To the President and Members of the Court of Justice of the European Union

In Opinion 1/15

REQUEST FOR AN OPINION

submitted pursuant to Article 218(11) TFEU by the

EUROPEAN PARLIAMENT

on the compatibility with the Treaties of the envisaged agreement between the European Union and Canada on the transfer and processing of passenger name record data

---

WRITTEN OBSERVATIONS OF IRELAND

Submitted by Eileen Creedon, Chief State Solicitor, Osmond House, Little Ship Street, Dublin 8, acting as Agent, accepting service via e-curia, assisted by David Fennelly BL.

Ireland has the honour to submit written observations in these proceedings, the subject of a request for an Opinion pursuant to Article 218(11) TFEU lodged by the European Parliament at the Court Registry on 30 January 2015.

I. Introduction

1. In its Request pursuant to Article 218(11) of the Treaty on the Functioning of the European Union ("**TFEU**"), the European Parliament ("**the Parliament**") has sought the Opinion of this Court on the compatibility with the Treaties of the envisaged agreement between the European Union and Canada on the transfer and processing of passenger name record data ("**the Agreement**"). In particular, the Parliament has sought the Court's opinion on the following questions:

> *Is the envisaged 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 protection of personal data?*
>
> *Do Article 82(1)(d) and Article 87(2)(a) TFEU constitute the appropriate legal basis for the act of the Council concluding the envisaged agreement or must that act be based on Article 16 TFEU?*

In these written observations, Ireland will address each of these questions in turn.

2. In respect of the first question (Section II), Ireland submits that the Agreement is compatible with Article 16 TFEU and Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union ("**the Charter**") as regards the right of individuals to protection of personal data.

3. In respect of the second question (Section III), Ireland submits that Article 82(1)(d) and Article 87(2)(a) TFEU constitute the appropriate legal basis for the act of the Council concluding the Agreement. In the context of matters properly falling within Title V of Part Three of the TFEU, on the area of freedom, security and justice, the effect of Protocol No. 21 to the TFEU is such that the choice of legal basis has a particular constitutional significance for Ireland.

II. The Compatibility of the Agreement with the Treaties and the Charter of Fundamental Rights

4. By its first question, the Parliament has asked whether the Agreement is compatible with Article 16 TFEU and Articles 7, 8 and 52(1) of the Charter of Fundamental Rights as regards the right of individuals to protection of personal data. The Parliament has submitted that there is legal uncertainty as to the compatibility of the Agreement, particularly in light of this Court's judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland, Seitlinger & Others* ("***Digital Rights Ireland***").[1]

5. By way of general comment, Ireland submits that the Agreement is much more limited in its nature and effects than Directive 2006/24/EC ("**the Data Retention Directive**") which was the subject of the Court's judgment in *Digital Rights Ireland*. In reviewing the Agreement, particularly by reference to the principles laid down in the Court's judgment in *Digital Rights Ireland*, it is important to have regard to certain important differences between the Agreement, on the one hand, and the Data Retention Directive, on the other.

6. First, the Data Retention Directive imposed an obligation on providers of publicly available electronic communications services or of public communications networks to retain a significant amount of data (including in particular traffic and location data) in respect of all users of electronic communications in order to ensure that the data were available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law. The Court found that the data, taken as a whole, might "allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments

[1] Judgment in *Digital Rights Ireland, Seitlinger & Others*, Joined Cases C-293/12 and C-594/12, EU:C:2014:238.

frequented by them".[2] The Directive applied to "all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives" and covered "all subscribers and registered users", thus entailing "an interference with the fundamental rights of practically the entire European population".[3] In contrast, the Agreement regulates the international transfer and use of a very specific and limited category of data, Passenger Name Record ("**PNR**") data, from air carriers to the Canadian Competent Authority, strictly for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious transnational crime. The number and category of persons to whom the Agreement applies, and the nature of the conclusions which could be drawn about their private lives by reason of the transfer and use of PNR data, is therefore significantly more limited than was the case under the Data Retention Directive.

7. Secondly, whereas the Data Retention Directive sought to harmonise the regime for data retention within the EU, and therefore involved a derogation "from the system of protection of the right to privacy established by Directives 95/46 and 2002/58",[4] the Agreement seeks to ensure that, in the context of transfer and use of PNR data for the purposes of combating terrorism and serious transnational crime, air carriers flying to Canada are not prevented from complying with their obligations under Canadian law and further that, in complying with Canadian law, they do so in a manner compatible with the rights to privacy and to protection of personal data under EU law. In this way, in practical terms, the Agreement involves an extension of the EU's regime for protection of personal data to the transfer of PNR data to Canada for the purposes of combating terrorism and serious transnational crime.

8. Nevertheless, insofar as the Agreement permits the transfer from the EU to Canada of PNR data, and its possible use by the Canadian Competent Authority, it is clear that the Agreement may constitute an interference with the right to privacy and the right to protection of personal data enshrined in Articles 7 and 8 of the Charter. Assuming for the

[2] Judgment in *Digital Rights Ireland*, EU:C:2014:238, paragraph 27.
[3] Judgment in *Digital Rights Ireland*, EU:C:2014:238, paragraph 56.
[4] Judgment in *Digital Rights Ireland*, EU:C:2014:238, paragraph 32.

purposes of these observations that the Agreement does indeed constitute an interference with Articles 7 and 8 of the Charter, the question that arises is whether this interference can be justified under Article 52(1) of the Charter which provides:

> *Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made 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.*

Ireland submits that the limitation on the exercise of Articles 7 and 8 of the Charter that the Agreement entails is capable of justification under Article 52(1) of the Charter.

9. First, insofar as the Agreement entails a limitation on the exercise of the rights in Article 7 and 8 of the Charter, Ireland submits that such a limitation is indeed "provided for by law". Contrary to the Parliament's submission, the concept of "law" in Article 52(1) of the Charter is not co-extensive with the notion of "legislative act" found in Article 289 TFEU. While the concept of "law" may indeed "be close to that adopted by the European Court of Human Rights",[5] the European Court of Human Rights, in the very judgment relied upon by the Parliament, has emphasised that the term "law" must be understood in its substantive rather than its formal sense and includes "both enactments of lower rank than statutes… and unwritten law", the latter being of particular relevance in common law jurisdictions such as Ireland.[6] In any event, the concept of "law" under Article 52(1) of the Charter must be interpreted and applied within the specific context of the European Union legal order. Insofar as international agreements are concerned, Article 216(2) TFEU provides that agreements concluded by the Union "are binding upon the institutions of the Union and on its Member States". In its jurisprudence, this Court has consistently affirmed that, from the time they come into force, international agreements form an integral part of EU law.[7] Therefore, for the purposes of European Union law, the concept of "law" in Article 52(1) of the Charter undoubtedly includes within its scope

[5] Opinion of Advocate General Cruz Villalon in *Digital Rights Ireland*, EU:C:2013:845, paragraph 56.
[6] *Kruslin v. France* (1990) 12 EHRR 547, at paragraph 29.
[7] Judgment in *Haegeman v Belgium*, 181/73, EU:C:1974:41, paragraph 5; Opinion of the Court (Full Court) in Opinion 2/13, C:2014:2454, paragraph 180.

international agreements concluded by the Union, such as the envisaged Agreement. Indeed, if, as the Parliament appears to suggest, the concept of "law" in Article 52(1) were strictly limited to "legislative acts" within the meaning of Article 289 TFEU, that concept would exclude the primary law of the Union, the Treaties, as well as other sources of law not enshrined in legislative acts which form part of the European Union legal order.

10. Secondly, insofar as the Agreement constitutes a limitation on the exercise of the rights in Article 7 and 8 of the Charter, Ireland submits that the Agreement respects the essence of those rights and notes the Parliament does not appear to suggest otherwise. In this regard, the conclusions of the Court at paragraphs 39 and 40 of its judgment in *Digital Rights Ireland* apply *a fortiori* to the Agreement at issue in these proceedings.[8]

11. Thirdly, Ireland submits that the Agreement, insofar as it limits the rights protected under Articles 7 and 8 of the Charter, complies with the principle of proportionality. In particular, the provisions of the Agreement "genuinely meet objectives of general interest recognised by the Union". In its judgment in *Digital Rights Ireland*, this Court confirmed that the fight against international terrorism in order to maintain international peace and security and the fight against serious crime in order to ensure public security both constitute objectives of general interest.[9] As is clear from the Preamble to the Agreement, the use of PNR data is "a critically important instrument" for pursuing these objectives.[10] In Ireland's view, the transfer and use of PNR data in accordance with the Agreement is both appropriate and necessary for attaining the objectives being pursued and the Agreement does not go beyond what is necessary in order to achieve these objectives.[11]

12. In assessing the criteria and safeguards provided for in the Agreement, particularly by reference to the principles laid down in the Court's judgment in *Digital Rights Ireland*, Ireland would once again emphasize the importance of taking into account the significant

[8] Judgment in *Digital Rights Ireland*, EU:C:2014:238, paragraphs 29-40.
[9] Judgment in *Digital Rights Ireland*, EU:C:2014:238, paragraph 42.
[10] Agreement, Preamble, paragraph 4.
[11] Judgment in *Digital Rights Ireland*, EU:C:2014:238, paragraph 49.

differences between the Agreement, on the one hand, and the Data Retention Directive, on the other. While Ireland acknowledges that the review of the EU legislature's discretion should be strict where interferences with fundamental rights are at issue, regard must be had to the international character of this Agreement which addresses the manner in which PNR data may be transferred and used in a third country (in this case, Canada) and which is necessarily the outcome of negotiations between the EU and that third country. This is particularly the case when it comes to matters of detail in the Agreement.

13. In its Request for an Opinion, the Parliament has identified a number of specific concerns in relation to the Agreement which it suggests give rise to serious doubts about the Agreement's compatibility with Article 16 TFEU and Articles 7, 8 and 52(1) of the Charter.

14. First, while it is true that the Agreement affects all persons flying to Canada, as submitted at paragraph 6 above, the Agreement applies to a very specific and limited category of data and to a very significantly smaller category of persons than that affected by the Data Retention Directive.

15. Secondly, in respect of the objective criteria limiting access to the PNR data by the Canadian Competent Authority, Ireland submits that Article 3 of the Agreement, along with other provisions of the Agreement, lay down clear and objective criteria which ensure that access to PNR data does not go beyond what is strictly necessary. In this respect, the Agreement stands in sharp contrast to the Data Retention Directive which, this Court found, did not expressly provide that access and use of the data in question was "strictly restricted to the purpose of preventing and detecting precisely defined serious offences or of conducting criminal prosecutions relating thereto".[12] In particular, Article 3(1) of the Agreement imposes an obligation to ensure that the Canadian Competent Authority processes PNR data received pursuant to the Agreement "strictly for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious offences". It is because the Agreement, by its very nature, is concerned with the

[12] Judgment in *Digital Rights Ireland*, EU:C:2014:238, paragraph 61.

regulation of the transfer and use of PNR data in Canada that the category of offences constituting "serious transnational crime" is defined by reference to Canadian law. Similarly, the fact that "the Canadian Competent Authority" is not defined in the Agreement itself but instead is the subject of a notification requirement under Article 30(2) does not deprive the criteria used of their clear and objective character.

16. Thirdly, while the Agreement does not specifically define the precise number of officials to whom access is restricted, it does impose a clear obligation on Canada to restrict access "to a limited number of officials specifically authorized by Canada" in Article 16(2) and to restrict disclosure to the circumstances satisfying the conditions set out in Article 18. Moreover, in accordance with Article 20 of the Agreement, air carriers transfer PNR data to the Canadian Competent Authority "exclusively on the basis of the push method". In contrast, this Court in *Digital Rights Ireland* found that the Data Retention Directive did "not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued".[13] It was in this specific context that the Court noted that the access by competent national authorities to data retained under the Directive was "not made dependent on a prior review carried out by a court or by an independent administrative body".[14] In Ireland's view, taking account of the range of safeguards protecting transfer and use of PNR data under the Agreement, the absence of a prior review mechanism in the Agreement is not such as to render the Agreement incompatible with the Charter.

17. Fourthly, it is the case, as the Parliament submits, that the Agreement does not require that the data be retained in the EU. The Agreement is after all designed to regulate the transfer and use of PNR data in Canada for the purpose of ensuring public security in the context of the fight against terrorism and serious transnational crime. Nevertheless, Article 5 of the Agreement provides that, subject to compliance with its provisions, "the Canadian Competent Authority is deemed to provide an adequate level of protection,

[13] Judgment in *Digital Rights Ireland*, EU:C:2014:238, paragraph 62.
[14] Judgment in *Digital Rights Ireland*, EU:C:2014:238, paragraph 62.

within the meaning of relevant European Union data protection law, for the processing and use of PNR data". An adequate level of protection does not necessarily require an equivalent level of protection in precisely the same form and framework as that provided under EU law. Nevertheless, Article 10 of the Agreement provides that the data protection safeguards in the Agreement "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 (the "overseeing authority")" while Article 14 of the Agreement provides for administrative and judicial redress. In Ireland's submission, these provisions ensure that compliance with the data protection safeguards is "subject to control by an independent authority" within the meaning of Article 8(3) of the Charter, as this term has been interpreted by this Court.[15]

18. Fifthly, insofar as the data retention period under Article 16 of the Agreement is concerned, Ireland submits that this does not go beyond what is strictly necessary within the overall context of this Agreement. Given the complex and challenging nature of investigations into terrorism and serious transnational crime, it may be some time after a journey has taken place before the law enforcement authorities need to access PNR data for the purposes of detecting, investigating or prosecuting such crime. While in some cases PNR data may be useful to law enforcement authorities on a real-time basis, in other cases, its value lies in being able to trace the travel patterns of persons reasonably suspected of being involved in terrorism and serious transnational crime on a specific earlier date or over a specific period of time. Moreover, while the retention period has been extended to 5 years under the Agreement, compared to 3.5 years under the 2005 agreement, the Agreement does so in circumstances where it provides for significantly enhanced protection for personal data: for example, in the form of the safeguards enshrined in Article 9 (Data security and integrity), Article 10 (Oversight), Article 11 (Transparency), Article 12 (Access for individuals), Article 13 (Correction or Annotation for individuals), and Article 14 (Administrative and judicial redress) of the Agreement.

[15] See e.g. Judgment in *Commission v. Germany*, C-518/07, EU:C:2010:125; Judgment in *Commission v. Austria*, C-614/10, EU:C:2012:631; Judgment in *Commission v. Hungary*, C-288/12, ECLI:EU:C:2014:237.

19. Moreover, in assessing the proportionality of the retention period, regard must be had to the nuanced manner in which the data is retained which affords additional protection for personal data. In particular, Article 16(3) of the Agreement imposes an obligation on Canada to "depersonalize the PNR data through masking the names of all passengers 30 days after Canada receives it" and further that, two years after Canada receives the data, Canada "shall further depersonalize it" through masking further information in the PNR data. Under Article 16(4) of the Agreement, Canada may unmask the PNR data "only if on the basis of available information, it is necessary to carry out investigations under the scope of Article 3" and, even then, subject to the restricted access provisions set out in subparagraphs (a) and (b) of Article 16(4). In addition, the Agreement makes special provision in respect of sensitive data which must, in accordance with Article 8(5) and with one very limited exception, be deleted no later than 15 days from the data Canada receives it.

20. When the Agreement is looked at as a whole and in its context, Ireland submits that it is clear that its provisions comply with the principle of proportionality enshrined in Article 52(1) and, consequently, fully respect the right to privacy and the right to protection of personal data enshrined in Articles 7 and 8 of the Charter of Fundamental Rights.

21. In conclusion, in respect of the first question, Ireland submits that the Agreement is indeed compatible with Article 16 TFEU and Articles 7, 8 and 52(1) of the Charter of Fundamental Rights.

III. The Appropriate Legal Basis for the Act of the Council concluding the Agreement

22. By its second question, the Parliament has asked whether Articles 82(1)(d) and 87(2)(a) TFEU constitute the appropriate legal basis for the act of the Council concluding the Agreement or whether the Act must be based on Article 16 TFEU.

23. As the Parliament has stated in its Request, it is settled case law that the choice of legal basis for an EU measure "must rest on objective factors amenable to judicial review", which factors include in particular the aim and content of the measure.[16] As the case law also makes clear, the choice of the appropriate legal basis has "constitutional significance".[17] This is certainly the case in respect of the Agreement because the effect of the Parliament's submission – that Article 16 TFEU, rather than Articles 82(1)(d) and 87(2)(a) TFEU, is the appropriate legal basis for the Council act concluding the Agreement – would be to ignore the special regime applicable to Ireland, the United Kingdom and Denmark in the area of freedom, security and justice which is enshrined in Protocols No. 21 and 22 to the TFEU.

24. The aim of the Agreement is apparent from Article 1 of the Agreement, entitled Purpose of Agreement, particularly when read in light of the Preamble to the Agreement. Article 1 provides that, in this Agreement, "the Parties set out the conditions for the transfer and use of Passenger Name Record (PNR) data to ensure the security and safety of the public and prescribe the means by which the data is protected". In Ireland's view, the aim of the Agreement articulated in this provision is "to ensure the security and safety of the public". Ireland agrees with the written observations of the Council that the transfer and use of PNR data, and the conditions attaching thereto, are the means by which this aim is achieved rather than a distinct aim. If Article 1 left any doubt as to the aim of the

[16] Opinion 1/08, EU:C:2009:739; 2/00, paragraph 172.
[17] Opinion 1/08, EU:C:2009:739; 2/00, paragraph 110.

Agreement, this is removed by the detailed provisions of the Preamble to the Agreement which set out the intentions of the Parties *inter alia* in the following terms:

> *"SEEKING to prevent, combat, repress, and eliminate terrorism and terrorist-related offences, as well as other serious transnational crime, as a means of protecting their respective democratic societies and common values to promote security and the rule of law;*
>
> *RECOGNISING the importance of preventing, combating, repressing, and eliminating terrorism and terrorist-related offences, as well as other serious transnational crime, while preserving fundamental rights and freedoms, in particular rights to privacy and data protection;*
>
> *SEEKING to enhance and encourage cooperation between the Parties in the spirit of the partnership between Canada and the European Union;*
>
> *RECOGNISING that information sharing is an essential component of the fight against terrorism and related crimes and other serious transnational crime, and that in this context, the use of Passenger Name Record (PNR) data is a critically important instrument to pursue these goals;*
>
> *RECOGNISING that, in order to safeguard public security and for law enforcement purposes, rules should be laid down to govern the transfer of PNR data by air carriers to Canada;*
>
> *….*
>
> *NOTING the commitment of Canada that the Canadian Competent Authority processes PNR data for the purpose of preventing, detecting, investigating and prosecuting terrorist offences and serious transnational crime in strict compliance with safeguards on privacy and the protection of personal data, as set out in this Agreement;*
>
> *STRESSING the importance of sharing PNR data and relevant and appropriate analytical information containing PNR data obtained under this Agreement by Canada with competent police and judicial authorities of Member States of the European Union, Europol and Eurojust as a means to foster international police and judicial cooperation; …."*

The Preamble also makes clear that it is specifically "in order to safeguard public security and for law enforcement purposes" that "rules should be laid down to govern the transfer of PNR data by air carriers to Canada" in a manner which recognizes the Parties' common values with respect to privacy and data protection and, in particular, in a manner which is mindful of the European Union's commitments under the Treaties and the Charter of Fundamental Rights.

25. While the Parliament has laid emphasis in its Request on the fact that most articles of the Agreement relate to the protection of personal data, in Ireland's view, this is to confuse the means by which the aim is achieved in the Agreement and the aim of the Agreement itself. Ireland supports the submissions of the Council in this regard and in relation to the proper scope and application of Article 16 TFEU.[18] In Ireland's submission, the core substantive provisions of the Agreement reflect the aim of ensuring public security and safety in the context of the fight against terrorism and serious transnational crime. Thus, Article 3, entitled 'Use of PNR data', provides that Canada "shall ensure that the Canadian Competent Authority processes PNR data received pursuant to this Agreement strictly for the purpose of preventing, detecting, investigating or prosecuting terrorist offences or serious transnational crime". Article 4, entitled 'Ensuring PNR data is provided', provides *inter alia* that the EU "shall ensure that air carriers are not prevented from transferring PNR data to the Canadian Competent Authority pursuant to this Agreement". Article 5, 'Adequacy', confirms that, subject to compliance with the Agreement, the Canadian Competent Authority is deemed to provide an adequate level of protection for the processing and use of PNR data. Article 6, entitled 'Police and judicial cooperation', provides for the sharing of information between the Canadian and EU and Member States authorities. These are the essential provisions that establish the legal framework for the transfer and use of PNR data between the EU and Canada which forms the core of the Agreement. While the detailed provisions of Articles 7 to 21 are extremely important as a means of giving effect to this legal framework, properly considered, they merely set out the detailed requirements of the guarantee of adequacy enshrined in Article 5. Notwithstanding their importance for ensuring that EU action complies with Article 16 TFEU and the Charter, in the overall context of this Agreement, these provisions are ancillary to the core provisions of Articles 1 to 6 of the Agreement which establishes the framework for transfer and use of PNR data between the EU and Canada

[18] Ireland also refers in this regard to the Declaration on Article 16 of the Treaty on the Functioning of the European Union: "The Conference declares that, whenever rules on protection of personal data to be adopted on the basis of Article 16 could have direct implications for national security, due account will have to be taken of the specific characteristics of the matter. It recalls that the legislation presently applicable (see in particular Directive 95/46/EC) includes specific derogations in this regard."

for the purpose of ensuring public security and safety in the fight against terrorism and serious transnational crime.

26. If, contrary to Ireland's submission, the protection of personal data was itself considered an aim of the Agreement, and not simply the means by which the aim of ensuring public security and safety is achieved, Ireland would submit that this aim is merely incidental to the predominant aim of ensuring public security and safety. The settled case law of this Court confirms that, if examination of a measure reveals that it pursues a twofold purpose or that it has a twofold component, and if one of those is identifiable as the main or predominant purpose or component, whereas the other is merely incidental, the measure "must be based on a single legal basis, namely that required by the main or predominant purpose or component".[19] It is only in exceptional circumstances if it is established that the measures pursues several objectives "which are inseparably linked without one being secondary and indirect in relation to the other" that the measure must be founded on the various corresponding legal bases.[20] However, no dual legal basis is possible where, as in this case, where the procedures required by each legal basis are incompatible with each other.[21]

27. In this regard, Ireland notes that the Parliament has framed its question in relation to the appropriate legal basis for the act of the Council concluding the Agreement as in effect a choice between Articles 82(1)(d) and 87(1)(a) TFEU, on the one hand, and Article 16 TFEU, on the other hand. It has not suggested that the Parliament and Council could rely on a dual legal basis for the act of the Council concluding the Agreement. Ireland is of the view that it would not be possible to combine Articles 82(1)(d) and 87(1)(a) TFEU and Article 16 TFEU as the legal basis for the act of the Council in this case and supports the written observations of the Council in this regard. Because of the distinct manner in which the ordinary legislative procedure operates under Article 16 TFEU, on the one hand, and under Articles 82(1)(d) and 87(1)(a) TFEU by reason of the special position of Ireland, United Kingdom and Denmark, on the other hand, Ireland is of the view that the

[19] See e.g. Judgment in *Commission v Council*, C-137/12, EU:C:2013:675, paragraph 58.
[20] See e.g. Judgment in *Commission v Council*, C-377/12, EU:C:2014:1903, paragraph 34.
[21] See below paragraph 36.

procedures required by each legal basis are incompatible with each other and that no dual legal basis would be possible.[22]

28. In light of the clear aim of the Agreement to ensure public security and safety, it is submitted that Articles 82(1)(d) and 87(2)(a) TFEU constitute the appropriate legal basis for the Council act concluding the Agreement. Both of these provisions form part of Title V of Part Three of the TFEU under which the Union constitutes "an area of freedom, security and justice with respect for fundamental rights and the different legal systems and traditions of the Member States".[23] In this area of freedom, security and justice, the Union shall *inter alia* "endeavour to ensure a high level of security through measures to prevent and combat crime, racism and xenophobia, and through measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgments in criminal matters and, if necessary, through the approximation of criminal laws".[24] Chapter 4 of Title V addresses judicial cooperation in criminal matters. Within this Chapter, Article 82 confers power on the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, to adopt measures to *inter alia* "(d) facilitate cooperation between judicial or equivalent authorities of the Member States in relation to proceedings in criminal matters and the enforcement of decisions". Chapter 5 of Title V addresses police cooperation. Article 87(2) confers power on the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, to adopt measures concerning *inter alia* "(a) the collection, storage, processing, analysis and exchange of relevant information". The external dimension of these policies manifests itself in police and judicial cooperation agreements between the EU and third countries, including in the processing and exchange of relevant information, as in the case of the envisaged Agreement. While in adopting internal measures and in concluding international agreements in this field the EU institutions must respect Article 16 TFEU and the Charter, the mere fact that such measures or agreements contain provisions to ensure respect for those provisions does not of itself change the nature, aim or legal basis for the relevant

[22] Judgment in *Commission v. Council*, Case C-377/12, EU:C:2014:1903, paragraph 34.
[23] Article 67(1) TFEU.
[24] Article 67(3) TFEU.

measure or agreement. For these reasons, Ireland submits that Articles 82(1)(d) and 87(1)(a) constitute the appropriate legal basis for the Agreement.

29. This conclusion is consistent with, and indeed reinforced by, the approach adopted by this Court to earlier measures involving the transfer and use of PNR data. In Joined Cases C-317/04 and C-318/04, the European Parliament sought, in a first case, the annulment of Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection and, in a second case, the annulment of the Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States Bureau of Customs and Border Protection.[25] While the cases concerned an earlier international agreement with a different third country, which pre-dated the entry of the Treaty of Lisbon, the Court's core findings on the nature and characterization of the transfer of PNR data remain instructive. In its judgment, this Court first considered Commission Decision 2004/535/EC which was adopted on the basis of Article 25(6) of Directive 95/46/EC. Directive 95/46/EC, which was itself adopted on the basis of Article 95 EC, excluded from its scope "processing operations concerning public security, defence, State security ... and the activities of the State in areas of criminal law" (Article 3(2)). The Court concluded that "the transfer of PNR data… constitutes processing operations concerning public security and the activities of the State in the areas of criminal law", thereby falling within "a framework established by the public authorities that relates to public security".[26] For this reason, the Court concluded that Commission Decision 2004/535/EC did not fall within the scope of Directive 95/46/EC and thus had to be annulled. In relation to Council Decision 2004/496/EC, the Court concluded that the agreement related to the same transfer of data as the Commission Decision and therefore to data processing operations falling outside the scope of the Directive.[27] As a result, the

[25] Judgment in *Parliament v. Council; Parliament v. Commission*, Joined Cases C-317/04 and C-318/04, EU:C:2006:346.
[26] Judgment in *Parliament v. Council*, EU:C:2006:346., paragraphs 56-58.
[27] Judgment in *Parliament v. Council*, EU:C:2006:346., paragraph 68.

Court held that the Council Decision could not have been validly adopted on the basis of Article 95 EC, the legal basis which had been used for the adoption of the Directive itself. Notwithstanding the creation of a distinct provision conferring competence on the EU institutions in the field of data protection in Article 16 TFEU, the Court's characterization of the underlying data processing operations remains valid. If measures relating to the transfer and use of PNR data are to be adopted, it is submitted that they are properly adopted within the framework of the area of security, justice and freedom and, in particular, under the provisions conferring competence on the Union in the fields of judicial and police cooperation.[28]

30. While the Parliament is correct to submit that the choice of legal basis, being based on objective factors, cannot rest on a mere practice on the part of the Council or the legal basis of other Union measures which might display similar characteristics, the practice of the institutions nonetheless supports the conclusion that the proper legal basis for the Council act concluding the Agreement is Articles 82(1)(d) and 87(2)(a) TFEU. Following the Court's judgment in Joined Cases C-317/04 and C-318/04, the Council adopted acts concluding international agreements with the United States and Australia in relation to the transfer and use of PNR data on the basis of Articles 24 and 36 of the TEU.[29] Moreover, since the coming into force of the Treaty of Lisbon, the Council has adopted, with the consent of the Parliament, acts concluding revised agreements with these third countries using as the legal basis Articles 82(1)(d) and 87(1)(a) TFEU.[30]

---

[28] The material objective of that directive is, therefore, to contribute to the fight against serious crime and thus, ultimately, to public security.

[29] See: Council Decision 2008/651/CFSP/JHA of 30 June 2008 on the signing, on behalf of the European Union, of an Agreement between the European Union and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian Customs Service; Council Decision 2007/551/CFSP/JHA of 23 July 2007 on the signing, on behalf of the European Union, of an Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS).

[30] See: 2012/381/EU: Council Decision of 13 December 2011 on the conclusion of the Agreement between the European Union and Australia on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service; 2012/472/EU: Council Decision of 26 April 2012 on the conclusion of the Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security.

31. In this case, from Ireland's perspective, there are important additional considerations of a constitutional nature that support the choice of legal basis proposed by the Council for the adoption of the Council act concluding the Agreement. While the Treaty of Lisbon has effected significant changes to the legal framework of the area of freedom, security and justice, and integrated it to a large extent into the TFEU framework governing other Union policies, Title V of Part Three of the TFEU remains subject to distinct decision-making procedures in certain respects. First, under provisions in Title V, including Article 82 and 87 TFEU, there is provision for enhanced cooperation among Member States in certain circumstances. Secondly, and more significantly for the purposes of these proceedings, by reason of Protocols No. 21 and 22 to the TFEU, Ireland, the United Kingdom and Denmark are subject to a special regime within the context of the area of freedom, security and justice. Protocol No. 21 deals with the position of the United Kingdom and Ireland (specifically in respect of the area of freedom, security and justice) while Protocol No. 22 deals with the position of Denmark under the Treaties.

32. Article 1 of Protocol No. 21 provides that, subject to Article 3, the United Kingdom and Ireland shall not take part in the adoption by the Council of proposed measures pursuant to Title V of Part Three of the Treaty on the Functioning of the European Union. As a consequence of this, Article 2 of the Protocol No. 21 provides that none of the provisions of Title V of Part Three of the TFEU, no measure adopted pursuant to that Title, no provision of any international agreement concluded by the Union pursuant to that Title, and no decision of the Court of Justice interpreting any such provision or measure "shall be binding upon or applicable in the United Kingdom or Ireland". However, Article 3 of Protocol No. 21 allows the United Kingdom or Ireland to notify the President of the Council in writing, within three months of the presentation of a proposal or initiative to the Council, that "it wishes to take part in the adoption and application of any such proposed measure, whereupon that State shall be entitled to do so", which measure, if adopted, shall be binding on all Member States which took part in its adoption. Article 4, for its part, allows the United Kingdom or Ireland to notify the Council and the Commission of its desire to accept a measure which has already been adopted. With

respect to the protection of personal data specifically, Article 6a of Protocol No. 21 specifically provides that the United Kingdom and Ireland "shall not be bound by the rules laid down on the basis of Article 16 of the Treaty on the Functioning of the European Union which relate to the processing of personal data by the Member States when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of that Treaty where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation which require compliance with the provisions laid down on the basis of Article 16".

33. This special regime governing Ireland's participation in the area of freedom, security and justice has been reflected in an amendment of the Constitution of Ireland, 1937 approved by the Irish People. Article 29.4.7° of the Constitution provides that the State may exercise the options or discretions *inter alia* under Protocol No. 21 but that "any such exercise shall be subject to the prior approval of both Houses of the Oireachtas". Thus, where Ireland wishes to participate in measures adopted under Title V of Part Three of the TFEU, it can only do so as a matter of Irish constitutional law where it has obtained the prior approval of the Irish parliament. In the case of the Agreement, Ireland decided to exercise its option to take part in the adoption and conclusion of the Agreement. To this end, on 14 November 2013, Dáil Éireann and Seanad Éireann approved Ireland's participation in the adoption and application of the Agreement.

34. If, however, the appropriate legal basis for the adoption of the Council act concluding the Agreement was instead Article 16 TFEU alone, as the Parliament suggests, this would radically alter the legal framework within which Ireland is participating in the Agreement. In this particular case, Ireland has decided to participate in the Agreement. However, if at a future date Ireland did not wish to participate in a similar agreement governing the transfer and use of PNR data in a third country, and the appropriate legal basis was Article 16 TFEU rather than Articles 82(1)(d) and 87(1)(a) TFEU, Ireland would no longer enjoy the option enshrined in Protocol No. 21 and the requirement enshrined in the

Constitution of Ireland to seek parliamentary approval for participation would be set at naught.

35. While Article 6a of Protocol No. 21 serves to remove the binding effect of measures adopted under Article 16 TFEU to Ireland and the United Kingdom when carrying out activities under "Chapter 4 or Chapter 5 of Title V of Part Three of that Treaty where the United Kingdom and Ireland are not bound by the rules governing the forms of judicial cooperation in criminal matters or police cooperation", substituting Article 16 TFEU for Articles 82(1)(d) and 87(1)(a) TFEU as the legal basis for the Council act concluding this Agreement would have the altogether more radical effect of removing matters properly falling within Title V from their proper place within the Treaties and from the special decision-making regime applicable to them, at least insofar as Ireland, the United Kingdom and Denmark are concerned. This would fundamentally alter the division of competences in the Treaties in a manner incompatible with Article 4 TEU.

36. While Ireland's observations focus on its own position, these considerations would appear to apply *a fortiori* to the position of Denmark as defined in Protocol No. 22 of the TFEU. In contrast to Ireland and the United Kingdom, which have exercised their option to participate in the Agreement, Denmark is not taking part in the adoption of the decision and is not bound by the Agreement or subject to its application.

37. It follows that the choice of legal basis in this case has constitutional significance for the EU and its Member States, and in particular for Ireland, the United Kingdom and Denmark.

IV. Conclusions

38. FOR THESE REASONS it is submitted that the Court should respond as follows to the Request for an Opinion pursuant to Article 218(11) TFEU lodged by the European Parliament at the Court Registry on 30 January 2015:

The envisaged agreement is 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 protection of personal data.

Article 82(1)(d) and Article 87(2)(a) TFEU constitute the appropriate legal basis for the act of the Council concluding the envisaged agreement.

Dated the 29th day of May 2015

Signed: **Gemma Hodge**
Agent for Ireland
on behalf of Eileen Creedon, Chief State Solicitor

Signed: **Tony Joyce**
Agent for Ireland
on behalf of Eileen Creedon, Chief State Solicitor