreign judgments are not recognised, there is a limited access to justice, the destination country is not bound by international conventions for recognition of enforcement of foreign judgments, etc.), it clearly indicates areas of concern about enforceable rights and effective legal remedies.

64. If there are concerns over the enforceability of the IDTA, the ICO proposes to assess the overall risks to data subjects arising from the specific circumstances of the transfer (*i.e.* evaluate the level of risk of harm to data subjects). This assessment shall notably consider:
– The categories of personal data, (*e.g.* in the context of staff's personal data):

Low risk	*Moderate risk*	*High risk*
Basic employment contact details	Non-sensitive employment records (CV, payroll history)	Sickness or absence records, health information, monitoring data, sensitive information (*e.g.* banking details, passwords)

– The circumstances of the transfer (indeed, some factors may reduce or increase the risk of harm to data subjects), *e.g.*

Reducing the risk	*Increasing the risk*
– Data already in public domain – The data subject has expressly confirmed that he has been informed of the potential risks of the transfer and has no concerns in relation to the same, and this has been documented	– Data subjects are children or vulnerable adults – Risk of harm to additional individuals other than the data subjects (*e.g.* family members) – A large volume of data relating to an individual is transferred

– The circumstances which may decrease the risk of the importer ignoring a UK court order or UK arbitration award (and thus, causing no harm to data subjects):
• Importer and exporter are within the same group of companies.
• Importer is bound by professional codes of conduct (*e.g.* solicitors).
• Importer is bound by regulatory obligations (*e.g.* financial services sector).
• Importer is a reputable global company (*e.g.* an international bank or major cloud hosting service).
• Importer has signed up to an EU-approved code of conduct.
• Importer has a certification under an EU-approved scheme.

65. Once the potential risks have been identified, extra steps and protections to safeguard the data and reduce the risk should be considered. The ICO gives a non-exhaustive list of typical extra steps and protections and guidance on the effectiveness of each type of measure:

Type of measure:	*Basic*	*Enhanced*	*Significant*
Access controls	Protecting personal data by applying a password (which is transferred separately to the importer, if it must process the data beyond storing it)	Personal data are encrypted before the transfer (using storing encryption/encryption at-rest) and suitable key management procedures are implemented	Personal data are encrypted before the transfer, using appropriate encryption solution, and the encrypted datasets are split between multiple parties
Changes to the data	After reviewing the purposes of the transfer, the amount of personal data transferred is minimized	Pseudonymization techniques are applied prior to the transfer and the importer does not have access to the additional information	Pseudonymized datasets are split between multiple entities (Anonymization techniques should also be considered)
Contractual	Implementing an enhanced data subject complaints process, including compensation scheme	If exporter's financial resources are sufficient, implementing a contractual right for data subject to bring a claim against the exporter if the importer fails to comply with the EU laws	Commitments to maintain:- – Professional or regulatory status – ICO code of conduct – ICO certification

66. If, after having assessed the enforceability of contractual safeguards in the destination country and the overall risks to data subjects, the level of risk is considered "high", and no supplementary measure can help, ICO considers that the organization concerned should not continue using the TRA tool for the risk assessment. Instead, a more detailed risk assessment should be performed or specific exceptions should be envisaged.

67. If there is no risk or the risk is low, the next step is to determine if there is appropriate protection for the data from third-party access. We reproduce hereunder the ICO's decision tree[119]:

<table>
<tr><th colspan="6">Decision tree</th></tr>
<tr><td colspan="6">Is the destination country's regime similar enough to the UK's regime in terms of regulating third party access to data (including surveillance)?</td></tr>
<tr><td>Yes
↓</td><td colspan="2">Don't know
↓
Assume serious concerns</td><td colspan="3">No
↓</td></tr>
<tr><td>Make the transfer</td><td colspan="5">How likely is third party access to the data (including surveillance)?</td></tr>
<tr><td></td><td>Minimal risk
↓
Make the transfer</td><td colspan="2">Don't know
↓
Assume more than a minimal risk
↓</td><td colspan="2">More than a minimal risk
↓</td></tr>
<tr><td></td><td colspan="4">Considering the circumstances of the transfer and the destination country's regime, what is the risk of harm to data subjects?</td></tr>
<tr><td></td><td colspan="2">Low risk
↓
Make the transfer</td><td colspan="3">Enhanced risk
↓</td></tr>
<tr><td></td><td colspan="2"></td><td colspan="3">Are you able to take extra steps and protections to reduce the risk of harm to low risk?</td></tr>
<tr><td></td><td colspan="2"></td><td>Yes
↓
Make the transfer</td><td colspan="2">No
↓
TRA tool not suitable</td></tr>
</table>

The ICO seems flexible (and pragmatic!) in its expectations regarding the assessment of the law of the country of destination when it says: "*We recognise that this is a complicated exercise for organisations, particularly for those with limited resources; we don't expect you to become experts in international surveillance regimes*".[120] We hope the supervisory

119. Obviously, this decision tree does not give a "ready-made answer" but helps to structure the reflection.
120. ICO, Draft International Transfer Risk Assessment and Tool, *op. cit.*, p. 30.

authorities within the EU countries will similarly remain reasonable in their expectations.

3.4. Major challenges

68. The assessment of the laws and practices of third countries relating to data protection raises at least two major challenges for the European organizations and companies transferring personal data.

69. The assessment – As explained, there are many circumstances and elements that can (or must) be taken into account in the assessment. The first difficulty is therefore to identify the relevant factors to consider in light of the processing activities.

In addition, the assessment requires knowledge and resources, while many organizations may not have dedicated privacy staff and are supposed to become experts in data protection laws across the world.

The icing on the cake is that the required assessment takes time. For example, the European Commission itself is taking months to review the regulatory regime in the countries for which it grants an adequacy decision, and the European Commission can rely on expert staff and external specialists.

70. The supplementary measures – The identification of the appropriate supplementary measures to restore an equivalent level of protection is another challenge which requires expertise and resources.

The EDPBs recommmendations are providing some guidance, but remain very generic, while the requirement is to justify the appropriateness of the implemented measures in light of the circumstances of the relevant data processing activities. In addition, even based on reasonably justified advices, the choice of supplementary measures will remain subject to the supervisory authority's final validation. The only efficient means to mitigate such a risk would be that the EDPB and/or the European Commission publishes a detailed list of measures based on various data transfer scenarios, in order to provide a broad "best practices" implementation tool to the business operators.

4. Conclusion

71. The *Schrems II* case imposes heavy duties on EU entities transferring personal data outside of the EU.

In the present paper, we tried to summarise the essence of these requirements and provide some insight into the available practical tools or tips to support the required assessment process.

72. More fundamentally, from a purely pragmatic point of view, it is questionable whether it is realistic for all companies to conduct a TIA for each international data transfer.

Indeed, the core business of most of the companies is not to make money from personal data. It therefore appears unreasonable to require from companies and organisations to perform their own assessment of the laws and practices applicable in third countries while the European Commission and EDPB are not able to provide such assessment to support a consistent and harmonized regime for international transfers of personal data.[121]

73. The lack of a kind of official detailed assessment database following the *Schrems II* judgment raises questions.

Indeed, European companies may be discouraged from using service providers located outside of the EU. Is it the hidden goal of such a duty to assess third countries' law and practices?

For EU institutions related transfers, the European Data Protection Supervisor (EDPS) has rendered an opinion on transfers to a third country resulting from the use of a newsletter service by ENISA. In this opinion, the EDPS clearly encourages ENISA to "*ensure that any new processing operations or new contracts with any service providers does not involve transfers of personal data to the United States*" and states that "*ENISA should primarily assess with the processor the availability of alternative newsletter solutions not involving the transfer of personal data to sub-processors in the US*".[122] The position sounds logical for institutional bodies. The *Schrems II* judgment seems to lead to a similar approach for private companies, which is more subject to discussion.

74. As noted by scholars, "*the CJEU developed and uses as a benchmark 'essential equivalence' both as a standard to achieve but also as a fundamental rights test for destinations of data transfers to pass*".[123]

121. However, it should be noted that the EDPB published, on 8 November 2021, a legal study (prepared by external providers) on Government access to data in third countries. The study notably provides for information on the legislation and practice in China, India, and Russia on their governments' access to personal data processed by economic operators. Such initiatives are welcomed. Final report is available at: https://edpb.europa.eu/system/files/2022-01/legalstudy_on_government_access_0.pdf.
122. EDPS Opinion on transfers to a third country resulting from the use of a newsletter service by ENISA, Case 2020-1122, available at: https://media-exp1.licdn.com/dms/document/C4E1FAQHqA-j5KHMYJA/feedshare-document-pdf-analyzed/0/1634482945248?e=1637002800&v=beta&t=ETw2R_IgH1gIv1204psZmqY0eN5zAZNm-7XjXihQdYQ.
123. See L. DRECHSLER and I. KAMARA, "Essential Equivalence as a Benchmark for International Data Transfers After Schrems II" in *Research Handbook on EU data protection*, *op. cit.*, p. 2.

The benchmark approach could be questioned, especially when the basis for the assessment is not properly defined and the ability of the data exporters to perform such an assessment is highly uncertain. The expected goal is very ambitious, while the support from the authorities in charge of the GDPR implementation[124] is obviously not at the same level. Without a rapid and massive support from said authorities, the challenge imposed on the European organizations and companies does not seem reasonable and will be very difficult to achieve for most of the data exporters.

124. National supervisory authorities, EDPB, European Commission.