Council of the European Union

Brussels, 7 September 2017
(OR. en)

11931/17

LIMITE

JUR 407
JAI 761
DATAPROTECT 135
AVIATION 110
RELEX 729
CDN 5
ENFOPOL 397
EUROJUST 134
CATS 89

INFORMATION NOTE

From:	Legal Service
To:	Permanent Representatives Committee (Part 2)
Subject:	Draft EU-Canada PNR Agreement - Opinion 1/15 of the Court of Justice on its compatibility with the Treaties

I. INTRODUCTION

1. On 26 July 2017, the Court of Justice (Grand Chamber) delivered its Opinion in Case 1/15 on the envisaged agreement between the Union and Canada providing a legal framework for the transfer of Passenger Name Record ("PNR") data from European air carriers to Canada and for further processing of the PNR data by Canadian authorities in order to combat terrorism and serious transnational crime (the Agreement).

2. The Opinion was requested by the European Parliament pursuant to Article 218(11) TFEU, prior to giving its consent to the conclusion of the Agreement. The Agreement was signed in 2014 but has not yet been concluded by the EU and is not yet in force.

3. The two questions raised by the European Parliament were worded as follows:

   - is the Agreement compatible with the provisions of the Treaties (Article 16 TFEU) and the Charter of Fundamental Rights of the European Union (Articles 7, 8 and Article 52(1)) as regards the right of individuals to the protection of personal data?

   - do point (d) of the second subparagraph of Article 82(1) and Article 87(2)(a) TFEU constitute the appropriate legal basis for the act of the Council concluding the Agreement or must this act be based on Article 16 TFEU?

4. In its Opinion, the Court addressed the question of the legal basis for the Council decision on the conclusion of the Agreement and the question of the compatibility of the Agreement with the Charter of Fundamental Rights of the European Union (the Charter). On the first question, the Court found that the Council decision to conclude the Agreement should be based jointly on Articles 16(2) and 87(2)(a) TFEU. On the second question, the Court found that the Agreement does not fully comply with the rights to respect for private life and to protection of personal data guaranteed by Articles 7, 8 and 52(1) of the Charter. In particular, the Court holds that the Agreement breaches these provisions because it does not preclude the transfer, use and retention of sensitive data. In addition to the need to exclude sensitive data, the Court lists seven distinct points which the Agreement must include, specify, limit or guarantee in order to be compatible with the Charter. As a consequence, the Agreement cannot be concluded and enter into force and the Union will need to inform Canada thereof. The Agreement should be revised in order to comply with the Court's Opinion. This will require the agreement of Canada. In addition, all Council decisions relating to the revised Agreement will need to be adopted on the double legal basis indicated by the Court.

II. ANALYSIS OF THE COURT'S OPINION AND ITS CONSEQUENCES

Appropriate legal basis for the Council decision

5. The Court recalled its case-law on the choice of legal basis, in particular on the conditions for a dual legal basis (paragraphs 76 to 78) and brought new elements with regard to the interpretation of Article 2a of Protocol 22 (on the position of Denmark).

6. On the legal basis of the Council decision concluding the draft Agreement, the Court combined the (opposing) views defended by the Council and the European Parliament. It held that the legal basis should be both a sectoral Justice and Home Affairs ("JHA") provision (Council's approach), namely Article 87(2)(a) TFEU on police cooperation, and the horizontal provision for data protection - Article 16(2) TFEU (European Parliament's approach). The Court rejected the position of the Council to include also Article 82 TFEU (judicial cooperation in criminal matters) in the legal basis. It confirmed the Advocate General's view that none of the provisions of the draft agreement refer to facilitating cooperation between judicial authorities since the Canadian Competent Authority under the Agreement does not constitute a judicial authority, nor does it constitute an equivalent authority (paragraph 103).

7. The Court considered that the Agreement pursues two objectives and has two components: first, public security through the transfer and use of PNR data for fighting against terrorism and serious transnational crime; second, the protection of PNR data as personal data, in particular through the "*establishment of a system consisting of a body of rules intended to protection personal data and with which Canada has undertaken comply* (…)" (paragraph 89). The Court admits that the public security objective is the sole justification for the transfer and use of PNR data (paragraph 91).

Nevertheless, the data protection component of the agreement is equally important for the purposes of the legal basis. This is because the transfer of personal data to a third country "*is lawful only if there are rules in that country which ensure a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the EU*", and because that the Agreement "*largely consists of detailed rules*" on the data protection-compatible use of PNR data for public security.

8. On that basis, the Court concluded that the public security component is not predominant compared to the component of the protection of PNR data and that these two components are inextricably linked and "*must, therefore, both be considered to be fundamental in nature*" (paragraph 94).

9. The Court went on to check whether a JHA (Title V) legal basis can be combined with Article 16 TFEU. Different voting rules within the Council pursuant to Protocol 22 (Denmark) could make those legal bases incompatible and thus impossible to combine in a single decision.[1] The Council had interpreted the Protocols to the effect that the concerned Member States always vote on Article 16 TFEU measures, making this provision incompatible with a Title V legal basis because of the different voting rights within the Council. The Court had a different reading making it possible to combine those legal bases.

10. With regard to Ireland and the UK, the Court found that the question does not arise in the case at hand because Ireland and the UK have opted-in, under Protocol 21, to the draft Council decision concluding the agreement. Thus, Protocol 21 will not affect the voting rules within the Council on the draft Council decision, as Ireland and the UK will participate in the adoption of the draft Council decision (unless they do not opt in to the relevant decision in the three-month period from the recommendation or proposal).

[1] Both Protocols 21 and 22 contain provisions for the non-participation of those Member States in the adoption of Title V measures, but no provision on the non-participation in the adoption (i.e. the voting) of Article 16 TFEU measures. Instead, Protocols 21 and 22 each contain provisions to the effect that those Member States are not bound by data protection rules under Article 16 TFEU which relate to data processing under Title V where such Member States are not bound by the Title V provisions themselves because they have not opted-in (UK and Ireland) or because they have a Title V opt-out (Denmark).

11. With regard to Denmark, which, pursuant to Protocol 22, has a "compulsory" opt-out from Title V new legal acts, the Court held, in line with the Advocate General's view, that Denmark cannot vote in Article 16 TFEU measures by which it is not bound. The Court made a systematic interpretation of Protocol 22 which prevailed over the textual interpretation defended by the Council[2] (paragraphs 114 and 115).

The compatibility of the Agreement with European Union Fundamental Rights

12. The Court focused its Opinion on the compatibility of the Agreement with fundamental rights, notably the right to respect for private life (Article 7 of the Charter) and the right to protection of personal data (Article 8 of the Charter) (see *inter alia*, paragraph 120 of the Opinion). The Court found that the transfer of PNR data to Canada and its subsequent use by the Canadian authorities as well as its subsequent transfer to Europol, Eurojust or authorities of third countries, constitute an interference with those fundamental rights. The Court then examined the justification for the interferences on the basis of the criteria laid down in Article 52(1) of the Charter as interpreted by its case law on data protection, such as *Schecke*[3], *Schrems*[4], *Digital Rights Ireland*[5] and *Tele2*[6] as well as *S. and Marper*[7] which is a leading case of the European Court of Human Rights (see paragraph 141 of the Opinion).

---

2 Article 2a of Protocol 22, which concerns Article 16 TFEU, only refers to Article 2 of Protocol 22, which deals with the provisions of Title V being inapplicable to Denmark. It does not refer to Article 1 of Protocol 22 about the voting, therefore, in the view of the Council, allowing Danemark to vote on Article 16 measures.

3 Cases C-92/09 and C-93/09

4 Case C-362/14

5 Joined Cases C-293/12 and C-594/12.

6 Joined Cases C-203/15 and C-698/15.

7 ECtHR, 4 December 2008, *S. and Marper v. the United Kingdom*, CE: ECHR:2008:1204JUD003056204.

(a) The basis laid down by 'law' for the processing of PNR data

13. The Court acknowledged that the basis of the interference with fundamental rights can be based on the Agreement which can be regarded as '*law*' within the meaning of Articles 8(2) and 52(1) of the Charter, even though the Agreement does not constitute a *'legislative act'*. The Court also recalled, in paragraph 146 of its Opinion, that a '*law*' must meet the requirements as to accessibility and predictability - in line with the case law of the European Court of Human Rights on the 'quality of the law' - and that it has not in any way been argued in this case that the Agreement does not meet those requirements.

14. It should also be noted that the Advocate General's opinion on this aspect (paragraphs 190 to 193 of the Advocate General's opinion) provides for further guidelines on the requirements of the 'law', in particular on the 'quality of the law', in the light of the case law of the European Court of Human Rights which may be of interest in the context of pending legislative files where the issue has arisen.

(b) The objective of general interest and respect for the essence of the fundamental rights in question

15. The Court considered that the interference can be justified by the pursuit of the objective of public security in the context of the fight against terrorism and serious transnational crime, which constitutes an objective of general interest of the Union within the meaning of Article 52(1) of the Charter and that it does not adversely affect the essence of the two fundamental rights (privacy and data protection) within the meaning of Article 52(1) of the Charter, since it only reveals very specific information limited to certain aspects of private life and the Agreement contains rules relating to purpose limitation, security, confidentiality and integrity of personal data.

(c) The appropriateness of the processing of the PNR data having regard to the objective

16. The Court, relying in particular on the Commission's findings that analysing PNR data before the arrival of passengers "*largely facilitates and expedites security and border control checks*" and on figures provided by the Canadian authorities that the processing of PNR data enabled to arrest 178 persons from among the 28 million travellers between the Union and Canada, concluded that the processing of the PNR data is appropriate having regard to the objective of ensuring public security (paragraphs 152 and 153 of the Opinion).

(d) The necessity of the interferences entailed by the Agreement

17. The Court, applying its case law on data protection, recalls that the interferences must be limited to what is strictly necessary and the Agreement should lay down clear and precise rules governing the scope and application of the measures provided for (paragraphs 140, 141 and 154 of the Opinion).

18. Like in other data protection cases, the 'necessity' test is the most challenging test to pass. In this case, the Court identified several shortcomings following a strict judicial review[8] which concretely led the Court to go into every single detail of the Agreement, including each individual PNR data heading in the Annex to the Agreement. This 'necessity test', like in previous recent data protection cases (*Digital Rights Ireland*, *Schrems* or *Tele2*), which is analysed by the Court in this case at length (from paragraph 154 to 217 of the Opinion) is therefore not met on several grounds. For the purpose of this note, the Council Legal Service will mainly focus on the shortcomings identified by the Court which will need to be corrected if a renegotiation of the Agreement takes place.

[8] On the strict test of judicial review of the legislature's discretion for extensive and serious interferences with data protection rights, see paragraph 48 of Case C-293/12 *Digital Rights Ireland*.

However, it should be noted that, on several occasions, the Court came to the conclusion that specific provisions of the Agreement met the test and therefore that the provisions at stake were sufficiently clear and precise and did not exceed the limits of what is strictly necessary (see e.g. paragraphs 159, 161, 176, 177, 180, 185, 189, 197, 198, 209 and 227).

19. Firstly, the Court considered that heading 5 (available frequent flyer information and benefit information), heading 7 (all available contact information) and heading 17 (general remarks) of the 19 PNR data headings do not define in a sufficiently clear and precise manner the PNR data to be transferred (see paragraphs 155 to 163 of the Opinion).

20. Secondly, the Court considered that some of those headings could be sensitive data (e.g. special meal requests), in the sense that they may reveal notably ethnic origin, political opinions, religious beliefs or health condition, processing of which is prohibited in the EU PNR Directive (Directive 2016/681 currently being transposed by Member States). Since there is no justification for the processing of such sensitive data which should be based on grounds other than the protection of public security, the transfer of such sensitive data to Canada is not possible.

21. Thirdly, the Court considered that automated processing based on pre-established models and criteria and on cross-checking with various databases (i.e. profiling) should be better framed, and monitored in the context of the joint review under the Agreement. In this regard, the Court considered that the pre-established models and criteria should be specific and reliable making it possible to arrive at results targeting individuals who might be under a 'reasonable suspicion' of participation in terrorist offences or serious transnational crime and should be non-discriminatory (paragraph 172 of the Opinion). Like in the Union data protection legislation in force, the Court requires that any positive result obtained following the automated processing should be subject to an individual re-examination by non-automated means before an individual measure adversely affecting the air passengers concerned is adopted. Consequently, such a measure may not be based solely and decisively on the result of automated processing of PNR data (paragraph 173 of the Opinion).

22. Fourthly, the Court criticised the lack of precision and clarity in Article 3(5)(a) and (b) of the Agreement as to the processing of PNR data on a case-by-case basis for other purposes (ensuring the oversight or accountability of the public administration or complying with the subpoena or warrant issued or an order made by a court) than those inherent in the Agreement.

23. Fifthly, concerning the retention and use of PNR data, the Court made a distinction between the retention and use of PNR data before the arrival of air passengers up until their departure from Canada (first category) and after their departure from Canada (second category). It also made a distinction within the first category between the lawfulness of retention versus the lawfulness of use of PNR data by public authorities, depending on the situation of air passengers.These concrete distinctions giving rise to different results as to whether the 'necessity test' is met, have horizontal implications and constitute a nuanced application of the main principles laid down by the Court in *Digital Rights Ireland*[9] and *Tele2*[10] cases on retention of electronic communications personal data. Indeed, the principle remains that the necessity test is not met where a law provides for compulsory retention in a generalised manner of all persons by all means and all (traffic) data with no differentiation, limitation or exception to the objective pursued and where a relationship between the data which must be retained and a threat to public security is not established[11].

[9] Joined Cases C-293/12 and C-594/12
[10] Joined Cases C-203/15 and C-598/15
[11] See paragraphs 105 and 106 of *Tele 2* in Joined Cases C-203/15 and C-698/15.

(i) The retention and use of PNR data before the arrival of air passengers, during their stay in Canada and on their departure

24. As regards the first category of PNR data (i.e. before the arrival of air passengers, during their stay in Canada and on their departure), the Court recognised that because the necessary connection between the PNR data and security checks and border control checks is established, the systematic retention of all PNR data for all passengers travelling between the Union and Canada up until their departure from Canada (including during their stay in that third country) and without a prior authorisation by a court or by an independent administrative body, does not exceed the limits of what is strictly necessary (paragraph 197 of the Opinion).

25. As regards the use of the PNR data, the Court accepted the systematic use of those data before the passengers enter the territory of Canada, for the purpose of verifying the reliability and topicality of the pre-established models and criteria on which the automated processing of that data is based, or of defining new models and criteria for such processing (paragraph 198 of the Opinion). However, the Court introduced a further limitation on the use of the PNR data during the passengers' stay in Canada which must be based on new circumstances justifying that use which requires rules laying down the substantive and procedural conditions governing that use (paragraph 200 of the Opinion) including a prior review carried out either by a court or by an independent administrative body, except in cases of validly established urgency (paragraph 202 of the Opinion). The Court concluded that where there is objective evidence from which it may be inferred that the PNR data of one or more air passengers might make an effective contribution to combating terrorist offences and serious transnational crime, the use of that data does not exceed the limits of what is strictly necessary (paragraph 201 of the Opinion).

(ii) The retention and use of PNR data after the air passengers' departure from Canada

26. As regards the second category of PNR data (i.e. after the air passengers' departure from Canada), the Court rejected the systematic retention of those data, because there would not appear to be, once the passengers have left Canada, a connection - even a merely indirect connection - between the PNR data and the objective pursued since no risk has been identified on their arrival in Canada and up to their departure (paragraph 205 of the Opinion). The continued storage of PNR data of all air passengers after their departure from Canada for the purposes of possibly accessing that data, regardless of whether there is any link with serious crime is not limited to what is strictly necessary, according to the Court. However, in specific cases with objective evidence, PNR data of certain air passengers which may present a risk in terms of the fight against terrorism and serious transnational crime, may be stored and the use of such data should be subject as a general rule, to a prior review by an independent body or court. The Court merely applied the criteria it had laid down in *Digital Rights Ireland* and *Tele 2*. In this case, the Court did not specify what could be the specific cases where objective evidence is identified from which it may be inferred that certain air passengers may present a risk in terms of the fight against terrorism and serious transnational crime. This suggests that the Court does not require that those air passengers whose PNR data may be stored after their departure from Canada, should have the status of suspects subject to a police or a criminal investigation. One could argue that the limitation criteria laid down in the *Tele 2* judgment, would be relevant in this context and that the assessment by Canadian authorities could relate to a 'group' of air passengers (e.g. excluding certain areas of origin of those passengers) likely to be involved, in one way or another, in a serious crime, or air passengers who could, for other reasons, contribute, through their data being retained, to fighting crime. However, those criteria should be objective and non-discriminatory and should be applied to air passengers by non-automated means, in specific cases, on the basis of objective evidence.

27. It is noteworthy that the Court accepted that a retention of PNR data of certain air passengers presenting a risk, for a period of five years and subject to an irreversible destruction of the data after that period, does not exceed what is strictly necessary (paragraphs 209 and 210 of the Opinion). A contrario, this confirms that masking the data while it is technically feasible to unmask them, does not amount to an irreversible destruction of the data.

28. Sixthly, the Court rejected the possibility for Canadian authorities to disclose PNR data to other Canadian government authorities and to government authorities of third countries. As regards the latter, the Court referred to the *Schrems* case[12] and pointed out the risk of circumvention of the rules on transfers of personal data to third countries. The Court criticised the fact that the Canadian Competent Authority has a discretionary power to assess the level of data protection in third countries and logically required that an agreement with the Union or a Commission adequacy decision are in place with those third countries in order to allow the disclosure of PNR data to those third countries and thereby ensure that the 'level of data protection in those third countries is essentially equivalent to that guaranteed in the Union'[13]. Contrary to what some parties to the Court proceedings had suggested, the Court does not make any distinction on the type of instruments used to ensure an essentially equivalent level of data protection, be it by way of a Commission adequacy decision (implementing act) or by a Union agreement pursuant to Article 218 TFEU.

29. Seventhly, the Court held that Article 12(3) of the Agreement which allows Canada to make any disclosure of information to individuals as exceeding the limits of what is strictly necessary.

---

12 Case C-362/04.

13 Requirement developed by the Court for the first time in the above-mentioned *Schrems* case.

30. Eighthly, the Court underlined the importance of the information rights for air passengers as they are necessary to enable them to exercise their fundamental rights to request access and if appropriate, rectification of their PNR data (paragraph 220 of the Opinion) which are rights explicitly mentioned in Article 8(2) of the Charter. The Court then required to introduce an obligation for the Canadian competent authorities to notify air passengers individually on the transfer and use of the PNR data, in cases where Canadian authorities either use PNR data during passengers' stay in Canada or retain PNR data after the passengers' departure from Canada as well as in cases of disclosure to other government authorities or individuals, noting that in those cases, a general information on the relevant website is not sufficient. However, in line with its case law and the data protection legislation in force, that information must be provided only once it is no longer liable to jeopardise the investigations being carried out by the government authorities (paragraph 224 of the Opinion).

31. Ninthly, the right to judicial redress in Canada is found to be an effective judicial protection for air passengers covered by the Agreement (paragraph 227 of the Opinion). However, the oversight of PNR data which may also be by an authority created by administrative means exercising its functions in an impartial manner and that has a proven record of autonomy, does not meet the high standard of 'complete independence' required by Article 16(2) TFEU and Article 8(3) of the Charter as interpreted by the case law of the Court on the data protection supervisory authorities cited in paragraph 229 of the Opinion.

III. CONCLUSIONS AND FOLLOW-UP

Conclusions for the EU-Canada PNR Agreement

32. As the Opinion was rendered pursuant to Article 218(11) TFEU, it has not led to the annulment of an act of the Council but it is clear that the Agreement in its current form cannot be concluded by the Union and cannot enter into force.[14] It should be recalled that currently the Agreement has been signed by both Canada and the Union. The Union will need to inform Canada that it is not possible for the Union to conclude (ratify) the Agreement in is its current form.[15]

33. It is assumed that both the Union and Canada are ready to revise the Agreement to comply with the requirements set out by the Court in its Opinion of 26 July 2017. The Council should invite the Commission to explore this intention with Canada. Following the confirmation that both the Union and Canada are ready to revise the text of the Agreement, the Council should invite the Commission to come forward with an appropriate recommendation authorising the opening of the negotiations for the revision of the draft Agreement, pursuant to Article 218 (3) TFEU.[16] The negotiating directives pursuant to Article 218 (4) TFEU could consist of the list of issues provided by the Court in its Opinion of 26 July 2017[17].

---

14 Pursuant to the second sentence of Article 218(11) TFEU, "[*w*]*here the opinion of the Court is adverse, the agreement may not enter into force unless it is amended or the Treaties are revised*".

15 Under Article 18 of the 1969 Vienna Convention of the Law of Treaties the Union (and Canada) are following their signature of the Agreement under the international legal obligation not to defeat the object and purpose of the Agreement but this obligation ends when the Union is not able to ratify the Agreement.

16 Because the Council has already adopted a decision signing the Agreement, the previous negotiating authorisation adopted pursuant to Article 218 (3) TFEU is no longer in force. This situation is therefore not comparable with the draft EU accession agreement to the ECHR, which the Union had not yet signed when the Court of Justice issued its opinion 2/13: See Information Note from the Legal Service, 5227/15, 14 January 2015, paragraph 23.

17 Opinion 1/15, point 232 (2) and (3).

34. Provided that a revised text for the Agreement can be agreed on, a new Council decision on signature and, if necessary, provisional application can be adopted pursuant to Article 218 (5) TFEU. Pursuant to Article 218 (6) (a) TFEU, the Council can then adopt a decision on conclusion of the revised Agreement once the consent of the European Parliament has been obtained.

35. These three aforementioned Council decisions will need to be adopted on the joint substantive legal bases indicated by the Court in its Opinion 1/15[18], and will exclude participation (voting) by Denmark. The right of the UK and Ireland to opt in under Protocol 21 will not be affected. Furthermore, pursuant to Article 218 (10) TFEU, the European Parliament shall be immediately and fully informed at all stages of the procedure.

Horizontal conclusions

(a) Consequences as regards the appropriate legal basis

36. There is no practical consequence for the Agreement of adding Article 16 TFEU as a second legal basis in the Council decision concluding the Agreement since Denmark will continue not to take part in that instrument and will, as judged by the Court, not vote for the adoption of possible future Council decisions in relation to a renegotiated agreement with Canada.

37. However, there are some horizontal consequences for other Union legal acts in the JHA field, notably with respect to the application of Protocol 22 to Denmark.

38. Firstly, one should analyse the consequences of the systematic interpretation of Article 2a of Protocol 22 which the Court followed in the PNR Canada case in other cases where a legal act is based solely on Article 16 TFEU and relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of police cooperation and judicial cooperation in criminal matters.

[18] Article 16(2) and Article 87(2) (a) TFEU.

In the Council Legal Service's view, if the afore-mentioned activities are at least partly covered by acts of the Union in the field of police cooperation and judicial cooperation in criminal matters adopted before the entry into force of the Treaty of Lisbon (ex-third pillar acts) which, pursuant to Article 2 of Protocol 22, shall continue to be binding upon and applicable to Denmark unchanged, Denmark shall take part in (and therefore vote in) the adoption by the Council of the relevant legal act based solely on Article 16 TFEU.

39. Secondly, where other Union legal acts have as a sole justification a JHA objective but their contents largely consist of detailed data protection rules, Article 16 TFEU should be added to the JHA legal basis, like in the PNR Canada case. Where the JHA legal basis refers to the ordinary legislative procedure to be combined with the legal basis of Article 16 under the ordinary legislative procedure, the two legal bases are compatible and such a combination of legal bases will not change the voting rule as the UK and Ireland will continue to have their opt in/opt out rights under Protocol 21 and Denmark its opt-out under Protocol 22. However, where the JHA legal basis refers to a non-legislative procedure or a special legislative procedure (for example Council acting unanimously) which are not compatible procedures with the ordinary legislative procedure under Article 16 TFEU, two separate acts would need to be adopted using different voting rules within the Council.

40. Thirdly, where other Union legal acts have as a sole justification a JHA objective but their contents do not largely consist of detailed data protection rules which are then merely ancillary to the JHA rules, only the JHA legal basis as the "predominant" component of the legal act should be used. Currently, Regulation No 2016/794/EU (the "Europol Regulation") and the draft Eurojust Regulation[19] which are respectively based on Article 88 and 85 TFEU contain a body of data protection rules which could be regarded as an ancillary component of those Regulations which mainly consist of rules regulating the structure and operation of those JHA agencies.

[19] Council document 6643/15.

In that case, those Regulations would not need to be amended. Even if this view was not upheld and therefore if Article 16 TFEU was to be added, this would not affect the validity of those Regulations, since the adoption procedure within the Council would be the same (i.e. ordinary legislative procedure with application of opt-out/opt-in Protocols 21 and 22)[20].

41. Fourthly, as regards legal acts regulating data bases (such as VIS, SIS, Eurodac) which contain a substantial number of data protection provisions, a further analysis would need to be carried out by the Council Legal Service to determine whether Article 16 TFEU should be added to the JHA legal basis. This would in any event have neither practical consequences nor affect the validity of those legal acts which are adopted under the ordinary legislative procedure. The possible addition of Article 16 TFEU will indeed not give the right to vote to those Member States which do not or cannot participate in the relevant instrument.

(b) Consequences as regards compliance with fundamental rights in data retention schemes such as PNR data schemes

42. The other PNR agreements (PNR Australia[21] and PNR USA[22]) remain in force as long as they have not been challenged. Their validity could be challenged by means of a preliminary reference from a national court to the Court of Justice, pursuant to Article 267 TFEU. Even though those agreements have an expiration period (2019), they are automatically renewed if no notice is sent twelve months before the expiration date[23].

---

[20] An incorrect reference to a legal basis in a Union act is no more than a purely formal defect, unless it gave rise to irregularity in the procedure applicable to the adoption of that act (see, to that effect, Case 165/87 *Commission* v *Council* [1988] ECR 5545, paragraph 19, and Joined Cases C-184/02 and C-223/02 *Spain and Finland* v *Parliament and Council* [2004] ECR I-0000, paragraph 44).

[21] OJ 14.07.2012, L186, p. 4.

[22] OJ 11.08.2012, L215, p. 5.

[23] Article 26 of the PNR Australia and PNR USA Agreements.

Since those two agreements contain the same or similar shortcomings as those identified by the Court in its Opinion 1/15, they all need to be renegotiated. If the third country does not accept such a renegotiation, the Union should terminate those PNR agreements in accordance with the procedure provided for therein[24], on the ground that they do not comply with Union law.

43. The main substantial difficulty to overcome in those renegotiations as well as in the recently adopted PNR Directive to be implemented by Member States (except Denmark) before May 2018[25], is the retention and use of PNR data by law enforcement authorities after the air passengers have departed from the relevant territory and therefore after all border checks (entry/exit) have been carried out. In this particular situation, the Court requires a targeted retention limited to those passengers presenting a risk which needs to be evidenced. Furthermore, it is uncertain to what extent Canadian authorities (and the US and Australian authorities) would accept to change their domestic laws, in particular on the competent supervisory authority for non-Canadian air passengers wishing to exercise their rights of access and rectification.

44. In the case of the USA, it should be borne in mind that, were the PNR USA Agreement cease to apply, the Umbrella Agreement between the Union and USA which provides for a data protection framework in the field of police cooperation and judicial cooperation in criminal matters, which is already in force, would apply.

45. There may also be some further horizontal consequences with respect to the application of the 'necessity test' on possible future data bases retaining data of persons who cross a Union border and may not present a risk in terms of public security (e.g. non-EU residents who after visiting the Union return to their home country or EU residents returning to the EU after a visit in a third country) but whose data may be potentially useful in the future in relation to terrorist or other serious crimes.

---

[24] See the dispute resolution mechanisms respectively in Article 23 of the PNR Australia Agreement and Article 24 of the PNR USA Agreement and the termination clause in Article 25 of both Agreements.

[25] The obligation of Member States to implement the PNR Directive is not affected by this Opinion.

46. As regards the retention of electronic communications metadata, the Court made it clear, in particular in paragraphs 105 and 106 of the *Tele 2* judgment, that a legislation which covers, in a generalised manner, all subscribers and registered users and all means of electronic communication as well as all traffic data and provides for no differentiation, limitation or exception according to the objective pursued, exceeds the limits of what is strictly necessary for the pursuit of a public security objective. For the purposes of fighting terrorism and serious crime such electronic communications metadata retention legislation should establish a relationship between the data which must be retained and a threat to public security. In particular, it should be restricted to retention in relation to (i) data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or (ii) persons who could, for other reasons, contribute, through their data being retained, to fighting crime.

47. The more nuanced approach followed by the Court in the way these limitation criteria could be applied, for instance in paragraph 197 of the Opinion on the systematic retention of all PNR data until the departure of air passengers from Canada (limitation in time and in the categories of air passengers in relation to their entry and exit of the border), could open the way for a reflection on how to frame a future possible legislation requiring relevant operators to retain metadata of electronic communications by introducing limitations such as those relating to the geographical area and a group of persons likely to present a security risk coupled with a short retention period and more limited metadata. However, it is clear from the Opinion, in particular in its paragraphs 204 to 211, that a generalised retention of all metadata of electronic communications of the entire EU population without limitations, exceeds the limits of what is strictly necessary for the pursuit of the objective of public security.