EDPS CASE LAW DIGEST:

Transfers of personal data to third countries

EUROPEAN DATA PROTECTION SUPERVISOR

The EU's independent data protection authority

From *Lindqvist* to *Schrems II:* case law of the CJEU on **transfers of personal data to third countries**

edps.europa.eu

1

INTRODUCTION

- **The GDPR regulates** *"any **transfer** of personal data which are undergoing processing **or are intended for processing after transfers** to a third country or to an international organisation"* (Art. 44). These data flows (transfers and onward transfers) are subject to the rules set out in Chapter V of the GDPR, as well as to all rules and principles of the GDPR, notably the principles under Article 5 (lawfulness, fairness, and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability).

- Transfers of personal data must rely **on one of the legal basis for transfers provided by the GDPR under Chapter V** (namely, Article 45, transfers on the basis of an adequacy decision; Article 46, transfers on the basis of appropriate safeguards; Article 49, derogations for specific situations).

- **Since 2003**, when the Lindqvist judgment was issued, the Court of Justice of the European Union (CJEU) clarified the meaning of the provisions relating to transfers of personal data to third countries or international organisations. Initially the CJEU did so having regard to the provisions of the now repealed Directive 95/46 (which in many cases do not substantially differ substantially from the corresponding provisions of the GDPR), later by providing interpretation of the provisions of the GDPR.

- The **overarching principle** of 'the law of transfers' is **the continuity of protection of personal data**, and in so doing **of the protection of fundamental rights and freedoms of the individual**. Being a **fundamental right**, data protection concerns everyone in the Union, and wherever her or his personal data goes, even when data 'travels' to a third country.

  > *"Article 25(6) of Directive 95/46 implements the express obligation laid down in **Article 8(1) of the Charter** to protect personal data and, as the Advocate General has observed in point 139 of his Opinion, is intended to **ensure that the high level of that protection continues where personal data is transferred to a third country.**" (paragraph 72, Schrems)*
  >
  > *"As the Advocate General stated in point 117 of his Opinion, the provisions of Chapter V of the GDPR are intended to ensure **the continuity of that high level of protection where personal data is transferred to a third country**, in accordance with the objective set out in recital 6 thereof. (paragraph 93, Schrems II)*
  >
  > *"That right to the protection of personal data requires, inter alia, that the high level of protection of fundamental rights and freedoms conferred by EU law **continues where personal data is transferred from the European Union to a non-member country.** Even though **the means** intended to ensure such a level of protection **may differ** from those employed within the European Union in order to ensure that the requirements stemming*

from EU law are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union." (paragraph 134, PNR Canada Opinion) in order to ensure protection essentially equivalent to that guaranteed within the European Union." (paragraph 134, PNR Canada Opinion)

The aim of this **case law digest** is to:

- **clarify the structure of the analysis** carried out by the CJEU in judgments concerning the transfer of personal data to third countries, highlighting the logic/steps followed and the jurisprudential acquis in relevant case law (See Part 3 of the Case Law Digest entitled Sources) [link to part 3 sources];

- provide the reader the possibility to explore the **key issues relating to international transfers of personal data**: by selecting one or more "Questions" on page 4, the reader can visualise relevant paragraphs of the judgments of the CJEU relating to this issue in one place (See Part 4 of the Case Law Digest entitled Replies to Questions).

2

QUESTIONS

1. When does a **transfer to a third country** within the meaning of Chapter V of the GDPR (Chapter IV of Directive 95/46) take place? What criteria has the CJEU used to determine the existence of a transfer? What is the overall data protection regime applicable to transfers?

2. What are the **powers available to the national supervisory authorities** in respect of the transfers? In case of: a) Safe Harbor; b) Standard Contractual Clauses (SCC); c) International Agreement.

3. What is meant by an **adequate level of protection**? In case of: a) transfer to a third country; b) in particular, as provided by Safe Harbor (and by Privacy Shield); c) in particular, as provided by Standard Contractual Clauses (SCC).

4. What is meant by transfers of personal data as **interference**?

   a) with Articles 7 and 8 of the Charter;

   b) requiring compliance with inter alia Articles 47 and 52 of the Charter in order for such interference to be lawful;

   c) and which should be limited to what is strictly necessary and should not compromise the essence of the fundamental rights to privacy and to the protection of personal data

5. When and subject to which conditions **have SCC been considered valid** by the CJEU as a tool for transfer of personal data?

6. What is meant by **effective judicial and administrative redress**?

7. What is meant by the duty to **notify to the data subject** the transfer of personal data?

8. Are specific safeguards needed in case of transfer of personal data subject to **automated processing** or involving **sensitive data?**

9. What are the data protection requirements in case of onward transfer of personal data?

3

SOURCES

1) Judgment of 6 November 2003, *Lindqvist*, C-101/01, EU:C:2003:596

Transfer of personal data to a third country, *Lindqvist*

Mrs Lindqvist was charged with breach of the Swedish data protection legislation for **publishing on her internet site personal data on a number of people** working with her on a voluntary basis in a parish of the Swedish Protestant Church. In criminal proceedings before it, the referring court (Göta Court of Appeal) raised preliminary ruling questions. It sought, among others, to establish **whether Ms Lindqvist had carried out a transfer** of data **to a third country** within the meaning of Directive 95/46/EC.

The Court held that "there is **no 'transfer [of data] to a third country**' within the meaning of Article 25 of Directive 95/46 where **an individual in a Member State loads personal data onto an internet page** which is s**tored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.**" (paragraph 71).

(i) Absence of definition in the law:

"56. Directive 95/46 does not define the expression '**transfer to a third country**' in Article 25 or any other provision, including Article 2."

(ii) Still, the Court provides several criteria:

"57. In order to determine **whether loading personal data onto an internet page constitutes a 'transfer'** of those data to a third country within the meaning of Article 25 of Directive 95/46 merely because it makes them accessible to people in a third country, it is necessary to take account both of **the technical nature of the operations** thus carried out and of **the purpose and structure of Chapter IV of that directive** where Article 25 appears."

One must therefore take into account:

(a) Firstly, pointing out to the technical nature of the operations carried out

"59. **Under the procedures for use of the internet available to individuals like Mrs Lindqvist during the 1990s**, the author of a page intended for publication on the internet transmits the data making up that page to **his hosting provider**. **That provider** manages the

to the internet. That allows the subsequent transmission of those data **to anyone who connects to the internet and seeks access to it**. The computers which constitute that infrastructure may be located, and indeed often are located, in one or more countries other than that where the hosting provider is established, without its clients being aware or being in a position to be aware of it."

"60. It appears from the court file that, in order to obtain the information appearing on the internet pages on which Mrs Lindqvist had included information about her colleagues, an internet user would not only have to **connect to the internet** but **also personally carry out the necessary actions to consult those pages**. In other words, Mrs Lindqvist's internet pages did not contain the technical means to send that information **automatically to people** who did not intentionally seek access to those pages."

"61. It follows that, in circumstances such as those in the case in the main proceedings, personal data which appear on the computer of a person in a third country, coming from a person who has loaded them onto an internet site, were **not directly transferred** between those two people but through the computer infrastructure of the hosting provider where the page is stored".

> *(b) Secondly, a **case-by-case assessment** is necessary, which takes into consideration the **intentions of the legislature** (purpose and structure of the transfers provisions), as well as **the consequences of the qualification** of the data processing as transfer to third countries*

"62. It is in that light that it must be examined **whether the Community legislature intended**, for the purposes of the application of Chapter IV of Directive 95/46, to include within the expression '**transfer [of data] to a third country**' within the meaning of Article 25 of that directive activities such as those carried out by Mrs Lindqvist. It must be stressed that the fifth question asked by the referring court concerns **only those activities and not those carried out by the hosting providers.**"

"67. Chapter IV of Directive 95/46 contains no provision concerning **use of the internet**. In particular, it does not lay down criteria for deciding whether operations carried out by **hosting providers** should be deemed to occur in the **place of establishment of the service** or at its **business address** or in the **place where the computer or computers constituting the service's infrastructure are located.**"

"68. **Given, first, the state of development of the internet** at the time Directive 95/46 was drawn up and, second, **the absence, in Chapter IV, of criteria applicable to use of the internet,** one cannot presume that the Community legislature intended the expression 'transfer [of data] to a third country' to cover **the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page**, even if those data are thereby made accessible to persons in third countries with the technical means to access them."

"69. If Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an internet page, that transfer would necessarily be a **transfer to all the third countries** where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even

one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet."

"70. Accordingly, it must be concluded that Article 25 of Directive 95/46 is to be interpreted as meaning that operations such as **those carried out by Mrs Lindqvist** do not as such constitute a 'transfer [of data] to a third country'. It is thus unnecessary to investigate whether an individual from a third country has accessed the internet page concerned or whether the server of that hosting service is physically in a third country."

2) Judgment of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650

Mr. Schrems lodged a complaint asking the Irish Data Protection Commissioner to prohibit Facebook Ireland from **transferring** his personal data to the United States. He submitted that the United States did not ensure an adequate level of protection of personal data because of the surveillance activities conducted by the public authorities. The Irish Data Protection Commissioner in its decision considered in particular that the allegations raised by Mr Schrems in his complaint could not be profitably put forward since any question of the adequacy of data protection in the United States had to be determined in accordance with Decision 2000/520 and the Commission had found in that decision that the United States ensured an adequate level of protection. Mr. Schrems challenged the decision by the Irish Data Protection Commissioner before the Irish High Court, which referred to the CJEU the question whether the Irish Data Protection Commissioner is bound by the findings by the Commission on the adequacy of protection or it can examine the claim of a person concerned by the data processing which contends that the level of protection in question is inadequate.

Transfer of personal data to a third country, *Schrems*

*a) **Technical nature of the operations** of the transfer:*

The judgment concerns the transfer of personal data carried out by Facebook Ireland, a subsidiary of Facebook Inc whereby "[s]ome or all of the **personal data of Facebook** Ireland's **users who reside in the European Union is transferred to servers** belonging to Facebook Inc. that are **located in the United States, where it undergoes processing.**" (paragraph. 27)

"45. [T]he operation consisting in **having personal data transferred from a Member State to a third country** constitutes, in itself, **processing of personal data** within the meaning of Article 2(b) of Directive 95/46 (see, to this effect, judgment in Parliament v Council and Commission, C-317/04 and C-318/04, EU:C:2006:346, paragraph 56) carried out in a Member State. That provision defines 'processing of personal data' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means' and mentions, by way of example, 'disclosure by transmission, dissemination or otherwise making available'."

*b) **Legal requirements applicable to** transfers: **not limited to Chapter IV** of Directive 95/46 (**now Chapter V** of the GDPR):*

"46. Recital 60 in the preamble to Directive 95/46 states that transfers of personal data to third countries may be effected only **in full compliance with the provisions adopted by the Member States pursuant to the directive**. In that regard, **Chapter IV** of the directive, in which Articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries. That regime **is complementary to the general regime set up by Chapter II of the directive laying down the general rules on the lawfulness of the processing of personal data** (see, to this effect, judgment in Lindqvist, C-101/01, EU:C:2003:596, paragraph 63).

Transfer to a third country: **Safe Harbor, powers available to the national supervisory authorities in respect of the transfers,** *Schrems*

The referring court asks, in essence, whether and to what extent Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that **a decision adopted pursuant to that provision, such as Decision 2000/520**, by which the Commission finds that a third country ensures an **adequate level of protection, prevents a supervisory authority** of a Member State, within the meaning of Article 28 of that directive, **from being able to examine the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data related to him which has been transferred** from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

"55. [T]he first subparagraph of Article 28(4) of Directive 95/46, under which the national **supervisory authorities are to hear 'claims** lodged by any person ... concerning the protection of his rights and freedoms in regard to the processing of personal data', does not provide for any exception in this regard where the Commission has adopted a decision pursuant to Article 25(6) of that directive."

"56. [I]t would be contrary to the system set up by Directive 95/46 and to the objective of Articles 25 and 28 thereof for a Commission decision adopted pursuant to Article 25(6) to have the effect of **preventing a national supervisory authority from examining a person's claim** concerning the protection of his rights and freedoms in regard to the processing of his personal data which has been or could be transferred from a Member State to the third country covered by that decision."

"57. [...] **Article 28 of Directive 95/46 applies, by its very nature, to any processing of personal data.** Thus, **even if the Commission has adopted a decision pursuant to Article 25(6)** of that directive, the national supervisory authorities, when hearing a claim lodged by a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, must be able to **examine, with complete independence, whether the transfer of that data complies** with the requirements laid down by the directive."

"65. Where the national supervisory authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights and freedoms in regard to the processing of his personal data are well founded, **that authority must**, in accordance with the third indent of the first subparagraph of Article 28(3) of Directive 95/46, read in the light in particular of Article 8(3) of the Charter, **be able to engage in legal proceedings.** It is incumbent upon the national legislature to provide for legal remedies **enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity.**"

The Court declared Article 3 of Decision 2000/520/EC to be invalid in so far as it denied national supervisory authorities the powers which derive from Article 28 of Directive 95/46/EC, where a person puts forward matters that may call in question whether a Commission decision that has found that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals (paragraphs 102-104).

Transfer to a third country: **adequate level of protection,** *Schrems*

"74. It is clear from the express wording of Article 25(6) of Directive 95/46 that it is **the legal order of the third country** covered by the Commission decision that must ensure an adequate level of protection. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection **may differ** from those employed within the European Union in order to ensure that the requirements stemming from Directive 95/46 read in the light of the Charter are complied with, those means must nevertheless prove, in practice, **effective** in order to ensure protection **essentially equivalent** to that guaranteed within the European Union."

"75. [W]hen examining the level of protection afforded by a third country, the Commission is obliged to assess **the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules**, since it must, under Article 25(2) of Directive 95/46, take account of all the circumstances surrounding a transfer of personal data to a third country."

Transfer to a third country: **adequate level of protection, as provided under Decision 2000/520/EC, Safe Harbor,** *Schrems*

*a) The **international commitments and practice** designed to ensure an essential equivalent level of protection in the case before the Court of Justice, nature and scope*

"79. The Commission found in Article 1(1) of **Decision 2000/520** that the **principles set out in Annex I thereto, implemented in accordance with the guidance provided by the FAQs set out in Annex II**, ensure an adequate level of protection for personal data transferred from the European Union to organisations established in the United States. It is apparent from that provision that both those **principles and the FAQs** were **issued by the United States Department of Commerce.**"

"80. An organisation adheres to the safe harbour principles on the basis of a system of self-certification, as is apparent from Article 1(2) and (3) of Decision 2000/520, read in conjunction with FAQ 6 set out in Annex II thereto."

"81. Whilst recourse by a third country to a **system of self-certification** is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 that the third country concerned must **ensure an adequate level of protection 'by reason of its domestic law or ... international commitments**', the reliability of such a system, in the light of that requirement, is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be identified and punished in practice."

"82. In the present instance, by virtue of the second paragraph of Annex I to Decision 2000/520, the safe harbour principles are '**intended for use solely by US organisations receiving personal data from the European Union** for the purpose of qualifying for the safe harbour and the

presumption of "adequacy" it creates'. Those principles are therefore applicable solely **to self-certified United States organisations receiving personal data from the European Union [...]**."

*b) **Relationship** of Safe Harbor principles **with the US legal order***

"84. Under the fourth paragraph of Annex I to Decision 2000/520, the applicability of the safe harbour principles may be limited, in particular, 'to the extent necessary to meet national security, public interest, or law enforcement requirements' and 'by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'."

"85. In this connection, Decision 2000/520 states in Part B of Annex IV, with regard to the limits to which the safe harbour principles' applicability is subject, that, **'[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law'."**

"86. Thus, **Decision 2000/520 lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles**, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them."

*c) **Conclusion** taking into account the above relationship and the assessment of the relevant aspects of the third country legal order*

"96. [I]n order for the Commission to adopt a decision pursuant to Article 25(6) of Directive 95/46, it must find, duly stating reasons, that the third country concerned **in fact ensures, by reason of its domestic law or its international commitments**, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order, a level that is apparent in particular from the preceding paragraphs of the present judgment."

"97. However, the Commission did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments."

"98. Consequently, **without there being any need to examine the content of the safe harbour principles**, it is to be concluded that Article 1 of Decision 2000/520 fails to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of the Charter, and that it is accordingly invalid."

Transfers of personal data as **interference** with Articles 7 and 8 of the Charter, requiring compliance with Article 52 of the Charter in order for such interference to be lawful, *Schrems*

"87. In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus **enables interference, founded on national security and public interest requirements or on domestic legislation of the United States,** with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States."

As regards the impossibility of **justifying such interference**, the Court, first of all, observed that EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the **persons, whose personal data is concerned** have sufficient **guarantees** enabling their data to be effectively protected against the risk of abuse and against any unlawful access to and use of those data. The need for such safeguards is all the greater when personal data is subjected to **automatic processing** and where there is a significant risk of **unlawful access to this data** (paragraph 91).

Interference should be limited to what is **strictly necessary** and should not compromise the **essence** of the fundamental rights to privacy and to the protection of personal data

Protection of the fundamental rights to respect for private life and to the protection of personal data requires derogations and limitations in relation to the protection of personal data to apply **only in so far as is strictly** necessary. (paragraph 92)

Legislation is **not limited to what is strictly necessary** where it authorises, on a **generalised basis**, storage of all the personal data of all the persons whose data has been transferred from the European Union **without any differentiation, limitation or exception** being made in the light of the objective pursued, and **without an objective criterion being laid down by which to determine the limits** of the access of the public authorities to the data, and of the subsequent use of this data, for **purposes which are specific, strictly restricted and capable of justifying the interference** which both access to this data and their use entail. (paragraph 93)

Legislation permitting public authorities to have **access on a generalised basis** to the content of electronic communications compromises **the essence** of the fundamental right to respect for private life. (paragraph 94)

Legislation not providing for any possibility for an individual to pursue **legal remedies** in order to have access to personal data relating to him, or to obtain the **rectification or erasure** of such data, does not respect **the essence** of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. (paragraph 95)

3) Opinion 1/15 of the Court of 26 July 2017, *EU-Canada PNR Agreement*, EU:C:2017:592

Transfer of personal data to a third country (pursuant to **an international agreement**), *PNR Opinion*

The European Union and Canada negotiated an **agreement on the transfer and processing of Passenger Name Record data** (PNR agreement) which was signed in 2014. The Council of the European Union then requested the European Parliament adecision on the conclusion of the agreement envisaged. Upon receiving the request, the European Parliament decided to refer the matter to the CJEU in order to ascertain whether the envisaged agreement was compatible with the Treaties. The envisaged agreement allows the **systematic and continuous transfer of PNR data** of all air passengers to a Canadian authority with a view of using, retaining and possibly transferring this data subsequently to other authorities in Canada (further processing) and to other countries (onward transfer), for the purpose of combating terrorism and serious transnational crime. On 26 July 2017, the CJEU delivered its opinion on the compatibility of the **international agreement** with the Charter of Fundamental Rights of the European Union, and, in particular, with provisions related to respect for private life and the protection of personal data.

Transfer to a third country: adequate level of protection - as provided by an **international agreement**, *PNR Opinion*

"120. To the extent that the assessments that follow relate to the compatibility of the envisaged agreement with the right to the protection of personal data, enshrined in both **Article 16(1) TFEU** and **Article 8 of the Charter**, the Court will refer solely to the second of those provisions. Although both of those provisions state that everyone has the right to the protection of personal data concerning him or her, only **Article 8 of the Charter** lays down in a more specific manner, in paragraph 2 thereof, the conditions under which such data may be processed."

"122. Since the PNR data therefore includes information on identified individuals, namely air passengers flying between the European Union and Canada, the various forms of processing to which, under the envisaged agreement, that data may be subject, namely its transfer from the European Union to Canada, access to that data with a view to its use or indeed its retention, affect the fundamental right to respect for private life, guaranteed in **Article 7 of the Charter.**"

"123. Furthermore, the processing of the PNR data covered by the envisaged agreement also falls within the scope of **Article 8 of the Charter** because it constitutes the processing of personal data within the meaning of that article and, accordingly, must necessarily satisfy the data protection requirements laid down in that article."

"134. That right to the protection of personal data requires, inter alia, that the high level of protection of fundamental rights and freedoms conferred by EU law **continues where personal data is transferred from the European Union to a non-member country**. Even though **the means** intended to ensure such a level of protection [in this case, the international agreement] may differ from those employed within the European Union in order to ensure that the requirements stemming from EU law are complied with, those means must nevertheless

prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union."

Conclusion on the validity of the international agreement taking into account the above relationship and the assessment of the relevant aspects of the third country legal order

"232. In the light of all the foregoing considerations, it must be held that:

(2) the envisaged agreement is incompatible with Articles 7, 8 and 21 and Article 52(1) of the Charter in so far as it does not preclude the transfer of sensitive data from the European Union to Canada and the use and retention of that data;
(3) the envisaged agreement must, in order to be compatible with Articles 7 and 8 and Article 52(1) of the Charter:

a) determine in a clear and precise manner the PNR data to be transferred from the European Union to Canada;

b) provide that the models and criteria used in the context of automated processing of PNR data will be specific and reliable and non-discriminatory; provide that the databases used will be limited to those used by Canada in relation to the fight against terrorism and serious transnational crime;

c) used will be limited to those used by Canada in relation to the fight against terrorism and serious transnational crime;

d) save in the context of verifications in relation to the pre-established models and criteria on which automated processing of PNR data is based, make the use of that data by the Canadian Competent Authority during the air passengers' stay in Canada and after their departure from that country, and any disclosure of that data to other authorities, subject to substantive and procedural conditions based on objective criteria; make that use and that disclosure, except in cases of validly established urgency, subject to a prior review carried out either by a court or by an independent administrative body, the decision of that court or body authorising the use being made following a reasoned request by those authorities, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime;

e) limit the retention of PNR data after the air passengers' departure to that of passengers in respect of whom there is objective evidence from which it may be inferred that they may present a risk in terms of the fight against terrorism and serious transnational crime;

f) make the disclosure of PNR data by the Canadian Competent Authority to the government authorities of a third country subject to the condition that there be either an agreement between the European Union and that third country equivalent to the envisaged agreement, or a decision of the Commission, under Article 25(6) of Directive 95/46, covering the authorities to which it is intended that PNR data be disclosed;

provide for a right to individual notification for air passengers in the event of use of PNR data concerning them during their stay in Canada and after their departure from that country, and in the event of disclosure of that data by the Canadian Competent Authority to other authorities or to individuals; and

g) guarantee that the oversight of the rules laid down in the envisaged agreement relating to the protection of air passengers with regard to the processing of PNR data concerning them will be carried out by an independent supervisory authority."

See also EDPS Guidelines on Proportionality (at pages 18, 26, 30, 34) and The EDPS quick-guide to necessity and proportionality.

Transfers of personal data **as interference** with **Articles 7 and 8** of the Charter, *PNR Opinion*

"124. As the Court has held, the communication of personal data to a third party, such as a public authority, constitutes **an interference** with the fundamental right enshrined in **Article 7** of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities. In this connection, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference."

"126. Those operations also constitute an interference with the fundamental right to the protection of personal data guaranteed in **Article 8** of the Charter since they constitute the processing of personal data."

Transfers of personal data **as interference**, requiring compliance with **Article 52** of the Charter in order for such interference to be lawful

"138. [I]n accordance with the first sentence of **Article 52(1)** of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Under the second sentence of Article 52(1) of the Charter, subject to the principle of **proportionality**, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

"139. It should be added that the requirement that **any limitation** on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned. [...]"

"140. As regards observance of the principle of **proportionality**, the protection of the fundamental right to respect for private life at EU level requires, in accordance with settled case-law of the Court, that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary."

"141. In order to satisfy that requirement, the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have **sufficient guarantees** to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is **strictly necessary**."

An interference should not compromise the essence of the fundamental rights to privacy and to the protection of personal data

The Court points out the essence of the fundamental rights at stake under, respectively, Article 7 and 8 of the Charter.

"150. As regards **the essence of the fundamental right to respect for private life**, enshrined in **Article 7** of the Charter, even if PNR data may, in some circumstances, reveal very specific information concerning the private life of a person, the nature of that information is limited to certain aspects of that private life, in particular, relating to air travel between Canada and the European Union.

As for **the essence of the right to the protection of personal data**, enshrined in **Article 8** of the Charter, the envisaged agreement limits, in Article 3, the purposes for which PNR data may be processed and lays down, in Article 9, rules intended to ensure, inter alia, the security, confidentiality and integrity of that data, and to protect it against unlawful access and processing."

Necessity of the interference

"154. As regards **the necessity of the interferences** entailed by the envisaged agreement, it is necessary to check, in accordance with the case-law cited in paragraphs 140 to 141 of this Opinion, whether they are limited to what is strictly necessary and, in that context, whether that agreement lays down clear and precise rules governing the scope and application of the measures provided for."

The Court considered in this regard:

(1) The PNR data covered by the envisaged agreement:

(i) Whether the envisaged agreement is sufficiently precise as regards the PNR data to be transferred (paras 155-162) and concludes (para 163) that "In those circumstances, as regards the PNR data to be transferred to Canada, headings 5, 7 and 17 of the Annex to the envisaged agreement do not delimit in a sufficiently clear and precise manner the scope of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter;"

(ii) [Whether the transfers of personal data concerns] sensitive data (paras 164-166) and concludes (para 167) that "Having regard to the assessments set out in the two preceding paragraphs, it must be held that Articles 7, 8 and 21 and Article 52(1) of the Charter preclude both the transfer of sensitive data to Canada and the framework negotiated by the European Union with that non-member State of the conditions concerning the use and retention of such data by the authorities of that non-member State."

(2) Whether the data transferred are **subject to automated processing** (paras 168-174, *PNR Opinion*).

See in this regard in particular:

"168. As stated in paragraphs 130 to 132 of this Opinion and as the Advocate General has noted in point 252 of his Opinion, the PNR data transferred to Canada is mainly intended to be subject to **analyses by automated means**, based on pre-established models and criteria and on cross-checking with various databases."

"169. The assessment of the risks to public security presented by air passengers is carried out [...] by means of automated analyses of the PNR data before the arrival of those air passengers in Canada. Since those analyses are carried out on the basis of unverified personal data and are based on pre-established models and criteria, they necessarily present some **margin of error**, as, inter alia, the French Government and the Commission conceded at the hearing."

"170. As stated in point 30 of the Opinion of the EDPS on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (OJ 2008 C 110, p. 1), to which the EDPS referred in his answer to the questions posed by the Court, that **margin of error** appears to be significant."

(3) The **purposes** for which PNR data may be processed (paras 175-181)

(4) The Canadian **authorities covered** by the envisaged agreements (paras 182-185)

(5) The **air passengers concerned** (paras 186-189)

(6) The **retention and use** of PNR data (paras 190-211)

(7) The **disclosure** of PNR data (paragraph 214, *PNR Opinion*)

In this regard, the Court clarified the data protection requirements concerning **onward transfers**:

"214. [...] it must be recalled that **a transfer of personal data** from the European Union to a non-member country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union. That **same requirement applies** in the case of the disclosure of PNR data by Canada to **third countries**, referred to in Article 19 of the envisaged agreement, **in order to prevent the level of protection provided for in that agreement from being circumvented by transfers of personal data to third countries and to ensure the continuity of the level of protection afforded by EU law** [...]. In those circumstances, such **disclosure** requires the existence of either an agreement between the European Union and the non-member country concerned equivalent to that agreement, or a decision of the Commission, under Article 25(6) of Directive 95/46, finding that the third country ensures an adequate level of protection within the meaning of EU law and covering the authorities to which it is intended PNR data be transferred."

Transfer of data subject to **automated processing** and of **sensitive data**, *PNR Opinion*

"141. The need for such safeguards is all the greater where personal data is subject to automated processing (see paras 168-174).

Those considerations apply particularly where the protection of the particular category of

personal data that is sensitive data is at stake." (see also paragraphs 164-167).

Onward transfers, *PNR Opinion*

125. "[B]**oth the transfer** of PNR data from the European Union to the Canadian Competent Authority **and the framework negotiated by the European Union with Canada of the conditions concerning the retention of that data, its use and its subsequent transfer** to other Canadian authorities, Europol, Eurojust, judicial or police authorities of the Member States or indeed to authorities of third countries, which are permitted, inter alia, by Articles 3, 4, 6, 8, 12, 15, 16, 18 and 19 of the envisaged agreement, constitute interferences with the right guaranteed in Article 7 of the Charter."

"214. In this connection, it must be recalled that a transfer of personal data from the European Union to a non-member country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the

European Union. That **same requirement applies in the case of the disclosure of PNR data by Canada to third countries**, referred to in Article 19 of the envisaged agreement, in order to prevent the level of protection provided for in that agreement from being circumvented by transfers of personal data to third countries and to ensure the continuity of the level of protection afforded by EU law (see, by analogy, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraphs 72 and 73). In those circumstances, such disclosure requires the existence of either an agreement between the European Union and the non-member country concerned equivalent to that agreement, or a decision of the Commission, under Article 25(6) of Directive 95/46, finding that the third country ensures an adequate level of protection within the meaning of EU law and covering the authorities to which it is intended PNR data be transferred."

Duty to **notify** the transfer to the data subject, *PNR Opinion*

"The Court held that the fundamental right to respect for private life, enshrined in Article 7 of the Charter of Fundamental Rights of the European Union, "means that the person concerned may be certain that his personal data are processed in a correct and lawful manner" (paragraph 219).

The Court pointed out in that regard that air passengers must be **notified of the transfer** of their PNR data to the third country concerned and of the use of those data **as soon as that information is no longer liable to jeopardise the investigations** being carried out by the government authorities referred to in the envisaged agreement." (paragraph 220; see also paragraphs 221-225)

Effective **judicial and administrative redress**, *PNR Opinion*

"226. As regards air passengers' **right to redress**, Article 14(2) of the envisaged agreement provides that Canada is to ensure that any individual who is of the view that their rights have been infringed by a decision or action in relation to their PNR data may seek **effective judicial redress,** in accordance with Canadian law, or such other remedy which may include compensation."

Powers available to the national supervisory authorities in respect of the transfers, *PNR Opinion*

"228. Under Article 8(3) of the Charter, compliance [of the international agreement] with the requirements stemming from Article 8(1) and (2) thereof is subject to **control by an independent authority.**"

It might be worth also recalling that the requirement for an **independent supervisory authority** was not fully met under the PNR agreement (see paragraphs 230-231: "230. In this instance, the first sentence of Article 10(1) of the envisaged agreement states that the data protection safeguards for the processing of PNR data will be subject to oversight by an 'independent public authority' or by an 'authority created by administrative means that exercises its functions in an impartial manner and that has a proven record of autonomy'. In so far as that provision provides that the oversight is to be carried out by an independent authority, it corresponds to the requirement set out in Article 8(3) of the Charter. By contrast, **its formulation in the alternative seems to permit the oversight to be carried out, partly or wholly, by an authority which does not carry out its tasks with complete independence**, but which is subordinate to a further supervisory authority, from which it may receive instructions, and which is therefore not free from any external influence liable to have an effect on its decisions.

231. In those circumstances, and as the Advocate General has observed in point 316 of his Opinion, Article 10 of the envisaged agreement does not guarantee in a sufficiently clear and precise manner that the oversight of compliance with the rules laid down in that agreement relating to the protection of individuals with regard to the processing of PNR data will be carried out by an independent authority, within the meaning of Article 8(3) of the Charter.

4) Judgment of 16 July 2020, *Schrems II*, C-311/18, EU:C:2020:559

Following the Schrems I judgment and the subsequent annulment by the referring court of the decision rejecting Mr Schrems' complaint, the Irish supervisory authority asked Mr Schrems to reformulate his complaint in the light of the declaration by the Court that Decision 2000/520 was invalid. In his reformulated complaint, Mr Schrems claims that the United States does not offer sufficient protection of data transferred to that country. He seeks the suspension or prohibition of future transfers of his personal data from the EU to the United States, which Facebook Ireland now carries out pursuant to the **standard data protection clauses** set out in the Annex to Decision 2010/87.

Transfer to a third country, *Schrems II*

*a) **Legal aspects** of the transfer:*

"86. The possibility that the **personal data transferred between two economic operators for commercial purposes** might undergo, at the time of the transfer or thereafter, **processing for the purposes of public security, defence and State security** by the authorities of that third country c**annot remove that transfer from the scope of the GDPR**." (see also paragraphs 87, 88).

"89. [...] Article 2(1) and (2) of the GDPR must be interpreted as meaning that that regulation applies to the **transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective** of whether, at the time of that transfer or thereafter, that data is **liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.**"

In this regard, see also judgment of 6 October 2020, ***Privacy International*, C-623/17**, which **confirms this approach** (see in particular at paragraphs 35, 39, 44 and 49. Paragraph 44 states in particular "[...] according to the settled case-law of the Court, although it is for the Member States to define their essential **security interests** and to adopt appropriate measures to ensure their internal and external security, **the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law.** [...]"

*b) **Legal regime** of transfers: **not only Chapter IV** of Directive 95/46 (**now Chapter V** of the GDPR):*

"82. Under Article 2(1) of the GDPR, that regulation applies to the **processing of personal data** wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Article 4(2) of that regulation defines '**processing**' as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means' and mentions, by way of example, 'disclosure by transmission, dissemination or otherwise making

available', but **does not distinguish between operations which take place within the European Union and those which are connected with a third country. Furthermore, the GDPR subjects transfers of personal data to third countries to specific rules in Chapter V** thereof, entitled 'Transfers of personal data to third countries or international organisations', and also confers specific powers on the supervisory authorities for that purpose, which are set out in Article 58(2)(j) of that regulation."

Transfer to a third country: adequate level of protection - as **provided by standard contractual clauses** - assessment, *Schrems II*

"102. The referring court also seeks to ascertain **what factors** should be taken into consideration for the purposes of determining the adequacy of the level of protection where personal data is transferred to a third country pursuant to **standard data protection clauses** adopted under Article 46(2)(c) of the GDPR."

"103. In that regard, although that provision **does not list the various factors** which must be taken into consideration for the purposes of assessing the adequacy of the level of protection to be observed in such a transfer, Article 46(1) of that regulation states that data subjects must be afforded **appropriate safeguards, enforceable rights and effective legal remedies**."

"105. [...] Article 46(1) and Article 46(2)(c) of the GDPR must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to **standard data protection clauses** are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration **both the contractual clauses** agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned **and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country**, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation."

Transfer to a third country: adequate level of protection, as provided under SCC, **powers available to the national supervisory authorities** in respect of the transfers, *Schrems II*

"146. Article 4 of the SCC Decision, read in the light of recital 5 of Implementing Decision 2016/2297, supports the view that **the SCC Decision does not prevent the competent supervisory authority from suspending or prohibiting**, as appropriate, a transfer of personal data to a third country pursuant to the standard data protection clauses in the annex to that decision. In that regard, as is apparent from the answer to the eighth question, **unless there is a valid Commission adequacy decision, the competent supervisory authority is required, under Article 58(2)(f) and (j) of the GDPR, to suspend or prohibit such a transfer**, if, in its view and **in the light of all the circumstances of that transfer**, those clauses are not or

cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer."

"147. As regards the fact, underlined by the Commissioner, that transfers of personal data to such a third country may result in the supervisory authorities in the various Member States adopting divergent decisions, it should be added that, as is clear from Article 55(1) and Article 57(1)(a) of the GDPR, the task of enforcing that regulation is conferred, in principle, on **each supervisory authority on the territory of its own Member State**. Furthermore, in order to avoid divergent decisions, Article 64(2) of the GDPR provides for **the possibility for a supervisory authority which considers that transfers of data to a third country must, in general, be prohibited, to refer the matter to the European Data Protection Board (EDPB) for an opinion**, which may, under Article 65(1)(c) of the GDPR, adopt a binding decision, in particular where a supervisory authority does not follow the opinion issued."

Transfer to a third country: adequate level of protection - **validity of standard contractual clauses/SCC decision**, *Schrems II*

*a) On the **difference between adequacy decisions and SCC decision***

"129. [S]uch a **standard clauses decision differs from an adequacy decision** adopted pursuant to Article 45(3) of the GDPR, which seeks, following an examination of the legislation of the third country concerned taking into account, *inter alia*, the relevant legislation on national security and public authorities' access to personal data, to find with binding effect that a third country, a territory or one or more specified sectors within that third country ensures an adequate level of protection and that the access of that third country's public authorities to such data does not therefore impede transfers of such personal data to the third country. Such an adequacy decision can therefore be adopted by the Commission only if it has found that the third country's relevant legislation in that field does in fact provide all the necessary guarantees from which it can be concluded that that legislation ensures an adequate level of protection."

"130. By contrast, in the case of a **Commission decision adopting standard data protection clauses, such as the SCC Decision**, in so far as such a decision does not refer to a third country, a territory or one or more specific sectors in a third country, **it cannot be inferred from Article 46(1) and Article 46(2)(c) of the GDPR that the Commission is required, before adopting such a decision, to assess the adequacy of the level of protection ensured by the third countries** to which personal data could be transferred pursuant to such clauses."

"131. [A]ccording to Article 46(1) of the GDPR, in the absence of a Commission adequacy decision, **it is for the controller or processor** established in the European Union to provide, *inter alia*, **appropriate safeguards**. Recitals 108 and 114 of the GDPR confirm that, where the Commission has not adopted a decision on the adequacy of the level of data protection in a third country, the controller or, where relevant, the processor 'should **take measures to compensate** for the lack of data protection in a third country by way of appropriate safeguards for the data subject'."

See also the EDPB "Recommendations 01/2020 **on measures that supplement transfer tools** to ensure compliance with the EU level of protection of personal data", available at: **edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (europa.eu)** and submitted to public consultation until 21 December 2020.

The EDPB has also adopted the "Recommendations 02/2020 on the **European Essential Guarantees** for surveillance measures", available at: **edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf (europa.eu)**

which updates and integrates the Article 29 Working Party working document on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data.

*b) Relationship of **SCC with third country legal framework - possible need for other clauses or additional safeguards that supplement SC***

"132. Since by their **inherently contractual nature** standard data protection clauses **cannot bind the public authorities of third countries** [...] but that Article 44, Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, require that the **level of protection** of natural persons guaranteed by that regulation is not undermined, it may prove **necessary to supplement the guarantees contained in those standard data protection clauses**. In that regard, recital 109 of the regulation states that 'the possibility for the controller ... to use standard data-protection clauses adopted by the Commission ... should [not] prevent [it] ... from **adding other clauses or additional safeguards**' and states, in particular, that the controller 'should be encouraged to provide **additional safeguards** ... that **supplement** standard [data] protection clauses'."

*c) Responsibility of the **controller or processor, or, failing that, of the competent supervisory authority***

"134. [T]he contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the **responsibility of the controller or his or her subcontractor** established in the European Union and, in the alternative, of the **competent supervisory authority**. It is therefore, above all, for that controller or processor to verify, **on a case-by-case basis** and, **where appropriate, in collaboration with the recipient of the data**, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, **additional safeguards** to those offered by those clauses."

"135. Where the **controller or a processor** established in the European Union is not able to take adequate **additional measures** to guarantee such protection, the **controller or processor** or, failing that, **the competent supervisory authority**, are required to **suspend or end** the transfer of personal data to the third country concerned. That is the case, **in particular**, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data."

d) Conclusion on the validity of SCC

The Court examines the **validity of Decision 2010/87 (on SCC)**. The Court considers that the validity of that decision is not called into question by the mere fact that the standard data protection clauses in that decision **do not, given that they are contractual in nature, bind the authorities of the third country to which data may be transferred**. That validity depends on whether the decision includes **effective mechanisms** that make it possible, **in practice**, to **ensure compliance** with the level of protection required by EU law and that transfers of personal data pursuant to such clauses are **suspended or prohibited** in the event of the **breach of such clauses** or it being **impossible to honour them** (paragraph 137).

The Court finds that Decision 2010/87 **establishes such mechanisms** (in that regard, see para 138-146).

On the need to assess the level of protection as provided by the Privacy Shield, *Schrems II*

"161. [I]t should therefore be examined **whether the Privacy Shield Decision complies with the requirements stemming from the GDPR** read in the light of the Charter."

Reasons being that:

"154. In particular, the question **whether the finding in the Privacy Shield Decision that the United States ensures an adequate level of protection** is binding is relevant for the purposes of **assessing both the obligations**, set out in paragraphs 141 and 142 above (*), **of the controller and recipient** of personal data transferred to a third country pursuant to the standard data protection clauses in the annex to the SCC Decision **and also any obligations to which the supervisory authority may be subject** to suspend or prohibit such a transfer."

(*) [paragraph 141: "Clause 4(a) and Clause 5(a) and (b) in that annex oblige the controller established in the European Union and the recipient of personal data to satisfy themselves that the legislation of the third country of destination enables the recipient to comply with the standard data protection clauses in the annex to the SCC Decision, before transferring personal data to that third country"; paragraph 142: "a controller established in the European Union and the recipient of personal data are required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned. The recipient is, where appropriate, under an obligation, under Clause 5(b), to inform the controller of any inability to comply with those clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract."]

Transfer to a third country: adequate level of protection - as provided by the **Privacy Shield,** *Schrems II*

a) The international commitments and practice designed to ensure an essential equivalent level of protection in the case before the Court of Justice, nature and scope

"163. The Commission found, in Article 1(1) of the Privacy Shield Decision, that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the **EU-US Privacy Shield**, the latter being comprised, inter alia, under Article 1(2) of that decision, of the Principles issued by the US Department of Commerce on 7 July 2016 as set out in Annex II to the decision and the official representations and commitments contained in the documents listed in Annexes I and III to VII to that decision."

b) Relationship of Privacy Shield principles with the US legal order

"164. [T]he Privacy Shield Decision also states, in paragraph I.5. of Annex II, under the heading 'EU-U.S. Privacy Shield Framework Principles', that adherence to those principles **may be limited, inter alia, 'to the extent necessary to meet national security, public interest, or law enforcement** requirements'. Thus, that decision lays down, as did Decision 2000/520, that those requirements have primacy over those principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard the principles without limitation where they conflict with the requirements and therefore prove incompatible with them."

c) Conclusion taking into account the above relationship and the assessment of the relevant aspects of the third country legal order

On all those grounds (see paragraphs 168-200), the Court declares Decision 2016/1250 (Privacy Shield) **invalid** (paragraphs 199-201).

Transfers of personal data as **interference**, requiring compliance with Article 52 of the Charter in order for such interference to be lawful, *Schrems II*

"165. In the light of its general nature, the derogation set out in paragraph I.5 of Annex II to the Privacy Shield Decision **thus enables interference**, based on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States [...]. More particularly, as noted in the Privacy Shield Decision, such interference can arise from access to, and use of, personal data transferred from the European Union to the United States by US public authorities through the PRISM and UPSTREAM surveillance programmes under Section 702 of the FISA and E.O. 12333."

"174. [I]n accordance with the first sentence of **Article 52(1) of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence** of those rights and freedoms. Under the second sentence of Article 52(1) of the Charter, subject to the principle of **proportionality**, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others." (see also paragraph 178)

"175. Following from the previous point, it should be added that the requirement that any limitation on the exercise of fundamental rights must be provided for by law implies that **the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned**."

"176. Lastly, in order to satisfy the requirement of proportionality according to which derogations from and limitations on the protection of personal data must apply only in so far as is strictly necessary, **the legislation in question which entails the interference must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards**, so that the persons whose data has been transferred have sufficient guarantees to protect effectively their personal data against the risk of abuse. It must, in particular, indicate i**n what circumstances and under which conditions a measure providing for the processing of such data may be adopted**, thereby ensuring that the interference is limited to what is strictly necessary. The need for such safeguards is all the greater where personal data is subject to automated processing [...]."

"177. To that effect, Article 45(2)(a) of the GDPR states that, in its assessment of the adequacy of the level of protection in a third country, the Commission is, in particular, to take account of '**effective and enforceable data subject rights**' for data subjects whose personal data are transferred."

Interference should be limited to what is **strictly necessary** and should not compromise **the essence** of the fundamental rights to privacy and to the protection of personal data

In the view of the Court, **the limitations** on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data **transferred from the European Union to that third country**, which the Commission assessed in Decision 2016/1250, are **not** circumscribed in a way that satisfies requirements that are **essentially equivalent** to those required under EU law, by **the principle of proportionality,** in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary (paragraphs 184 and 185).

The Court points out that Section 702 of the FISA "**does not indicate any limitations on the power it confers to implement surveillance programmes**" (paragraph 180).

The Court highlights that "(a)s regards the monitoring programmes based on E.O. 12333, it is clear from the file before the Court that **that order does not confer rights which are enforceable against the US authorities in the court**s either." (paragraph 182).

The Court adds "PPD-28, with which the application of the programmes referred to in the previous two paragraphs must comply, allows for "bulk" collection ... of a relatively large volume of signals intelligence information or data under circumstances where the Intelligence Community cannot use an identifier associated with a specific target ... to focus the collection', as stated in a letter from the Office of the Director of National Intelligence to the United States Department of Commerce and to the International Trade Administration from 21 June 2016, set out in Annex VI to the Privacy Shield Decision. That possibility, which allows, in the context of the surveillance programmes based on E.O. 12333, access to data in transit to the United States without that access being subject to any judicial review, **does not, in any event, delimit in a sufficiently clear and precise manner the scope of such bulk collection of personal data**." (paragraph 183)

Transfers of personal data as **interference**, requiring compliance with Article 47 of the Charter

"186. [A]s regards **Article 47 of the Charter**, which also contributes to the required level of protection in the European Union, compliance with which must be determined by the Commission before it adopts an adequacy decision pursuant to Article 45(1) of the GDPR, it should be noted that the first paragraph of Article 47 requires everyone whose rights and freedoms guaranteed by the law of the Union are violated to have the **right to an effective remedy before a tribunal** in compliance with the conditions laid down in that article. According to the second paragraph of that article, everyone is entitled to a hearing by an independent and impartial tribunal."

"188. To that effect, Article 45(2)(a) of the GDPR requires the Commission, in its assessment of the adequacy of the level of protection in a third country, to take account, in particular, of '**effective administrative and judicial redress** for the data subjects whose personal data are being transferred'. Recital 104 of the GDPR states, in that regard, that the third country 'should ensure **effective independent data protection supervision** and should provide for cooperation mechanisms with the Member States' data protection authorities', and adds that 'the data subjects should be provided with **effective and enforceable rights and effective administrative and judicial redress**'."

Transfers of personal data **as interference**, requiring compliance with Article 8(3) of the Charter

In this regard, it is worth recalling that, in addition to the requirements under Article 47 of the Charter, also the requirements under **Article 8(3) of the Charter** shall be considered.

The right to supervision by an independent authority is enshrined as a specific element of the right to protection of personal data in Article 8(3) of the Charter and in Article 16(2) TFEU. Interpreting and applying Article 8(3) of the Charter, the CJEU has insisted on the "complete" independence of DPAs. In this regard, see, among others, the Opinion 1/15, EU-Canada PNR Agreement, at paragraph 229: "*In accordance with the settled case-law of the Court, the guarantee of the independence of such a supervisory authority, the establishment of which is also provided for in Article 16(2) TFEU, is intended to ensure the effectiveness and reliability of the monitoring*

of compliance with the rules concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. The establishment of an independent supervisory authority is therefore an essential component of the protection of individuals with regard to the processing of personal data (judgments of 9 March 2010, Commission v Germany, C-518/07, EU:C:2010:125, paragraph 25; of 8 April 2014, Commission v Hungary, C-288/12, EU:C:2014:237, paragraph 48; and of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 41)."

Effective **judicial and administrative redress,** *Schrems II*

"191. In that regard, the Commission found, in recital 115 of the Privacy Shield Decision, that 'while individuals, including EU data subjects, ... have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered'. Thus, as regards E.O. 12333, the Commission emphasised, in recital 115, the lack of any redress mechanism. [...]"

"192. Furthermore, as regards both the surveillance programmes based on Section 702 of the FISA and those based on E.O. 12333, it has been noted in paragraphs 181 and 182 above that neither PPD-28 nor E.O. 12333 grants data subjects rights actionable in the courts against the US authorities, from which it follows that data subjects have no right to an effective remedy."

The Court holds that the **Ombudsperson mechanism** referred to in that decision does not provide data subjects with any cause of action before a body which offers **guarantees substantially equivalent** to those required by EU law, such as to ensure both **the independence** of the Ombudsperson provided for by that mechanism and **the existence of rules empowering the Ombudsperson to adopt decisions that are binding** on the US intelligence services. (paragraphs 195-197)

4

REPLIES TO QUESTIONS

1 When does a **transfer to a third country** within the meaning of Chapter V of the GDPR (Chapter IV of Directive 95/46) take place? What criteria has the CJEU used to determine the existence of a transfer? What is the overall data protection regime applicable to transfers?

Transfer of personal data to a third country, *Lindqvist*

Mrs Lindqvist was charged with breach of the Swedish data protection legislation for **publishing on her internet site personal data on a number of people** working with her on a voluntary basis in a parish of the Swedish Protestant Church. In criminal proceedings before it, the referring court (Göta Court of Appeal) raised preliminary ruling questions. It sought, among others, to establish **whether Ms Lindqvist had carried out a transfer** of data **to a third country** within the meaning of Directive 95/46/EC.

The Court held that "there is **no 'transfer [of data] to a third country**' within the meaning of Article 25 of Directive 95/46 where **an individual in a Member State loads personal data onto an internet page** which is **stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country.**" (paragraph 71).

(i) Absence of definition in the law:

"56. Directive 95/46 does not define the expression '**transfer to a third country**' in Article 25 or any other provision, including Article 2."

(ii) Still, the Court provides several criteria:

"57. In order to determine **whether loading personal data onto an internet page constitutes a 'transfer'** of those data to a third country within the meaning of Article 25 of Directive 95/46 merely because it makes them accessible to people in a third country, it is necessary to take account both of **the technical nature of the operations** thus carried out and of **the purpose and structure of Chapter IV of that directive** where Article 25 appears."

One must therefore take into account:

(a) Firstly, pointing out to the technical nature of the operations carried out

"59. **Under the procedures for use of the internet available to individuals like Mrs Lindqvist during the 1990s**, the author of a page intended for publication on the internet

transmits the data making up that page to **his hosting provider**. **That provider** manages the computer infrastructure needed to **store those data** and **connect the server hosting the site to** the internet. That allows the subsequent transmission of those data to anyone who connects to the internet and seeks access to it. The computers which constitute that infrastructure may be located, and indeed often are located, in one or more countries other than that where the hosting provider is established, without its clients being aware or being in a position to be aware of it."

"60. It appears from the court file that, in order to obtain the information appearing on the internet pages on which Mrs Lindqvist had included information about her colleagues, an internet user would not only have to **connect to the internet** but **also personally carry out the necessary actions to consult those pages**. In other words, Mrs Lindqvist's internet pages did not contain the technical means to send that information **automatically to people** who did not intentionally seek access to those pages."

"61. It follows that, in circumstances such as those in the case in the main proceedings, personal data which appear on the computer of a person in a third country, coming from a person who has loaded them onto an internet site, were **not directly transferred** between those two people but through the computer infrastructure of the hosting provider where the page is stored".

> *(b) Secondly, a **case-by-case assessment** is necessary, which takes into consideration the **intentions of the legislature** (purpose and structure of the transfers provisions), as well as **the consequences of the qualification** of the data processing as transfer to third countries*

"62. It is in that light that it must be examined **whether the Community legislature intended**, for the purposes of the application of Chapter IV of Directive 95/46, to include within the expression '**transfer [of data] to a third country**' within the meaning of Article 25 of that directive activities such as those carried out by Mrs Lindqvist. It must be stressed that the fifth question asked by the referring court concerns **only those activities and not those carried out by the hosting providers.**"

"67. Chapter IV of Directive 95/46 contains no provision concerning **use of the internet**. In particular, it does not lay down criteria for deciding whether operations carried out by **hosting providers** should be deemed to occur in the **place of establishment of the service** or at its **business address** or in the **place where the computer or computers constituting the service's infrastructure are located.**"

"68. **Given, first, the state of development of the internet** at the time Directive 95/46 was drawn up and, second, **the absence, in Chapter IV, of criteria applicable to use of the internet,** one cannot presume that the Community legislature intended the expression 'transfer [of data] to a third country' to cover **the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page**, even if those data are thereby made accessible to persons in third countries with the technical means to access them."

"69. If Article 25 of Directive 95/46 were interpreted to mean that there is 'transfer [of data] to a third country' every time that personal data are loaded onto an internet page, that transfer would necessarily be a **transfer to all the third countries** where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive

would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet."

"70. Accordingly, it must be concluded that Article 25 of Directive 95/46 is to be interpreted as meaning that operations such as **those carried out by Mrs Lindqvist** do not as such constitute a 'transfer [of data] to a third country'. It is thus unnecessary to investigate whether an individual from a third country has accessed the internet page concerned or whether the server of that hosting service is physically in a third country."

Transfer of personal data to a third country, *Schrems*

*a) **Technical nature of the operations** of the transfer:*

The judgment concerns the transfer of personal data carried out by Facebook Ireland, a subsidiary of Facebook Inc whereby "[s]ome or all of the **personal data of Facebook** Ireland's **users who reside in the European Union is transferred to servers** belonging to Facebook Inc. that are **located in the United States, where it undergoes processing.**" (paragraph. 27)

"45. [T]he operation consisting in **having personal data transferred from a Member State to a third country** constitutes, in itself, **processing of personal data** within the meaning of Article 2(b) of Directive 95/46 (see, to this effect, judgment in Parliament v Council and Commission, C-317/04 and C-318/04, EU:C:2006:346, paragraph 56) carried out in a Member State. That provision defines 'processing of personal data' as 'any operation or set of operations which is performed upon personal data, whether or not by automatic means' and mentions, by way of example, 'disclosure by transmission, dissemination or otherwise making available'."

*b) **Legal requirements applicable to** transfers: **not limited to Chapter IV** of Directive 95/46 (**now Chapter V** of the GDPR):*

"46. Recital 60 in the preamble to Directive 95/46 states that transfers of personal data to third countries may be effected only **in full compliance with the provisions adopted by the Member States pursuant to the directive**. In that regard, **Chapter IV** of the directive, in which Articles 25 and 26 appear, has set up a regime intended to ensure that the Member States oversee transfers of personal data to third countries. That regime **is complementary to the general regime set up by Chapter II of the directive laying down the general rules on the lawfulness of the processing of personal data** (see, to this effect, judgment in Lindqvist, C-101/01, EU:C:2003:596, paragraph 63).

Transfer of personal data to a third country (pursuant to **an international agreement**), *PNR Opinion*

The European Union and Canada negotiated an **agreement on the transfer and processing**

of Passenger Name Record data (PNR agreement) which was signed in 2014. The Council of the European Union then requested the European Parliament adecision on the conclusion of the agreement envisaged. Upon receiving the request, the European Parliament decided to refer the matter to the CJEU in order to ascertain whether the envisaged agreement was compatible with the Treaties. The envisaged agreement allows the **systematic and continuous transfer of PNR data** of all air passengers to a Canadian authority with a view of using, retaining and possibly transferring this data subsequently to other authorities in Canada (further processing) and to other countries (onward transfer), for the purpose of combating terrorism and serious transnational crime. On 26 July 2017, the CJEU delivered its opinion on the compatibility of the **international agreement** with the Charter of Fundamental Rights of the European Union, and, in particular, with provisions related to respect for private life and the protection of personal data.

Transfer to a third country, *Schrems II*

*a) **Legal aspects** of the transfer:*

"86. The possibility that the **personal data transferred between two economic operators for commercial purposes** might undergo, at the time of the transfer or thereafter, **processing for the purposes of public security, defence and State security** by the authorities of that third country c**annot remove that transfer from the scope of the GDPR**." (see also paragraphs 87, 88).

"89. [...] Article 2(1) and (2) of the GDPR must be interpreted as meaning that that regulation applies to the **transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective** of whether, at the time of that transfer or thereafter, that data is **liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.**"

In this regard, see also judgment of 6 October 2020, ***Privacy International*, C-623/17**, which **confirms this approach** (see in particular at paragraphs 35, 39, 44 and 49. Paragraph 44 states in particular "[...] according to the settled case-law of the Court, although it is for the Member States to define their essential **security interests** and to adopt appropriate measures to ensure their internal and external security, **the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from their obligation to comply with that law.** [...]"

*b) **Legal regime** of transfers: **not only Chapter IV** of Directive 95/46 (**now Chapter V** of the GDPR):*

"82. Under Article 2(1) of the GDPR, that regulation applies to the **processing of personal data** wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Article 4(2) of that regulation defines '**processing**' as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means' and

mentions, by way of example, 'disclosure by transmission, dissemination or otherwise making available', but **does not distinguish between operations which take place within the European Union and those which are connected with a third country. Furthermore, the GDPR subjects transfers of personal data to third countries to specific rules in Chapter V** thereof, entitled 'Transfers of personal data to third countries or international organisations', and also confers specific powers on the supervisory authorities for that purpose, which are set out in Article 58(2)(j) of that regulation."

2 What are the **powers available to the national supervisory authorities** in respect of the transfers? In case of: a) Safe Harbor; b) Standard Contractual Clauses (SCC); c) International Agreement.

Transfer to a third country: **Safe Harbor, powers available to the national supervisory authorities in respect of the transfers,** *Schrems*

The referring court asks, in essence, whether and to what extent Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that **a decision adopted pursuant to that provision, such as Decision 2000/520**, by which the Commission finds that a third country ensures an **adequate level of protection, prevents a supervisory authority** of a Member State, within the meaning of Article 28 of that directive, **from being able to examine the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data related to him which has been transferred** from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

"55. [T]he first subparagraph of Article 28(4) of Directive 95/46, under which the national **supervisory authorities are to hear 'claims** lodged by any person ... concerning the protection of his rights and freedoms in regard to the processing of personal data', does not provide for any exception in this regard where the Commission has adopted a decision pursuant to Article 25(6) of that directive."

"56. [I]t would be contrary to the system set up by Directive 95/46 and to the objective of Articles 25 and 28 thereof for a Commission decision adopted pursuant to Article 25(6) to have the effect of **preventing a national supervisory authority from examining a person's claim** concerning the protection of his rights and freedoms in regard to the processing of his personal data which has been or could be transferred from a Member State to the third country covered by that decision."

"57. [...] **Article 28 of Directive 95/46 applies, by its very nature, to any processing of personal data.** Thus, **even if the Commission has adopted a decision pursuant to Article 25(6)** of that directive, the national supervisory authorities, when hearing a claim lodged by a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him, must be able to **examine, with complete independence, whether the transfer of that data complies** with the requirements laid down by the directive."

"65. Where the national supervisory authority considers that the objections advanced by the person who has lodged with it a claim concerning the protection of his rights and freedoms in regard to the processing of his personal data are well founded, **that authority must**, in accordance with the third indent of the first subparagraph of Article 28(3) of Directive 95/46, read in the light in particular of Article 8(3) of the Charter, **be able to engage in legal proceedings.** It is incumbent upon the national legislature to provide for legal remedies **enabling the national supervisory authority concerned to put forward the objections which it considers well founded before the national courts in order for them, if they share its doubts as to the validity of the Commission decision, to make a reference for a preliminary ruling for the purpose of examination of the decision's validity.**"

The Court declared Article 3 of Decision 2000/520/EC to be invalid in so far as it denied national

supervisory authorities the powers which derive from Article 28 of Directive 95/46/EC, where a person puts forward matters that may call in question whether a Commission decision that has found that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals (paragraphs 102-104).

Powers available to the national supervisory authorities in respect of the transfers, *PNR Opinion*

"228. Under Article 8(3) of the Charter, compliance [of the international agreement] with the requirements stemming from Article 8(1) and (2) thereof is subject to **control by an independent authority.**"

It might be worth also recalling that the requirement for an **independent supervisory authority** was not fully met under the PNR agreement (see paragraphs 230-231: "230. In this instance, the first sentence of Article 10(1) of the envisaged agreement states that the data protection safeguards for the processing of PNR data will be subject to oversight by an 'independent public authority' or by an 'authority created by administrative means that exercises its functions in an impartial manner and that has a proven record of autonomy'. In so far as that provision provides that the oversight is to be carried out by an independent authority, it corresponds to the requirement set out in Article 8(3) of the Charter. By contrast, **its formulation in the alternative seems to permit the oversight to be carried out, partly or wholly, by an authority which does not carry out its tasks with complete independence**, but which is subordinate to a further supervisory authority, from which it may receive instructions, and which is therefore not free from any external influence liable to have an effect on its decisions.

231. In those circumstances, and as the Advocate General has observed in point 316 of his Opinion, Article 10 of the envisaged agreement does not guarantee in a sufficiently clear and precise manner that the oversight of compliance with the rules laid down in that agreement relating to the protection of individuals with regard to the processing of PNR data will be carried out by an independent authority, within the meaning of Article 8(3) of the Charter.

Transfer to a third country: adequate level of protection, as provided under SCC, **powers available to the national supervisory authorities** in respect of the transfers, *Schrems II*

"146. Article 4 of the SCC Decision, read in the light of recital 5 of Implementing Decision 2016/2297, supports the view that **the SCC Decision does not prevent the competent supervisory authority from suspending or prohibiting**, as appropriate, a transfer of personal data to a third country pursuant to the standard data protection clauses in the annex to that decision. In that regard, as is apparent from the answer to the eighth question, **unless there is a valid Commission adequacy decision, the competent supervisory authority is required, under Article 58(2)(f) and (j) of the GDPR, to suspend or prohibit such a transfer**, if, in its view and **in the light of all the circumstances of that transfer**, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has

required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer."

"147. As regards the fact, underlined by the Commissioner, that transfers of personal data to such a third country may result in the supervisory authorities in the various Member States adopting divergent decisions, it should be added that, as is clear from Article 55(1) and Article 57(1)(a) of the GDPR, the task of enforcing that regulation is conferred, in principle, on **each supervisory authority on the territory of its own Member State**. Furthermore, in order to avoid divergent decisions, Article 64(2) of the GDPR provides for **the possibility for a supervisory authority which considers that transfers of data to a third country must, in general, be prohibited, to refer the matter to the European Data Protection Board (EDPB) for an opinion**, which may, under Article 65(1)(c) of the GDPR, adopt a binding decision, in particular where a supervisory authority does not follow the opinion issued."

3 What is meant by an **adequate level of protection**? In case of: a) transfer to a third country; b) in particular, as provided by Safe Harbor (and by Privacy Shield); c) in particular, as provided by Standard Contractual Clauses (SCC).

Transfer to a third country: **adequate level of protection,** *Schrems*

"74. It is clear from the express wording of Article 25(6) of Directive 95/46 that it is **the legal order of the third country** covered by the Commission decision that must ensure an adequate level of protection. Even though the means to which that third country has recourse, in this connection, for the purpose of ensuring such a level of protection **may differ** from those employed within the European Union in order to ensure that the requirements stemming from Directive 95/46 read in the light of the Charter are complied with, those means must nevertheless prove, in practice, **effective** in order to ensure protection **essentially equivalent** to that guaranteed within the European Union."

"75. [W]hen examining the level of protection afforded by a third country, the Commission is obliged to assess **the content of the applicable rules in that country resulting from its domestic law or international commitments and the practice designed to ensure compliance with those rules**, since it must, under Article 25(2) of Directive 95/46, take account of all the circumstances surrounding a transfer of personal data to a third country."

Transfer to a third country: **adequate level of protection, as provided under Decision 2000/520/EC, Safe Harbor,** *Schrems*

*a) The **international commitments and practice** designed to ensure an essential equivalent level of protection in the case before the Court of Justice, nature and scope*

"79. The Commission found in Article 1(1) of **Decision 2000/520** that the **principles set out in Annex I thereto, implemented in accordance with the guidance provided by the FAQs set out in Annex II**, ensure an adequate level of protection for personal data transferred from the European Union to organisations established in the United States. It is apparent from that provision that both those **principles and the FAQs** were **issued by the United States Department of Commerce.**"

"80. An organisation adheres to the safe harbour principles on the basis of a system of self-certification, as is apparent from Article 1(2) and (3) of Decision 2000/520, read in conjunction with FAQ 6 set out in Annex II thereto."

"81. Whilst recourse by a third country to a **system of self-certification** is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46 that the third country concerned must **ensure an adequate level of protection 'by reason of its domestic law or ... international commitments**', the reliability of such a system, in the light of that requirement, is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights, in particular the right to respect for private life and the right to protection of personal data, to be

identified and punished in practice."

"82. In the present instance, by virtue of the second paragraph of Annex I to Decision 2000/520, the safe harbour principles are '**intended for use solely by US organisations receiving personal data from the European Union** for the purpose of qualifying for the safe harbour and the **presumption of "adequacy" it creates**'. Those principles are therefore applicable solely **to self-certified United States organisations receiving personal data from the European Union [...]**."

*b) **Relationship** of Safe Harbor principles **with the US legal order***

"84. Under the fourth paragraph of Annex I to Decision 2000/520, the applicability of the safe harbour principles may be limited, in particular, 'to the extent necessary to meet national security, public interest, or law enforcement requirements' and 'by statute, government regulation, or case-law that create conflicting obligations or explicit authorisations, provided that, in exercising any such authorisation, an organisation can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorisation'."

"85. In this connection, Decision 2000/520 states in Part B of Annex IV, with regard to the limits to which the safe harbour principles' applicability is subject, that, **'[c]learly, where US law imposes a conflicting obligation, US organisations whether in the safe harbour or not must comply with the law'."**

"86. Thus, **Decision 2000/520 lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles**, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them."

*c) **Conclusion** taking into account the above relationship and the assessment of the relevant aspects of the third country legal order*

"96. [I]n order for the Commission to adopt a decision pursuant to Article 25(6) of Directive 95/46, it must find, duly stating reasons, that the third country concerned **in fact ensures, by reason of its domestic law or its international commitments**, a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order, a level that is apparent in particular from the preceding paragraphs of the present judgment."

"97. However, the Commission did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments."

"98. Consequently, **without there being any need to examine the content of the safe harbour principles**, it is to be concluded that Article 1 of Decision 2000/520 fails to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of the Charter, and that it is accordingly invalid."

Transfer to a third country: adequate level of protection - as provided by an **international agreement**, *PNR Opinion*

"120. To the extent that the assessments that follow relate to the compatibility of the envisaged agreement with the right to the protection of personal data, enshrined in both **Article 16(1) TFEU** and **Article 8 of the Charter**, the Court will refer solely to the second of those provisions. Although both of those provisions state that everyone has the right to the protection of personal data concerning him or her, only **Article 8 of the Charter** lays down in a more specific manner, in paragraph 2 thereof, the conditions under which such data may be processed."

"122. Since the PNR data therefore includes information on identified individuals, namely air passengers flying between the European Union and Canada, the various forms of processing to which, under the envisaged agreement, that data may be subject, namely its transfer from the European Union to Canada, access to that data with a view to its use or indeed its retention, affect the fundamental right to respect for private life, guaranteed in **Article 7 of the Charter.**"

"123. Furthermore, the processing of the PNR data covered by the envisaged agreement also falls within the scope of **Article 8 of the Charter** because it constitutes the processing of personal data within the meaning of that article and, accordingly, must necessarily satisfy the data protection requirements laid down in that article."

"134. That right to the protection of personal data requires, inter alia, that the high level of protection of fundamental rights and freedoms conferred by EU law **continues where personal data is transferred from the European Union to a non-member country**. Even though **the means** intended to ensure such a level of protection [in this case, the international agreement] may differ from those employed within the European Union in order to ensure that the requirements stemming from EU law are complied with, those means must nevertheless prove, in practice, effective in order to ensure protection essentially equivalent to that guaranteed within the European Union."

Conclusion on the validity of the international agreement taking into account the above relationship and the assessment of the relevant aspects of the third country legal order

"232. In the light of all the foregoing considerations, it must be held that:

(2) the envisaged agreement is incompatible with Articles 7, 8 and 21 and Article 52(1) of the Charter in so far as it does not preclude the transfer of sensitive data from the European Union to Canada and the use and retention of that data;
(3) the envisaged agreement must, in order to be compatible with Articles 7 and 8 and Article 52(1) of the Charter:

a) determine in a clear and precise manner the PNR data to be transferred from the European Union to Canada;

b) provide that the models and criteria used in the context of automated processing of PNR data will be specific and reliable and non-discriminatory; provide that the database

used will be limited to those used by Canada in relation to the fight against terrorism and serious transnational crime;

c) save in the context of verifications in relation to the pre-established models and criteria on which automated processing of PNR data is based, make the use of that data by the Canadian Competent Authority during the air passengers' stay in Canada and after their departure from that country, and any disclosure of that data to other authorities, subject to substantive and procedural conditions based on objective criteria; make that use and that disclosure, except in cases of validly established urgency, subject to a prior review carried out either by a court or by an independent administrative body, the decision of that court or body authorising the use being made following a reasoned request by those authorities, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime;

d) limit the retention of PNR data after the air passengers' departure to that of passengers in respect of whom there is objective evidence from which it may be inferred that they may present a risk in terms of the fight against terrorism and serious transnational crime;

e) make the disclosure of PNR data by the Canadian Competent Authority to the government authorities of a third country subject to the condition that there be either an agreement between the European Union and that third country equivalent to the envisaged agreement, or a decision of the Commission, under Article 25(6) of Directive 95/46, covering the authorities to which it is intended that PNR data be disclosed;

f) provide for a right to individual notification for air passengers in the event of use of PNR data concerning them during their stay in Canada and after their departure from that country, and in the event of disclosure of that data by the Canadian Competent Authority to other authorities or to individuals; and

g) guarantee that the oversight of the rules laid down in the envisaged agreement relating to the protection of air passengers with regard to the processing of PNR data concerning them will be carried out by an independent supervisory authority."

See also EDPS Guidelines on Proportionality (at pages 18, 26, 30, 34) and The EDPS quick-guide to necessity and proportionality.

Transfer to a third country: adequate level of protection - as **provided by standard contractual clauses** - assessment, *Schrems II*

"102. The referring court also seeks to ascertain **what factors** should be taken into consideration for the purposes of determining the adequacy of the level of protection where personal data is transferred to a third country pursuant to **standard data protection clauses** adopted under Article 46(2)(c) of the GDPR."

"103. In that regard, although that provision **does not list the various factors** which must be taken into consideration for the purposes of assessing the adequacy of the level of protection to be observed in such a transfer, Article 46(1) of that regulation states that data subjects must be afforded **appropriate safeguards, enforceable rights and effective legal remedies**."

"105. [...] Article 46(1) and Article 46(2)(c) of the GDPR must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to **standard data protection clauses** are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration **both the contractual clauses** agreed between the controller or processor established in the European Union and the recipient of the transfer established in the third country concerned **and, as regards any access by the public authorities of that third country to the personal data transferred, the relevant aspects of the legal system of that third country**, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation."

Transfer to a third country: adequate level of protection - as provided by the **Privacy Shield**, *Schrems II*

a) The international commitments and practice designed to ensure an essential equivalent level of protection in the case before the Court of Justice, nature and scope

"163. The Commission found, in Article 1(1) of the Privacy Shield Decision, that the United States ensures an adequate level of protection for personal data transferred from the Union to organisations in the United States under the **EU-US Privacy Shield**, the latter being comprised, inter alia, under Article 1(2) of that decision, of the Principles issued by the US Department of Commerce on 7 July 2016 as set out in Annex II to the decision and the official representations and commitments contained in the documents listed in Annexes I and III to VII to that decision."

b) Relationship of Privacy Shield principles with the US legal order

"164. [T]he Privacy Shield Decision also states, in paragraph I.5. of Annex II, under the heading 'EU-U.S. Privacy Shield Framework Principles', that adherence to those principles **may be limited, inter alia, 'to the extent necessary to meet national security, public interest,**

or law enforcement requirements'. Thus, that decision lays down, as did Decision 2000/520, that those requirements have primacy over **those principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard the principles without limitation where they conflict with the requirements and therefore prove incompatible with them.**"

c) Conclusion taking into account the above relationship and the assessment of the relevant aspects of the third country legal order

On all those grounds (see paragraphs 168-200), the Court declares Decision 2016/1250 (Privacy Shield) **invalid** (paragraphs 199-201).

4

What is meant by transfers of personal data as **interference**?

a) with Articles 7 and 8 of the Charter;

b) requiring compliance with inter alia Articles 47 and 52 of the Charter in order for such interference to be lawful;

c) and which should be limited to what is strictly necessary and should not compromise the essence of the fundamental rights to privacy and to the protection of personal data

Transfers of personal data as **interference** with Articles 7 and 8 of the Charter, requiring compliance with Article 52 of the Charter in order for such interference to be lawful, *Schrems*

"87. In the light of the general nature of the derogation set out in the fourth paragraph of Annex I to Decision 2000/520, that decision thus **enables interference, founded on national security and public interest requirements or on domestic legislation of the United States,** with the fundamental rights of the persons whose personal data is or could be transferred from the European Union to the United States."

As regards the impossibility of **justifying such interference**, the Court, first of all, observed that EU legislation involving interference with the fundamental rights guaranteed by Articles 7 and 8 of the Charter must lay down clear and precise rules governing the scope and application of a measure and imposing minimum safeguards, so that the **persons, whose personal data is concerned** have sufficient **guarantees** enabling their data to be effectively protected against the risk of abuse and against any unlawful access to and use of those data. The need for such safeguards is all the greater when personal data is subjected to **automatic processing** and where there is a significant risk of **unlawful access to this data** (paragraph 91).

Interference should be limited to what is **strictly necessary** and should not compromise the **essence** of the fundamental rights to privacy and to the protection of personal data

Protection of the fundamental rights to respect for private life and to the protection of personal data requires derogations and limitations in relation to the protection of personal data to apply **only in so far as is strictly** necessary. (paragraph 92)

Legislation is **not limited to what is strictly necessary** where it authorises, on a **generalised basis**, storage of all the personal data of all the persons whose data has been transferred from the European Union **without any differentiation, limitation or exception** being made in the light of the objective pursued, and **without an objective criterion being laid down by which to determine the limits** of the access of the public authorities to the data, and of the subsequent use of this data, for **purposes which are specific, strictly restricted and capable of justifying the interference** which both access to this data and their use entail. (paragraph 93)

Legislation permitting public authorities to have **access on a generalised basis** to the content of electronic communications compromises **the essence** of the fundamental right to respect for private life. (paragraph 94)

Legislation not providing for any possibility for an individual to pursue **legal remedies** in order to have access to personal data relating to him, or to obtain the **rectification or erasure** of such data, does not respect **the essence** of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. (paragraph 95)

Transfers of personal data **as interference** with **Articles 7 and 8** of the Charter, *PNR Opinion*

"124. As the Court has held, the communication of personal data to a third party, such as a public authority, constitutes **an interference** with the fundamental right enshrined in **Article 7** of the Charter, whatever the subsequent use of the information communicated. The same is true of the retention of personal data and access to that data with a view to its use by public authorities. In this connection, it does not matter whether the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way on account of that interference."

"126. Those operations also constitute an interference with the fundamental right to the protection of personal data guaranteed in **Article 8** of the Charter since they constitute the processing of personal data."

Transfers of personal data **as interference,** requiring compliance with **Article 52** of the Charter in order for such interference to be lawful

"138. [I]n accordance with the first sentence of **Article 52(1)** of the Charter, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. Under the second sentence of Article 52(1) of the Charter, subject to the principle of **proportionality**, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others."

"139. It should be added that the requirement that **any limitation** on the exercise of fundamental rights must be provided for by law implies that the legal basis which permits the interference with those rights must itself define the scope of the limitation on the exercise of the right concerned. [...]"

"140. As regards observance of the principle of **proportionality**, the protection of the fundamental right to respect for private life at EU level requires, in accordance with settled case-law of the Court, that derogations from and limitations on the protection of personal data should apply only in so far as is strictly necessary."

"141. In order to satisfy that requirement, the legislation in question which entails the interference

must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose data has been transferred have **sufficient guarantees** to protect effectively their personal data against the risk of abuse. It must, in particular, indicate in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is **strictly necessary**."

An interference should not compromise the essence of the fundamental rights to privacy and to the protection of personal data, *PNR Opinion*

The Court points out the essence of the fundamental rights at stake under, respectively, Article 7 and 8 of the Charter.

"150. As regards **the essence of the fundamental right to respect for private life**, enshrined in **Article 7** of the Charter, even if PNR data may, in some circumstances, reveal very specific information concerning the private life of a person, the nature of that information is limited to certain aspects of that private life, in particular, relating to air travel between Canada and the European Union.

As for **the essence of the right to the protection of personal data**, enshrined in **Article 8** of the Charter, the envisaged agreement limits, in Article 3, the purposes for which PNR data may be processed and lays down, in Article 9, rules intended to ensure, inter alia, the security, confidentiality and integrity of that data, and to protect it against unlawful access and processing."

Necessity of the interference, *PNR Opinion*

"154. As regards **the necessity of the interferences** entailed by the envisaged agreement, it is necessary to check, in accordance with the case-law cited in paragraphs 140 to 141 of this Opinion, whether they are limited to what is strictly necessary and, in that context, whether that agreement lays down clear and precise rules governing the scope and application of the measures provided for."

The Court considered in this regard:

(1) The PNR data covered by the envisaged agreement:

(i) Whether the envisaged agreement is sufficiently precise as regards the PNR data to be transferred (paras 155-162) and concludes (para 163) that "In those circumstances, as regards the PNR data to be transferred to Canada, headings 5, 7 and 17 of the Annex to the envisaged agreement do not delimit in a sufficiently clear and precise manner the scope of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter;"

(ii) [Whether the transfers of personal data concerns] sensitive data (paras 164-166) and concludes (para 167) that "Having regard to the assessments set out in the two preceding paragraphs, it must be held that Articles 7, 8 and 21 and Article 52(1) of the Charter preclude both the transfer of sensitive

data to Canada and the framework negotiated by the European Union with that non-member State of the conditions concerning the use and retention of such data by the authorities of that non-member State."

(2) Whether the data transferred are **subject to automated processing** (paras 168-174, *PNR Opinion*).

See in this regard in particular:

"168. As stated in paragraphs 130 to 132 of this Opinion and as the Advocate General has noted in point 252 of his Opinion, the PNR data transferred to Canada is mainly intended to be subject to **analyses by automated means**, based on pre-established models and criteria and on cross-checking with various databases."

"169. The assessment of the risks to public security presented by air passengers is carried out [...] by means of automated analyses of the PNR data before the arrival of those air passengers in Canada. Since those analyses are carried out on the basis of unverified personal data and are based on pre-established models and criteria, they necessarily present some **margin of error**, as, inter alia, the French Government and the Commission conceded at the hearing."

"170. As stated in point 30 of the Opinion of the EDPS on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (OJ 2008 C 110, p. 1), to which the EDPS referred in his answer to the questions posed by the Court, that **margin of error** appears to be significant."

(3) The **purposes** for which PNR data may be processed (paras 175-181)

(4) The Canadian **authorities covered** by the envisaged agreements (paras 182-185)

(5) The **air passengers concerned** (paras 186-189)

(6) The **retention and use** of PNR data (paras 190-211)

(7) The **disclosure** of PNR data (paragraph 214, *PNR Opinion*)

In this regard, the Court clarified the data protection requirements concerning **onward transfers**:

"214. [...] it must be recalled that **a transfer of personal data** from the European Union to a non-member country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union. That **same requirement applies** in the case of the disclosure of PNR data by Canada to **third countries**, referred to in Article 19 of the envisaged agreement, **in order to prevent the level of protection provided for in that agreement from being circumvented by transfers of personal data to third countries and to ensure the continuity of the level of protection afforded by EU law** [...]. In those circumstances, such **disclosure** requires the existence of either an agreement between the European Union and the non-member country concerned equivalent to that agreement, or a decision of the Commission, under Article 25(6) of Directive 95/46, finding that the third country ensures an adequate level of protection within the meaning of EU law and covering the authorities to which it is intended PNR data be transferred."

Transfers of personal data as **interference**, requiring compliance with Article 47 of the Charter, *Schrems II*

"186. [A]s regards **Article 47 of the Charter**, which also contributes to the required level of protection in the European Union, compliance with which must be determined by the Commission before it adopts an adequacy decision pursuant to Article 45(1) of the GDPR, it should be noted that the first paragraph of Article 47 requires everyone whose rights and freedoms guaranteed by the law of the Union are violated to have the **right to an effective remedy before a tribunal** in compliance with the conditions laid down in that article. According to the second paragraph of that article, everyone is entitled to a hearing by an independent and impartial tribunal."

"188. To that effect, Article 45(2)(a) of the GDPR requires the Commission, in its assessment of the adequacy of the level of protection in a third country, to take account, in particular, of '**effective administrative and judicial redress** for the data subjects whose personal data are being transferred'. Recital 104 of the GDPR states, in that regard, that the third country 'should ensure **effective independent data protection supervision** and should provide for cooperation mechanisms with the Member States' data protection authorities', and adds that 'the data subjects should be provided with **effective and enforceable rights and effective administrative and judicial redress**'."

Transfers of personal data **as interference**, requiring compliance with Article 8(3) of the Charter, *PNR Opinion*

In this regard, it is worth recalling that, in addition to the requirements under Article 47 of the Charter, also the requirements under **Article 8(3) of the Charter** shall be considered.

The right to supervision by an independent authority is enshrined as a specific element of the right to protection of personal data in Article 8(3) of the Charter and in Article 16(2) TFEU. Interpreting and applying Article 8(3) of the Charter, the CJEU has insisted on the "complete" independence of DPAs. In this regard, see, among others, the Opinion 1/15, EU-Canada PNR Agreement, at paragraph 229: "*In accordance with the settled case-law of the Court, the guarantee of the independence of such a supervisory authority, the establishment of which is also provided for in Article 16(2) TFEU, is intended to ensure the effectiveness and reliability of the monitoring of compliance with the rules concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. The establishment of an independent supervisory authority is therefore an essential component of the protection of individuals with regard to the processing of personal data (judgments of 9 March 2010, Commission v Germany, C-518/07, EU:C:2010:125, paragraph 25; of 8 April 2014, Commission v Hungary, C-288/12, EU:C:2014:237, paragraph 48; and of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraph 41).*"

5 When and subject to which conditions **have SCC been considered valid** by the CJEU as a tool for transfer of personal data?

Transfer to a third country: adequate level of protection - **validity of standard contractual clauses/SCC decision**, *Schrems II*

*a) On the **difference between adequacy decisions and SCC decision***

"129. [S]uch a **standard clauses decision differs from an adequacy decision** adopted pursuant to Article 45(3) of the GDPR, which seeks, following an examination of the legislation of the third country concerned taking into account, *inter alia*, the relevant legislation on national security and public authorities' access to personal data, to find with binding effect that a third country, a territory or one or more specified sectors within that third country ensures an adequate level of protection and that the access of that third country's public authorities to such data does not therefore impede transfers of such personal data to the third country. Such an adequacy decision can therefore be adopted by the Commission only if it has found that the third country's relevant legislation in that field does in fact provide all the necessary guarantees from which it can be concluded that that legislation ensures an adequate level of protection."

"130. By contrast, in the case of a **Commission decision adopting standard data protection clauses, such as the SCC Decision**, in so far as such a decision does not refer to a third country, a territory or one or more specific sectors in a third country, **it cannot be inferred from Article 46(1) and Article 46(2)(c) of the GDPR that the Commission is required, before adopting such a decision, to assess the adequacy of the level of protection ensured by the third countries** to which personal data could be transferred pursuant to such clauses."

"131. [A]ccording to Article 46(1) of the GDPR, in the absence of a Commission adequacy decision, **it is for the controller or processor** established in the European Union to provide, *inter alia*, **appropriate safeguards**. Recitals 108 and 114 of the GDPR confirm that, where the Commission has not adopted a decision on the adequacy of the level of data protection in a third country, the controller or, where relevant, the processor 'should **take measures to compensate** for the lack of data protection in a third country by way of appropriate safeguards for the data subject'."

See also the EDPB "Recommendations 01/2020 **on measures that supplement transfer tools** to ensure compliance with the EU level of protection of personal data", available at: **edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf (europa.eu)** and submitted to public consultation until 21 December 2020.

The EDPB has also adopted the "Recommendations 02/2020 on the **European Essential Guarantees** for surveillance measures", available at: **edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf (europa.eu)**

which updates and integrates the Article 29 Working Party working document on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data.

*b) Relationship of **SCC with third country legal framework - possible need for other clauses or additional safeguards that supplement SC***

"132. Since by their **inherently contractual nature** standard data protection clauses **cannot bind the public authorities of third countries** [...] but that Article 44, Article 46(1) and Article 46(2)(c) of the GDPR, interpreted in the light of Articles 7, 8 and 47 of the Charter, require that the **level of protection** of natural persons guaranteed by that regulation is not undermined, it may prove **necessary to supplement the guarantees contained in those standard data protection clauses**. In that regard, recital 109 of the regulation states that 'the possibility for the controller ... to use standard data-protection clauses adopted by the Commission ... should [not] prevent [it] ... from **adding other clauses or additional safeguards**' and states, in particular, that the controller 'should be encouraged to provide **additional safeguards** ... that **supplement** standard [data] protection clauses'."

*c) Responsibility of the **controller or processor, or, failing that, of the competent supervisory authority***

"134. [T]he contractual mechanism provided for in Article 46(2)(c) of the GDPR is based on the **responsibility of the controller or his or her subcontractor** established in the European Union and, in the alternative, of the **competent supervisory authority**. It is therefore, above all, for that controller or processor to verify, **on a case-by-case basis** and, **where appropriate, in collaboration with the recipient of the data**, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, **additional safeguards** to those offered by those clauses."

"135. Where the **controller or a processor** established in the European Union is not able to take adequate **additional measures** to guarantee such protection, the **controller or processor** or, failing that, **the competent supervisory authority**, are required to **suspend or end** the transfer of personal data to the third country concerned. That is the case, **in particular**, where the law of that third country imposes on the recipient of personal data from the European Union obligations which are contrary to those clauses and are, therefore, capable of impinging on the contractual guarantee of an adequate level of protection against access by the public authorities of that third country to that data."

d) Conclusion on the validity of SCC

The Court examines the **validity of Decision 2010/87 (on SCC)**. The Court considers that the validity of that decision is not called into question by the mere fact that the standard data protection clauses in that decision **do not, given that they are contractual in nature, bind the authorities of the third country to which data may be transferred**. That validity depends on whether the decision includes **effective mechanisms** that make it possible, **in practice**, to **ensure compliance** with the level of protection required by EU law and that transfers of personal data pursuant to such clauses are **suspended or prohibited** in the event of the **breach of such clauses** or it being **impossible to honour them** (paragraph 137).

The Court finds that Decision 2010/87 **establishes such mechanisms** (in that regard, see para 138-146).

6 What is meant by **effective judicial and administrative redress**?

Effective **judicial and administrative redress**, *PNR Opinion*

"226. As regards air passengers' **right to redress**, Article 14(2) of the envisaged agreement provides that Canada is to ensure that any individual who is of the view that their rights have been infringed by a decision or action in relation to their PNR data may seek **effective judicial redress,** in accordance with Canadian law, or such other remedy which may include compensation."

Effective **judicial and administrative redress,** *Schrems II*

"191. In that regard, the Commission found, in recital 115 of the Privacy Shield Decision, that 'while individuals, including EU data subjects, ... have a number of avenues of redress when they have been the subject of unlawful (electronic) surveillance for national security purposes, it is equally clear that **at least some legal bases that U.S. intelligence authorities may use (e.g. E.O. 12333) are not covered**'. Thus, as regards E.O. 12333, the Commission emphasised, in recital 115, the **lack of any redress mechanism.** [...]"

"192. Furthermore, as regards both the surveillance programmes based on Section 702 of the FISA and those based on E.O. 12333, it has been noted in paragraphs 181 and 182 above that neither PPD-28 nor E.O. 12333 grants data subjects **rights actionable in the courts** against the US authorities, from which it follows that data subjects have no right to an effective remedy."

The Court holds that the **Ombudsperson mechanism** referred to in that decision does not provide data subjects with any cause of action before a body which offers **guarantees substantially equivalent** to those required by EU law, such as to ensure both **the independence** of the Ombudsperson provided for by that mechanism and **the existence of rules empowering the Ombudsperson to adopt decisions that are binding** on the US intelligence services. (paragraphs 195-197)

7 What is meant by the duty to **notify to the data subject** the transfer of personal data?

Duty to **notify** the transfer to the data subject, *PNR Opinion*

"The Court held that the fundamental right to respect for private life, enshrined in Article 7 of the Charter of Fundamental Rights of the European Union, "means that the person concerned may be certain that his personal data are processed in a correct and lawful manner" (paragraph 219).

The Court pointed out in that regard that air passengers must be **notified of the transfer** of their PNR data to the third country concerned and of the use of those data **as soon as that information is no longer liable to jeopardise the investigations** being carried out by the government authorities referred to in the envisaged agreement." (paragraph 220; see also paragraphs 221-225)

8 Are specific safeguards needed in case of transfer of personal data subject to **automated processing** or involving **sensitive data?**

Transfer of data subject to **automated processing** and of **sensitive data**, *PNR Opinion*

"141. The need for such safeguards is all the greater where personal data is subject to automated processing (see paras 168-174).

Those considerations apply particularly where the protection of the particular category of personal data that is sensitive data is at stake." (see also paragraphs 164-167).

"168. As stated in paragraphs 130 to 132 of this Opinion and as the Advocate General has noted in point 252 of his Opinion, the PNR data transferred to Canada is mainly intended to be subject to analyses by automated means, based on pre-established models and criteria and on cross-checking with various databases."

"169. The assessment of the risks to public security presented by air passengers is carried out [...] by means of automated analyses of the PNR data before the arrival of those air passengers in Canada. Since those analyses are carried out on the basis of unverified personal data and are based on pre-established models and criteria, they necessarily present some margin of error, as, inter alia, the French Government and the Commission conceded at the hearing."

"170. As stated in point 30 of the Opinion of the EDPS on the draft Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes (OJ 2008 C 110, p. 1), to which the EDPS referred in his answer to the questions posed by the Court, that margin of error appears to be significant."

9 What are the data protection requirements in case of onward transfer of personal data?

Onward transfers, *PNR Opinion*

125. "[B]**oth the transfer** of PNR data from the European Union to the Canadian Competent Authority **and the framework negotiated by the European Union with Canada of the conditions concerning the retention of that data, its use and its subsequent transfer** to other Canadian authorities, Europol, Eurojust, judicial or police authorities of the Member States or indeed to authorities of third countries, which are permitted, inter alia, by Articles 3, 4, 6, 8, 12, 15, 16, 18 and 19 of the envisaged agreement, constitute interferences with the right guaranteed in Article 7 of the Charter."

"214. In this connection, it must be recalled that a transfer of personal data from the European Union to a non-member country may take place only if that country ensures a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the

European Union. That **same requirement applies in the case of the disclosure of PNR data by Canada to third countries**, referred to in Article 19 of the envisaged agreement, in order to prevent the level of protection provided for in that agreement from being circumvented by transfers of personal data to third countries and to ensure the continuity of the level of protection afforded by EU law (see, by analogy, judgment of 6 October 2015, Schrems, C-362/14, EU:C:2015:650, paragraphs 72 and 73). In those circumstances, such disclosure requires the existence of either an agreement between the European Union and the non-member country concerned equivalent to that agreement, or a decision of the Commission, under Article 25(6) of Directive 95/46, finding that the third country ensures an adequate level of protection within the meaning of EU law and covering the authorities to which it is intended PNR data be transferred."

edps.europa.eu

@EU_EDPS

EDPS

European Data Protection Supervisor