ЕВРОПЕЙСКИ ПАРЛАМЕНТ PARLAMENTO EUROPEO EVROPSKÝ PARLAMENT EUROPA-PARLAMENTET
EUROPÄISCHES PARLAMENT EUROOPA PARLAMENT ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ EUROPEAN PARLIAMENT
PARLEMENT EUROPÉEN PARLAIMINT NA hEORPA PARLAMENTO EUROPEO EIROPAS PARLAMENTS
EUROPOS PARLAMENTAS EURÓPAI PARLAMENT IL-PARLAMENT EWROPEW EUROPEES PARLEMENT
PARLAMENT EUROPEJSKI PARLAMENTO EUROPEU PARLAMENTUL EUROPEAN
EURÓPSKY PARLAMENT EVROPSKI PARLAMENT EUROOPAN PARLAMENTTI EUROPAPARLAMENTET

Legal Service

SJ-0890/14

22 DEC. 2014

LEGAL OPINION

Re: LIBE – Questions relating to the judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others* - Directive 2006/24/EC on data retention - Consequences of the judgment.

I. Introduction

1. On 29 October 2014, the Legal Service received, by letter dated 27 October 2014 (annexed), a request from Mr Claude MORAES, Chairman of the Committee on Civil Liberties, Justice and Home Affairs, for an opinion on nine questions relating to the consequences of the judgment of the Court of Justice (Grand Chamber), dated 8 April 2014, in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others*,[1] (hereinafter the "*DRI judgment*"). This judgment declared as "*invalid*" Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (hereinafter the "*data retention Directive*").[2]

II. Legal context

2. In order to put the nine questions raised in their proper legal context, the Legal Service will first set out, below, the main aspects of the reasoning of the Court of Justice in the DRI judgment.

---

1 EU:C:2014:238.

2 OJ L 105, 13.4.2006, p. 54.

L-2929 Luxembourg - Tel +352 43 00 22 626 - Fax +352 43 23 07
B-1047 Bruxelles - Tel +32 2 284 27 24 - Fax +32 2 23 01 233
F-67070 Strasbourg - Tel +33 3 88 17 46 26 - Fax +33 3 88 37 02 36

II. A. Reasoning of the Court contained in the DRI judgment

Relevance of Articles 7 and 8 of the Charter

3. The starting point for the Court's reasoning is to consider the relevance of the Charter of Fundamental Rights of the European Union (hereinafter the "Charter"), and in particular Articles 7 and 8 thereof.[3]

4. In this respect the Court examines the nature of the data which providers of publicly available electronic communications services or of public communications networks must retain pursuant to the data retention Directive. The Court thus finds that those data, taken as a whole "*may 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 or residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them*".[4] Accordingly, the Court goes on to find that the retention of such data for the purpose of possible access to them by the competent national authorities "*directly and specifically affects private life*" and consequently the rights guaranteed by Article 7 and 8 of the Charter.[5] This being so, the Court considers it appropriate to proceed to examine the validity of the data retention Directive in the light of Articles 7 and 8 of the Charter.

Interference with fundamental rights guaranteed by Articles 7 and 8 of the Charter

5. Given that the data retention Directive (1) imposes an obligation on service providers to retain data and also (2) lays down rules relating to the access of the competent national authorities to the data, the Court next establishes the existence of an "*interference*" by the data retention Directive with both the fundamental right to privacy guaranteed by Article 7 of the Charter and the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter.[6]

6. The Court also states that this interference caused by the data retention Directive with the fundamental rights laid down in Articles 7 and 8 of the Charter is "*wide-ranging*" and "*particularly serious*".[7]

Justification for the interference under Article 52(1) of the Charter?

7. Having established that there is an interference with fundamental rights here, the Court next considers whether there was any "*justification*" for this interference, in accordance with Article 52(1) of the Charter.[8] Article 52(1) of the Charter provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, subject to the principle of proportionality, limitations may be made to those rights and freedoms only if they are

---

3 See paragraphs 24 to 31 of the DRI judgment.
4 See paragraph 27 of the DRI judgment.
5 See paragraph 29 of the DRI judgment.
6 See paragraphs 32 to 37 of the DRI judgment.
7 See paragraph 37 of the DRI judgment.
8 See paragraphs 38 to 69 of the DRI judgment

necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

8. Firstly, so far as concerns the "*essence*" of the fundamental right to privacy and the other rights laid down in Article 7 of the Charter, the Court holds that, even though the retention of data required by the data retention Directive constitutes a particularly serious interference with those rights, it is not such as to adversely affect the essence of those rights.[9] Nor is that retention of data such as to adversely affect the essence of the fundamental right to the protection of personal data enshrined in Article 8 of the Charter. This requirement is thus satisfied in the present case.

9. Secondly, as regards the question of whether that interference satisfies an "*objective of general interest*", the Court observes that the material objective of the data retention Directive is to contribute to the fight against serious crime and thus, ultimately, to public security. The Court then recalled that, according to previous case-law, the fight against international terrorism in order to maintain international peace and security constitutes an objective of general interest.[10] The same is true of the fight against serious crime in order to ensure public security.[11] Furthermore, the Court noted, in this respect, that Article 6 of the Charter lays down the right of any person not only to liberty, but also to security. In this respect, the Court holds that the retention of data for the purpose of allowing the competent national authorities to have possible access to those data, as required by the data retention Directive "*genuinely satisfies an objective of general interest*".[12] This requirement is thus also satisfied in the present case.

10. In these circumstances, the Court then proceeds, thirdly, to verify the "*proportionality*" of the interference found to exist.[13] This is indeed the crux of the whole judgment and it is the Court's examination, in quite some depth, of this issue which finally leads to the conclusion, at the end of the judgment, that the data retention Directive is invalid. For this reason, we should pay particular attention to this part of the judgment.

"Proportionality" of the interference under Article 52(1) of the Charter?

11. The Court recalls that, according to the settled case-law, the principle of proportionality requires that acts of the EU institutions be "*appropriate*" for attaining the legitimate objectives pursued by the legislation at issue and "*do not exceed the limits*" of what is appropriate and "*necessary*" in order to achieve those objectives.[14]

12. With regard to judicial review of compliance with those conditions, where interferences with fundamental rights are at issue, the Court declares, in a key passage, that "*the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors*", including, in particular, the area concerned, the nature of the right

---

9 See paragraphs 39 and 40 of the DRI judgment.

10 See Cases C-402/05 P and C-415/05 P *Kadi and Al Barakaat International Foundation* v *Council and Commission* EU:C:2008:461, paragraph 363, and Cases C-539/10 P and C-550/10 P *Al-Aqsa* v *Council* EU:C:2012:711, paragraph 130.

11 See Case C-145/09 *Tsakouridis* EU:C:2010:708, paragraphs 46 and 47.

12 See paragraphs 41 to 44 of the DRI judgment.

13 See paragraphs 45 to 69 of the DRI judgment.

14 See paragraph 46 of the DRI judgment.

at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference.[15] In this regard, the Court refers expressly to the case-law of the European Court of Human Rights in Strasbourg.[16]

13. In view of these factors, the Court then declares that, in the present case "*the EU legislature's discretion is reduced, with the result that review of that discretion should be strict*".[17]

14. The Court then proceeds to examine the details of the data retention Directive according to this "*strict*" standard of review. First, the Court asks whether this measure is "*appropriate*". Considering that data which must be retained pursuant to this Directive allow the national authorities which are competent for criminal prosecutions to have additional opportunities to shed light on serious crime, the Court finds that data retention here is therefore a "*valuable tool for criminal investigations*". Consequently, the Court rules that the retention of such data may be considered to be "*appropriate*" for attaining the objective pursued by that Directive.[18] This first part of the "*proportionality*" test is thus satisfied in the present case.

15. Second, as regards the "*necessity*" for the retention of data, the Court holds that the fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. Such an objective of general interest, however fundamental it may be, does not, in itself, justify a retention measure, such as that established by the data retention Directive, being considered to be necessary for the purpose of that fight.[19]

16. So far as the right to respect for private life is concerned, the protection of that fundamental right requires, according to the Court's settled case-law, in any event, that "*derogations and limitations in relation to the protection of personal data*" must apply only in so far as is "*strictly necessary*". In that regard, it should be noted that the protection of personal data resulting from the explicit obligation laid down in Article 8(1) of the Charter is "*especially important*" for the right to respect for private life enshrined in Article 7 of the Charter.[20]

17. Consequently, the Court makes the following declaration, in paragraph 54 of its judgment, referring, once again, explicitly to the case-law of the European Court of Human Rights[21] (emphasis added):

---

15 Paragraph 47 of the DRI judgment.

16 See, by analogy, as regards Article 8 of the European Convention on Human rights (hereinafter "ECHR" or the "Convention"), Eur. Court H.R., *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, § 102, ECHR 2008-V.

17 See paragraph 48 of the DRI judgment.

18 See paragraphs 49 and 50 of the DRI judgment.

19 See paragraph 51 of the DRI judgment.

20 See paragraphs 52 and 53 of the DRI judgment.

21 See, by analogy, as regards Article 8 of the ECHR, Eur. Court H.R., *Liberty and Others v. the United Kingdom*, 1 July 2008, no. 58243/00, § 62 and 63; *Rotaru v. Romania*, § 57 to 59, and *S. and Marper v. the United Kingdom*, § 99.

"[T]*he EU legislation in question 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 have been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data.*"

18. The need for such safeguards is all the greater where, as laid down in the data retention Directive, personal data are subjected to automatic processing and where there is a "*significant risk of unlawful access to those data*".[22]

19. As for the question of whether the interference caused by the data retention Directive is "*limited to what is strictly necessary*", the Court observes that the Directive requires the retention of all traffic data concerning fixed telephony, mobile telephony, Internet access, Internet e-mail and Internet telephony. It therefore applies to all means of electronic communication, the use of which is "*very widespread and of growing importance in people's everyday lives.*" Furthermore, the Directive covers all subscribers and registered users. It therefore entails "*an interference with the fundamental rights of practically the entire European population.*"[23]

20. In this respect, the Court notes, first, that the data retention Directive covers, in a "*generalised manner*", all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime.[24]

21. This Directive affects, in a "*comprehensive manner*", all persons using electronic communications services, but "*without the persons whose data are retained being, even indirectly, in a situation which is liable to give rise to criminal prosecutions.*" It therefore "*applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime.*" Furthermore, it does not provide for any exception, with the result that it applies even to persons whose communications are subject, according to rules of national law, to the obligation of professional secrecy.[25]

22. Moreover, the Court underlines the fact that, whilst seeking to contribute to the fight against serious crime, the data retention Directive "*does not require any relationship between the data whose retention is provided for and a threat to public security*" and, in particular, it is not restricted to a retention in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the retention of their data, to the prevention, detection or prosecution of serious offences.[26]

23. Thus, the Court finds that there is not only "*a general absence of limits*" in this Directive but that it also "*fails to lay down any objective criterion by which to*

---

22 Paragraph 55 of the DRI judgment.
23 Paragraph 56 of the DRI judgment.
24 Paragraph 57 of theDRI judgment.
25 Paragraph 58 of the DRI judgment.
26 Paragraph 59 of the DRI judgment.

determine the limits of the access of the competent national authorities" to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences that, in view of the extent and seriousness of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter, may be considered to be sufficiently serious to justify such an interference. On the contrary, the data retention Directive simply refers, in Article 1(1), in a "*general manner*" to serious crime, as defined by each Member State in its national law.[27]

24. Furthermore, the Court considers that the data retention Directive does not contain "*substantive and procedural conditions relating to the access of the competent national authorities to the data and to their subsequent use*".[28] In particular, the Directive does 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. Above all, the access by the competent national authorities to the data retained is "*not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions.*" Nor does it lay down a specific obligation on Member States designed to establish such limits.[29]

25. Also, the Court raises criticisms concerning the data retention period set out in the Directive "*without any distinction being made between the categories of data*" on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned. This data retention period is also criticised on the ground that the Directive does not state that the determination of the period of retention must be based on "*objective criteria*" in order to ensure that it is limited to what is strictly necessary.[30]

26. The Court therefore concludes from the above that the data retention Directive "*does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter.*" The Court therefore holds that this Directive entails a "*wide-ranging and particularly serious interference*" with those fundamental rights in the legal order of the EU, "*without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary*".[31]

27. Moreover, as far as the "*rules relating to the security and protection of data*" are concerned, the Court finds that the data retention Directive does not provide for "*sufficient safeguards*", as required by Article 8 of the Charter, to ensure effective protection of the data retained against "*the risk of abuse and against any unlawful access and use*" of that data. In the first place, the Directive does not lay down rules which are specific and adapted to (i) the "*vast quantity of data*" whose retention is

---

27 Paragraph 60 of the DRI judgment.

28 Paragraph 61 of the DRI judgment.

29 Paragraph 62 of the DRI judgment.

30 Paragraphs 63 and 64 of the DRI judgment.

31 Paragraph 65 of the DRI judgment.

required by that Directive, (ii) the "*sensitive nature*" of that data and (iii) the "*risk of unlawful access*" to that data, rules which would serve, in particular, to govern the protection and security of the data in question in a clear and strict manner in order to ensure their full integrity and confidentiality. Furthermore, a specific obligation on Member States to establish such rules has also not been laid down.[32]

28. In the second place, the Court adds that that this Directive does not require the data in question to be "*retained within the European Union*", with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an "*independent authority*" of compliance with the "*requirements of protection and security*" is fully ensured. Such a control, carried out on the basis of EU law, is an "*essential component*" of the protection of individuals with regard to the processing of personal data.[33]

29. Having regard to all the foregoing considerations, the Court finally holds that, by adopting Directive 2006/24, the EU legislature has "*exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter*".[34]

30. Consequently, the Court declares that the data retention Directive is "*invalid*".[35]

III. Legal Analysis

31. Before replying in detail to the nine specific questions raised by the LIBE Committee in the request for a legal opinion, the Legal Service considers it useful to first set out some general considerations which can now be drawn from the DRI judgment and which can be taken into account when examining all of these questions.

III.A General considerations

Is the Charter applicable according to Article 52(1)?

32. First of all, it must be underlined that the Court's reasoning in the DRI judgment is based on the provisions of the Charter, and in particular Articles 7, 8 and 52(1) thereof.

33. Consequently, the Court's reasoning in this particular case can only apply to other cases also if the Charter is applicable in the first place. In the case of other measures adopted by the EU legislature this will always be the case, but care must be taken in particular as regards other measures adopted by the Member States, given that Article 51(1) of the Charter provides that the Charter applies to the Member States "*only when they are implementing Union law*".[36] It must therefore be established, as a preliminary consideration, whether or not Member States are implementing Union law.

---

32 Paragraph 66 of the DRI judgment.
33 Paragraph 68 of the DRI judgment.
34 Paragraph 69 of the DRI judgment.
35 Paragraph 71 of the DRI judgment.
36 See the judgment of the Court of Justice in Case C-617/10, *Fransson*, EU:C:2013:105, paragraph 21.

Are Articles 7 and 8 of the Charter relevant and is there any interference?

34. For cases where the Charter does indeed apply, the next question which must be addressed is whether Articles 7 and 8 of the Charter are relevant and, if so, whether there is an "*interference*" with those fundamental rights. If Articles 7 and 8 are not relevant or if there is no interference with such fundamental rights under the Charter, then the reasoning of the DRI judgment will not be applicable in any event.

What is the extent of EU legislature's discretion?

35. If there is found to be an interference with the fundamental rights set out in Articles 7 and/or 8 of the Charter, then the validity of the measure in question should then be examined. In this regard, the standard of judicial review used to examine the validity of the measure will depend on the extent of the EU legislature's discretion (or the national legislature's discretion, in cases concerning Member State's implementation of EU law).

36. The Court has declared that, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, "*depending on a number of factors*", including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference.[37]

37. As in the DRI judgment, the EU legislature's discretion may then prove to be "*reduced*", in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right. If so, there will be a "*strict*" method of judicial review of that exercise of discretion.

Is there a sufficient "justification" under Article 52(1) of the Charter?

38. A very careful review of the "*justification*" (including the necessity and proportionality) of any interference, under Article 52(1) of the Charter, will then be required.

39. In particular, the EU legislature must provide for "*clear and precise rules*" to limit the interference to what is "*strictly necessary*", notably through the inclusion in the EU legislative act of "*minimum safeguards*" and "*sufficient guarantees*".

40. In order to fully respect the principle of proportionality, the EU legislature must ensure that an interference with fundamental rights is "*precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary*".[38] If this is not the case, then the measure in question may be declared invalid by the Court as being contrary to the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter.

---

37 See paragraph 47 of the DRI judgment.

38 See paragraph 65 of the DRI judgment.

Importance of the case-law of the European Court of Human Rights

41. In this context, it is important to underline the fact that the Court of Justice has paid particular attention, in its DRI judgment, to the case-law of the European Court of Human Rights. Indeed, the DRI judgment explicitly refers, repeatedly, to the case-law of that Court. In effect, the Court of Justice has effectively transposed the existing case-law of the European Court of Human Rights on the need for safeguards and guarantees in the field of privacy and data protection (under Article 8 of the Convention), through the application of Articles 7, 8 and 52(1) of the Charter and the "*proportionality*" test contained therein (cf. paragraph 54 of the DRI judgment).

42. The case-law of both the Luxembourg and Strasbourg courts are now thus closely "*aligned*". This is, of course, fully consistent with the provisions of the Charter (in particular, Articles 52(3) and (7) thereof), not to mention also the Treaties (Article 6(3) TEU).

43. There is, in fact, nothing new in the Court of Justice referring to the case-law of the European Court of Human Rights in cases where the rights to privacy and data protection under Articles 7, 8 and 52(1) of the Charter apply. The Court of Justice has already done so in other previous cases which led, depending on the particular circumstances of each legislative act, either to a ruling confirming the validity of an EU act[39] or to a ruling declaring that parts of the EU act are incompatible with the Charter and thus invalid.[40]

44. The reasoning followed by the Court in the DRI judgment could thus be considered as being fully consistent with this previous case-law in this regard, but it does present a novel aspect in so far as the Court of Justice refers specifically, in the case of the data retention Directive, to a particular body of the case-law of the European Court of Human Rights on the issue of "*surveillance*".[41]

45. Indeed, the European Court of Human Rights has already established a well-developed body of case-law on the legality - under the Convention - of national legislation in the field of surveillance by national security authorities and national law enforcement authorities of individuals. That case-law sets out detailed requirements, under the Convention, for national rules to be considered compatible with Article 8 of the Convention, which require that in the special context of surveillance, such as the

---

39 See the judgment of the Court of Justice dated 17 October 2013 in Case C-291/12, *Schwarz* v *Stadt Bochum*, EU:C:2013:670, where the Court concluded, after assessing the compatibility with the Charter, that there is nothing capable of affecting the validity of a provision of Council Regulation No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States.

40 See the judgment of the Court of Justice (Grand Chamber) dated 9 November 2010 in Joined Cases C-92/99 and C-93/09, *Volker und Markus Schecke and Eifert*, EU:C:2010:662, where the Court found that certain provisions of Council Regulation No 1290/2005 on the financing of the common agricultural policy were invalid, in so far as certain aspects relating to the protection of personal data were concerned.

41 See in particular paragraphs 47, 54 and 55 of the DRI judgment where the Court of Justice refers to the following cases of the European Court of Human Rights in the field of surveillance: *S and Marper v United Kingdom* [GC], nos. 30562/04 and 30566/04, ECHR 2008-V, *Liberty and others v United Kingdom*, no. 58243/00, *Rotaru v Romania*, [GC] no. 28341/95, ECHR 2000-V, and *M.K. v France*, no 19522/09.

interception of communications, it is essential to have "*clear, detailed rules*" which indicate, *inter alia*, the scope of any discretion of the authorities, "*minimum safeguards*", the nature of the offences in question, a definition of the categories of people liable to be affected. It is also essential to limit the duration of the measure and define the retention period before the data obtained must be destroyed. The European Court of Human Rights has also specifically confirmed that this approach in this field does apply, not only to measures of surveillance targeted at specific individuals or addresses, but also to "*general programmes of surveillance*".[42]

46. Given the striking similarity between the wording of the case-law of the European Court of Human Rights in the specific field of surveillance by State authorities and the wording of the DRI judgment itself (which refers expressly to this same case-law), it seems that the Court of Justice has effectively incorporated the same principles into EU law, in this field, by applying the same very detailed reasoning stemming from the case-law of the European Court of Human Rights also in the case of the application of the Charter to measures of EU law, adopted by the EU legislature, in the field of surveillance (such as data retention).

47. In view of the fact that the cited case-law of the European Court of Human Rights itself relates to a diverse category of surveillance measures (which is not at all limited to data retention issues), it is to be expected that the Court of Justice will then apply the same reasoning when assessing the validity, under the Charter, of other EU legislative acts in this same field of "*general programmes of surveillance*", as referred to by the European Court of Human Rights.

48. The reasoning contained in the DRI judgment is thus not limited only to the specific issue of data retention, but can equally well be applied - at least as regards the application of Articles 7 and 8 of the Charter - to other EU legislative acts in the field of surveillance.

Method for reviewing the validity of acts under Articles 7, 8 and 52(1) of the Charter

49. In effect, we can consider that the DRI judgment has now set out a "*method*" for reviewing whether or not other EU acts may be considered to be compatible with Articles 7 and 8 of the Charter, and in particular with the principle of proportionality under Article 52(1) of the Charter, in the specific field of general programmes of surveillance.

50. According to this method, in order to assess whether other EU acts in this field comply with the principle of proportionality as required by Article 52(1) of the Charter, a number of factors need to be considered, including *inter alia*:

---

42 See in particular paragraph 63 of the *Liberty* judgment, cited above, to which the Court of Justice specifically refers in paragraph 54 of the DRI judgment.

Personal scope. Link with a threat to public security.

- Does the act in question apply to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime?
- Does the act require a relationship between the data processing in question and a threat to public security? In particular, is the data processing restricted in relation (i) to data pertaining to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime, or (ii) to persons who could, for other reasons, contribute, by the processing of their data, to the prevention, detection or prosecution of serious offences?

Limits on the access of the competent national authorities to the data and their subsequent use:

- Does the act lay down any objective criterion by which to determine the limits of the access of the competent national authorities to the data and their subsequent use for the purposes of prevention, detection or criminal prosecutions concerning offences?
- Are there "*substantive and procedural conditions*" relating to the access of the competent national authorities to the personal data and to their subsequent use, with "*objective criterion*" by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary?
- Is access by the competent national authorities to the data retained "*made dependent on a prior review carried out by a court or by an independent administrative body*" whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions?

Data retention period:

- Does the data retention period set out in the act distinguish between different categories of data on the basis of their possible usefulness for the purposes of the objective pursued or according to the persons concerned? Is this data retention period based on "*objective criteria*" in order to ensure that it is limited to what is strictly necessary?

Rules on security and protection of data:

- Are there "*sufficient safeguards*" relating to the security and protection of data, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data?
- Are the data in question to be "*retained within the European Union*", with the result that the control, explicitly required by Article 8(3) of the Charter, by an "*independent authority*" of compliance with the requirements of protection and security is fully ensured?

51. In view of the above general considerations and in the light of the method established by the Court of Justice, we will now address the specific questions raised by the LIBE Committee.

III.B Replies to the specific questions raised:

As regards Union Law (in force or under consideration):

III.B.1. On the first question: ***What are the consequences of the judgment as regards existing Union law (either international agreements or secondary law) requiring mass personal data collection other than traffic data, storage of the data of a very large number of unsuspected persons and access to and use of such data by law enforcement authorities; e.g. PNR international agreements, TFTP Agreement, or on legal instruments proposed or to be proposed, EU PNR or an entry/exit system?***

52. It should be clarified, from the outset that, from a purely formal legal point of view, the DRI judgment itself concerns only the validity of the data retention Directive which was examined by the Court of Justice in that case. It does not therefore have any direct consequences for the validity of any other EU act.

53. Indeed, existing EU acts benefit from a presumption of legality[43] and so, formally, any other EU act will still remain valid, irrespective of the fact that the Court declared the data retention Directive to be invalid in the DRI judgment. Other EU acts could only be declared invalid following separate legal proceedings before the Court of Justice and until that time all other EU acts remain valid.

54. That said, the "*presumption*" of legality of EU acts can also be rebutted and so it cannot be excluded, at this stage, that any other EU act could also suffer the same fate as the data retention Directive in a separate legal procedure. The reasoning of the Court of Justice in the DRI judgment could therefore be invoked, in separate legal proceedings, to lead to the same or a similar result that either the whole or a part of the act in question is declared invalid.

55. In this respect, the DRI judgment could, in principle, have indirect consequences as regards existing EU acts, given that the same general legal considerations based on the Charter - and the relevant case-law of the European Court of Human Rights - can be invoked to challenge the validity of other EU acts also.

56. It is clear though that the validity of each EU act must be assessed on a case-by-case basis, in the light of the particular circumstances of each case. In particular, the specific wording of the provisions of each act must be assessed in each case, in view of the particular objectives of general interest to be attained and the justifications advanced for each measure. As the DRI judgment is based on a very detailed assessment of the particular wording of the data retention Directive, it cannot be automatically concluded,

---

[43] See Case T-36/09, *dm-drogerie markt GmbH & Co. KG* v *OHIM*, EU:T:2011:449, paragraph 83.

at this stage, that any other EU act risks being declared invalid, by the Court of Justice in separate legal proceedings, as a result of this same reasoning.

57. In this context, it should also be underlined that the legal procedures before the Court of Justice are, of course, subject to the limitations set out in the Treaties. For example, direct actions before the Court of Justice to review the legality of legislative acts, in accordance with Article 263 TFUE, must be instituted within two months of the publication of the measure.

58. As regards international agreements which have already been concluded by the Union - including those mentioned in the first question : i.e. existing PNR international agreements[44] and the TFTP Agreement[45] - the procedure set out in Article 218(11) TFEU for requesting an opinion of the Court of Justice will not be available, as this particular procedure only applies before an "*envisaged*" agreement is concluded.[46]

59. That said, national courts may, in appropriate cases, request the Court of Justice to give a ruling in accordance with the preliminary reference procedure foreseen in Article 267 TFEU. This was indeed the procedure followed in the case which led to the DRI judgment.

60. In any event, the Commission can be asked, as guardian of the Treaties, to examine, in the light of the DRI judgment, the legality of existing EU acts and to propose, under its right of initiative, any legislative amendments considered necessary to ensure full respect for the Charter.

III.B.2 On the second question: ***What are the consequences on legislative proposals requiring mass collection of personal data other than traffic data, storage of the data of a very large number of unsuspected persons and access to and use of such data by law enforcement authorities?***

61. All new and pending legislative proposals which concern the special context of general programmes of surveillance must clearly now take account of the reasoning of the Court of Justice in the DRI judgment.

62. Indeed, the Court has declared that the EU legislature's discretion is "*reduced*" in such cases, with the result that review of that discretion should be strict. Great care must therefore be taken in such cases to ensure full respect, at all stages of the legislative procedure, for the Charter. The European Parliament, Council and Commission must all therefore act in a spirit of mutual cooperation to this end.

---

44 Cf. bilateral EU agreements with the United States (OJ L 215, 11.8.2012. p. 5) and Australia (OJ L 186, 14.7.2012. p. 4).

45 Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program , OJ L 195, 27.7.2010, p. 3.

46 Where the text of the international agreement itself foresees a procedure for the review or even termination of the agreement then the competent EU institutions may possibly invoke such steps, but this normally requires at least prior consultations with the third country concerned and a certain period of prior notice.

63. The proposed EU PNR[47] and Entry/Exit System[48] (both mentioned in the request for a legal opinion) can both clearly raise such issues.[49] The data in question here are also to be processed for use by the competent national authorities in respect of large numbers of individuals, for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with crime. Accordingly, these cases also fall into the category of "*general programmes of surveillance*" covered by the case-law of the European Court of Human Rights to which the Court of Justice referred in the DRI judgment.

64. Great care must therefore be taken to ensure that the EU legislature does not exceed its "*reduced*" discretion in these cases and that adequate safeguards and objective limits are provided for, to avoid any risk that such legislation could later be declared "*invalid*" by the Court, as in the DRI judgment. The "*strict*" method of judicial review - outlined above - which was followed by the Court of Justice in the DRI judgment will also apply in these cases also and so every effort must be made to ensure full compliance with all the various factors identified by the Court in its reasoning, where applicable due to the nature and content of each particular legislative proposal.

III.B.3. On the third question: ***What are the consequences on Union's international agreements under negotiation regarding requiring mass personal data collection other than traffic data, storage of the data of a very large number of unsuspected persons and access to and use of such data by law enforcement authorities?***

65. The same considerations as just set out above will apply also in the case of international agreements under negotiation, given that the EU legislature's discretion, in external relations, to conclude international agreements, under the Treaty and in accordance with the Charter, cannot be wider than the discretion, in internal matters, to adopt EU legislation applying within the EU legal order.

66. As a matter of principle, equal respect for the fundamental rights of individuals which are protected by Articles 7 and 8 of the Charter must be ensured in all cases, whether there is an internal or external dimension of the application of EU law.

---

47 Commission proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final.

48 Commission proposal for a regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data of third country nationals crossing the external borders of the Member States of the European Union, COM(2013) 95 final.

49 As regards the Commission proposal for the Entry/Exit System (EES) it is to be underlined that the main objective of this proposal is to improve the management of the external borders and to combat irregular immigration (Article 4 of the draft regulation). However, recital 23 leaves open the possibility of a subsequent processing of the data collected for law enforcement purposes, if such a decision is taken 2 years after the start of operation of this system. The reasoning presented in this legal opinion is mostly relevant for this potential extension of the purpose of the Entry/Exit System, in case such an extension would be considered, given that the DRI judgment itself concerned the case of personal data retained and processed for law enforcement purposes. Nevertheless, it goes without saying that even within their primary purpose, i.e. the management of external borders, the draft regulation must respect the Charter, and in particular Articles 7 and 8 thereof.

67. As concerns international agreements, we may just add that Article 218(11) TFEU foresees a special procedure by which the Parliament - as well as the Council, the Commission and the Member States - "*may obtain the opinion of the Court of Justice as to whether an agreement envisaged is compatible with the Treaties.*" Where the opinion of the Court is adverse, the agreement envisaged may not enter into force unless it is amended or the Treaties are revised.

68. In cases of doubt, the Parliament may thus consider this procedure for obtaining the opinion of the Court of Justice as to whether an agreement envisaged is compatible with the Charter. This would ensure that any doubts as to the compatibility of an envisaged international agreement with the Charter may be resolved, one way or another, by the Court before the agreement is concluded and thus binds the Union under international law. This obviates any future problems and difficulties that may later arise.[50]

As regards Member States' law

III.B.4. On the fourth question: ***Does this judgment produce any effect on Member States' law?*** And

III.B.5. On the fifth question: ***What would be the consequences of Member States' laws enacted to implement the data retention Directive, declared invalid from the Court as from 2006?***

69. Since the DRI judgment is limited to declaring the invalidity of the data retention Directive, it does not directly affect the validity of the national measures adopted to implement this Directive. Nevertheless, it is to be noted that this judgment produces a twofold effect as regards Member States' law.

70. Firstly, since the data retention Directive has been declared invalid and is no longer applicable, Member States no longer have any obligation to retain data by service providers of publicly available electronic communications services or of public communications networks, at least as long as no new act replacing the data retention Directive is adopted. It is therefore possible for a Member State to repeal the existing implementing measures, without any risk of violating Union law.

71. Secondly, if a Member State decides to maintain the rules on data retention in the electronic communications sector, such rules need to be in conformity with the Charter, and fulfil the requirements set out by the Court of Justice in the DRI judgment, to the extent that these national rules fall within the scope of application of the Charter, as defined in its Article 51(1).

72. Article 51 of the Charter states that the Charter applies "[...] *to the Member States only when they are implementing Union law*". This provision has been interpreted by the Court of Justice in the *Fransson* case: "*Since the fundamental rights guaranteed by the*

---

50 See Opinion 1/09 of the Court of Justice dated 8 March 2011, paragraph 48.
See also the Resolution of the European Parliament of 25 November 2014 on seeking an opinion from the Court of Justice on the compatibility with the Treaties of the Agreement between Canada and the European Union on the transfer and processing of Passenger Name Record data (2014/2966(RSP)).

Charter must therefore be complied with where national legislation falls within the scope of European Union law, situations cannot exist which are covered in that way by European Union law without those fundamental rights being applicable" (emphasis added).[51]

73. It is therefore necessary to examine whether the national rules related to data retention in the area of electronic communications fall within the scope of Union law, even if, as a result of the invalidity of the data retention Directive, they no longer transpose this act.

74. In this regard, it is necessary to underline the fact that processing of personal data in the internal market is regulated in Directive 95/46[52], while processing of personal data in the electronic communications sector is, more specifically,[53] regulated in Directive 2002/58 (hereinafter the "e-Privacy Directive")[54], which, *inter alia*, imposes on the Member States the obligation to ensure the confidentiality of communications (Article 5) and the obligation to erase traffic data[55] after it is no longer needed for the purpose of the transmission of a communication (Article 6). However, Article 15(1) of the e-Privacy Directive allows the Member States to restrict the scope of these two rights (and also some other rights mentioned therein), "*when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union*" (emphasis added).

75. These rules were applicable to data retention in the electronic communications sector before the data retention Directive, adopted in 2006, introduced a derogation "*from the system of protection of the right to privacy established by Directives 95/46 and 2002/58*".[56] In effect, Article 15(1) of Directive 2002/58 already gave Member States an "*option*" (i.e "... *Member States ...may... adopt legislative measures providing for the*

---

51 Cf. Case C-617/10, *Fransson*, *Ibid.*, paragraph 21.

52 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

53 The Advocate General explained, in paragraphs 34 of his Opinion in the DRI case, that the e-Privacy Directive "*particularises and complements*", to use the actual wording of Article 1(2) of the e-Privacy Directive, the system of protection of personal data established by Directive 95/46 by means of specific rules applicable to the electronic communications sector.

54 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

55 According to Article 2(b) of the e-Privacy Directive, "*traffic data*" means "*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*".

56 See paragraph 32 of the DRI judgment; see also paragraphs 39, 40 and 106 of the opinion of the Advocate General.

retention of data...") of restricting the scope of the right to the protection of personal data and of the right to privacy.

76. Directive 2002/58 later changed this "*option*" into an "*obligation*" to adopt national measures on data retention (at least with respect to Member States that had no legislation in that regard). It is therefore clear that, as a result of the invalidity of the data retention Directive, Article 15(1) of the e-Privacy Directive is, once again, applicable to the national measures dealing with data retention in the electronic communications sector.[57] That has two important consequences. Firstly, all national measures providing for data retention in connection with the provision of publicly available electronic communications services, fall necessarily within the scope of Article 15(1) of the e-Privacy Directive and have to fulfil all the requirements laid down in this provision (a restriction constituting "*a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences (...); the retention of data for a limited period (...); in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union*").

77. Secondly, being subject to Article 15(1) of the e-Privacy Directive, these national rules are implementing Union law, which entails the applicability of the Charter. In fact, where the Member States adopt national measures as exceptions provided for by Union law to the exercise of fundamental freedoms and rights, these measures have to comply with the Charter. This interpretation has recently been confirmed by the Court of Justice in the *Pfleger* case, where the Court clearly stated that: "*where it is apparent that national legislation is such as to obstruct the exercise of one or more fundamental freedoms guaranteed by the Treaty, it may benefit from the exceptions provided for by EU law in order to justify that fa ct only in so far as that complies with the fundamental rights enforced by the Court. That obligation to comply with fundamental rights manifestly comes within the scope of EU law and, consequently, within that of the Charter. The use by a Member State of exceptions provided for by EU law in order to justify an obstruction of a fundamental freedom guaranteed by the Treaty must, therefore, be regarded, as the Advocate General states in point 46 of her Opinion, as 'implementing Union law' within the meaning of Article 51(1) of the Charter*".[58]

78. As a result, Member States must ensure that the national measures dealing with data retention in the electronic communications sector are compatible with the Charter, and in particular with Articles 7, 8 and 52(1) thereof, as interpreted by the Court of Justice in the DRI judgment. This includes all the criteria set out by the Court of Justice in this judgment, as regards the proportionality of the interference, including the existence of "*clear and precise rules*" to limit the interference to what is "*strictly necessary*", as well as the inclusion of "*minimum safeguards*".[59]

---

57 This conclusion can also be drawn from the wording of Article 15(1)(a) of the e-Privacy Directive, added to this act by the data retention Directive, which explicitly excluded the latter Directive from the scope of application of paragraph 1 of Article 15 of the e-Privacy Directive, confirming thereby that the scope of application of both acts was similar. It is to be stressed that as a result of the invalidity of the data retention Directive, Article 15(1)(a) of the e-Privacy Directive no longer applies.

58 Case 390/12, *Pfleger*, EU:C:2014:281, paragraph 36.

59 See paragraph 54 of the DRI judgment.

79. In this respect, the DRI judgment could, in principle, have indirect consequences as regards the national measures, given that the same general legal considerations based on the Charter could be invoked to challenge the validity of the national acts too.

80. That said, these conclusions do not necessarily apply to other national measures, going beyond "*retention*" of data initially collected by private service providers for business purposes, and concerning rather a subsequent processing of the retained data by public authorities on grounds of public interest, such as, for example, the rules on the access and the use of such data by the law enforcement authorities of the Member States. If such national measures - adopted mostly in the area of criminal law or national security - fall outside of the scope of the e-Privacy Directive (see Article 1(3)) and the scope of Directive 95/46 (see Article 3(2), 1st indent), and unless they fall within the scope of Union law on another ground,[60] they will be considered as being outside of Union law[61] and, as a consequence, the Charter will not be applicable to them.[62]

81. However, it is worth mentioning that even in the areas where the Charter does not apply, the European Convention of Human Rights does. As a result, national legislation adopted in these areas will have to respect not only fundamental rights' standards resulting from domestic constitutions but also the Convention, as well as the well-developed case-law of the European Court of Human Rights, mentioned above, whose interpretation of the right to privacy and of the right to protection of personal data in cases of surveillance is very similar to the Court of Justice's reasoning in the DRI judgment (see paragraphs 41 to 48 above). National courts will thus continue to review national legislation according to these standards in any event.

82. As regards the standards of protection of the right to privacy and of the right to the protection of personal data in the Member States, it can therefore be argued that the final result to be arrived at by national courts may not, in practice, vary significantly in either event, given that the interpretations of the fundamental rights' provisions by both the Luxembourg and Strasbourg Courts tend to be aligned.[63]

---

60 For example if EU legislation is adopted on a legal basis under Title V of Part III of the TFEU, particularly in the field of judicial cooperation in criminal matters (Chapter 4) and police cooperation (Chapter 5).

61 See, by analogy, Cases C-317/04 and C-318/04, *Parliament* v *Council and Commission*, EU:C:2006:346, paragraph 58 and 59.

62 This may, however, also need to be reviewed if and when the draft Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM(2012)010) enters into force, since it will bring important changes to the Union's data protection law in the area of criminal law, in comparison to the act currently in force, i.e. Council Framework Decision 2008/977/JHA, of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60).

63 See, also, the decision of the Polish Constitutional Court of 30 July 2014 in which various provisions related to the access and processing of the retained telecommunications data by police and other law enforcement authorities were declared unconstitutional. Even if the contested provisions were not implementing the data retention Directive and were just indirectly related to this act, the Polish Constitutional Court decided to take the DRI judgment into account in its reasoning. See more at: http://trybunal.gov.pl/rozprawy/wyroki/art/7004-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/

III.B.6. On the sixth question: ***What would be the alternatives for the Member States?***

- ***Repealing their entire national data retention legislation?***
- ***Modifying their national data retention law in order to meet the "proportionality concerns" raised by the Court?***

83. As mentioned above, following the DRI judgment, Member States have a choice between repealing their national measures on data retention in the electronic communications sector or maintaining them (see subpart III.B.5. above).

84. If a Member States chooses the latter option, its national legislation should be examined to see whether it fulfils the requirements laid down in Article 15(1) of the e-Privacy Directive and whether it is compatible with Articles 7, 8 and 52(1) of the Charter, as interpreted by the Court of Justice in the DRI judgment. If this assessment concludes that the national legislation does not comply with these fundamental rights' requirements, this should lead to the amendment of the Member State's legislation.

85. In this regard, it is important to note that, despite the fact that they transpose the same Directive, national implementing measures differed considerably between the Member States, since the Member States enjoyed discretion as to how to adopt implementing measures for this Union act.[64] That is why the national measures implementing the data retention Directive must be examined individually, on a country-by-country basis.

86. To illustrate this fact, it is important to examine the effects the DRI judgment has produced in the Member States so far.

87. In fact, in at least one Member State, the national data retention law has already been replaced: a new act - the Data Retention and Investigatory Powers Act 2014 - was passed in the **UK** on 17 July 2014 in a fast-tracked legislative procedure.[65]

88. Some of the Member States have already assessed their respective national legislation in the light of the DRI judgment and have come to the conclusion that it was lawful.[66]

---

64 See, by analogy, Case C-275/06, *Promusicae*, EU:C:2008:54, paragraph 67 and the case-law quoted therein.

65 The Bill was first introduced in the House of Commons on 14 July 2014 before being introduced in the House of Lords two days later and the Act then received Royal Assent the next day on 17 July 2014, completing the whole legislative procedure in just 3 days. See more at: http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf. It is to be noted, however, that two MPs and Liberty, the civil rights' organisation, have announced their intention to seek judicial review of this Act, before the UK courts - see more at: https://www.liberty-human-rights.org.uk/news/press-releases/liberty-represents-mps-david-davis-and-tom-watson-legal-challenge-government%E2%80%99s-.

66 See, for example, in **Denmark**, the government presented an analysis to the Danish parliament, which comes to the conclusion that Danish retention law is not affected by the DRI judgment. See more at: https://edri.org/denmark-data-retention-stay-despite-cjeu-ruling/. This analysis prepared by the Ministry of Justice is available at: http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf.

89. However, before national governments could take any action following the DRI judgment, the constitutional courts of several Member States were called to rule on the validity of the national data retention laws. In **Austria**,[67] **Slovenia**[68] and **Romania**[69] the relevant national legislation was declared invalid shortly after the DRI judgment. In **Poland** various provisions related to the access and processing of the retained telecommunications data by police and other law enforcement authorities were declared unconstitutional by the Polish Constitutional Court.[70] In **Slovakia** the proceedings are still pending, but the Slovak Constitutional Court decided to suspend the applicability of some provisions of the national law on data retention as an interim measure.[71] Finally, the **Belgian** Constitutional Court has yet to rule on the validity of the recently adopted data retention law[72].[73]

90. Apart from the above-mentioned recent court rulings handed down after the DRI judgment (or initiated after this date but not yet finished), it is worth mentioning that the national data retention laws were declared invalid even before the Court of Justice gave its judgment in the DRI case, in a number of Member States (**Bulgaria** in 2008, **Romania** in 2009, **Germany** in 2010, **Cyprus** and the **Czech Republic** in 2011). As regards **Germany** in particular, since the German Constitutional Court annulled, in 2010,[74] legislation transposing the data retention Directive, no new legislation has been adopted.

Similarly, in **Sweden**, a group of experts appointed by Swedish Ministry of Justice concluded that the Swedish legislation on data retention is lawful. More info at: http://www.regeringen.se/sb/d/18311/a/242360.

67 On 27 June 2014 the Austrian Constitutional Court declared void the Austrian Act implementing the data retention Directive. See more at: https://www.vfgh.gv.at/cms/vfgh-site/attachments/1/5/8/CH0006/CMS1409900579500/presseinformation_verkuendung_vorratsdaten.pdf.

68 On 3 July 2014 the Slovenian Constitutional Court annulled Articles 162, 163, 164, 165, 166, 167, 168, and 169 of the Electronic Communications Act. Additionally, the Slovenian Court ordered the deletion of all the retained data in question right after the publication of the judgment. See more at: http://odlocitve.us-rs.si/usrs/us-odl.nsf/o/4AFCECAACABDD309C1257D4E002AB008.

69 The national data retention act (*Legea nr.82/2012 privind retinerea datelor*) was declared unconstitutional by the Romanian Constitutional Court on 8 July 2014. It must be recalled that it is for the second time that the Romanian Constitutional Court found that the national data retention act was inconsistent with the Romanian Constitution. See more at: http://www.ccr.ro/files/products/Decizia_440_20141.pdf.

70 See the decision of the Polish Constitutional Court of 30 July 2014 at: http://trybunal.gov.pl/rozprawy/wyroki/art/7004-okreslenie-katalogu-zbieranych-informacji-o-jednostce-za-pomoca-srodkow-technicznych-w-dzialani/.

71 Decision of 23 April 2014 of the Slovak Constitutional Court to suspend applicability of §58 (5-7) and §63 (6) of the law on electronic communications (*zákon č. 351/2011 Z. z. o elektronických komunikáciách).* See more at: http://portal.concourt.sk/plugins/servlet/get/attachment/main/ts_data/TI_info_30_14_dan_el_kom.pdf.

72 *La loi du 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90decies du Code d'instruction criminelle.*

73 See pending cases nr 5959 and nr 5856 lodged respectively by *La Ligue des droits de l'Homme, la Liga voor Mensenrechten* and by *Ordre des barreaux francophones et germanophones.*

74 Judgement of the Bundesverfassungsgericht of 2 March 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

91. This overview of the situation in the Member States shows clearly therefore that, even if the national governments and legislative bodies have a choice between maintaining national measures on data retention in the electronic communications sector or not, once they choose the latter option they must ensure that these measures respect not only their constitutional provisions on fundamental rights, but also the applicable Union law, and in particular, the Charter, in the light of requirements laid down by the Court in the DRI judgment. If they fail to do so, they run the risk of having their legislation annulled by the national courts, in a similar way to what has already happened in a number of Member States. This risk, which also existed before the DRI judgment, seems higher since the data retention Directive - which was the blueprint for the national laws - was declared invalid by the Court of Justice.

III.B.7. On the seventh question: ***Would the judgment have consequences on Member States' law requiring mass collection of personal data, storage and access of the data for law enforcement purposes, such as, for instance PNR or API legislation?***

92. As regards Member States' legislation other than the one dealing with data retention in the electronic communications sector, the analysis follows the same pattern as explained in paragraphs 77 to 88 above.

93. If the national measures requiring mass collection of personal data, storage and access of the data for law enforcement purposes fall within the scope of Union law[75] and thus the Charter is applicable to them, national courts might be called upon to examine the compatibility of these measures with the fundamental rights' standards set out in the Charter as interpreted in the DRI judgment. It is also possible, in such cases, that the national courts could make a request for a preliminary ruling to the Court of Justice.

94. If, on the other hand, the national measures in question are adopted in areas falling outside of the scope of Union law, national courts will rather refer to the fundamental rights' standards resulting from domestic constitutions, as well as from the European Convention of Human Rights, including the relevant case-law of the European Court of Human Rights.

95. Whether or not particular national measures requiring mass collection of personal data, storage and access of the data for law enforcement purposes fall within the scope of Union law, has to be examined on a case-by-case basis.

---

[75] See the *Fransson* case, cited above, on the interpretation of Article 51(1) of the Charter.

96. As regards **API** (Advance Passenger Information),[76] the Legal Service understands that the question refers to Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.[77] As a result, if and as long as the national legislation concerned implements this directive, it is to be considered as falling within the scope of Union law, which entails the application of the Charter.[78]

97. Concerning **PNR** (Passenger Name Record),[79] the Union has concluded bilateral agreements with some third countries related to the transfer of PNR.[80] However, given the fact that the proposal for an EU-PNR scheme[81] has not been adopted, the use of PNR data is not currently regulated at Union level in a general manner.[82] At national level, some Member States have adopted internal measures on the use of PNR.[83] If the proposed EU-PNR directive is adopted and enters into force, such national PNR measures could potentially then fall within the scope of Union law. Until that happens, the precise relationship between these national measures and Union law remains rather unclear at present and more information about these existing national rules would be needed before assessing them in detail, on a case-by-case basis.

---

76 API data are the biographical information taken from the machine-readable part of a passport and contain the name, place of birth and nationality of the person, the passport number and expiry date. They have more limited scope than PNR data.

77 OJ L 261, 6.8.2004, p. 24.

78 Although the wording of the question suggests that API data are processed for "*law enforcement purposes*", API data are principally processed, on the basis of Directive 2004/82/EC, for the purpose of carrying out checks on persons at external borders, and not for law enforcement purposes as such, even if this Directive does also foresee the latter purpose, under certain conditions, see Article 6(1), 5th subparagraph: "*In accordance with their national law and subject to data protection provisions under Directive 95/46/EC, Member States may also use the personal data referred to in Article 3(1) for law enforcement purposes.*"
The Charter would be applicable in both cases, whether data is processed for border management purposes or whether it is processed for law enforcement purposes "*subject to data protection provisions under Directive 95/46/EC*". However, the proportionality test under Article 52(1) of the Charter must take into account the specific objectives of general interest being pursued in each individual case. The assessment of the Court in the DRI judgment concerned specifically the processing of data for law enforcement purposes. A separate assessment would be needed for processing of data for border management purposes.

79 PNR is a record of each passenger's travel requirements which contains information necessary to enable reservations to be processed and controlled by the booking and participating air carriers for each journey booked by or on behalf of any person, whether it is contained in reservation systems, Departure Control Systems (DCS) or equivalent systems providing the same functionalities, see Article 2(c) of the Commission proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final. PNR data are of a broader scope than API.

80 See bilateral EU agreements with the United States (OJ L 215, 11.8.2012. p. 5), with Canada (OJ L 82, 21.3.2006. p. 15) and Australia (OJ L 186, 14.7.2012. p. 4).

81 Commission proposal for a directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, COM(2011) 32 final.

82 See Explanatory Memorandum of the Commission proposal, COM(2011) 32 final, *ibid*, p.4.

83 See Explanatory Memorandum of the Commission proposal, COM(2011) 32 final, *Ibid*, p.4, according to which within the EU, the United Kingdom already has a PNR system, while France, Denmark, Belgium, Sweden and the Netherlands have either enacted relevant legislation or are currently testing using PNR data.

III.B.8. On the eighth question: ***Would the judgment have consequences on international agreements concluded by any Member State with a third country and requiring mass collection of personal data and exchange of personal data for law enforcement purposes, for instance a bilateral agreement on PNR?***

98. Similarly to what has just been explained above about Member States' internal laws, the DRI judgment could also potentially have consequences for international agreements concluded by a Member State with a third country and requiring mass collection and exchange of personal data for law enforcement purposes, but only if such an agreement would implement Union law, within the meaning of Article 51(1) of the Charter.

99. However, a situation where a Member State concludes a bilateral agreement with a third country "*when they are implementing Union law*", would seem to arise in only quite exceptional circumstances.

100. The bilateral agreements between Member States and third countries which are envisaged by this eighth question, for instance a bilateral agreement on PNR,[84] would presumably have been concluded in the exercise of the competence of the Member States.[85] As a result, it is to be expected that, when concluding and applying such agreements, Member States would not normally be "*implementing Union law*" within the meaning of Article 51(1) of the Charter. Consequently the Charter would not be applicable to such agreements and so the DRI judgment would not then have any particular consequences in this regard. Nevertheless, such bilateral agreements (before adoption), or the measures taken by Member States to conclude them, as well as the measures taken to implement them in the national legal order, could be subject to judicial review by the national courts, according to the mechanisms of judicial redress applicable in the Member State concerned.

III.B.9. On the ninth question: ***Is Article 51 of the Charter applicable when the Member States adopt national measures which restrict the rights and obligations provided for in Directives 95/46/EC or 2002/58/EC for the purposes of safeguarding national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences (e.g. national law requiring mass collection of personal data)?***

101. As explained above (see paragraphs 78 and 83 above), Article 51(1) of the Charter, stating that the Charter applies "[...] *to the Member States only when they are implementing Union law*", should be interpreted as being applicable, in the light of the *Fransson* and *Pfleger* case-law of the Court of Justice, to national legislation adopted as exceptions provided for by the Union law.

---

84 As explained in the reply to the previous question, the use of PNR data is not currently regulated at Union level in a general manner.

85 Assuming, in the absence of any evidence to indicate the contrary, that Member States have acted entirely within their own competences, without encroaching in any way on the Union's competences under the Treaties.

102. As a result, the Charter is applicable to national measures which restrict the scope of specific rights and obligations provided for in Directive 95/46 and in the e-Privacy Directive, where these national measures fall within the scope of these two acts and in particular, of Article 15(1) of the e-Privacy Directive (as regards processing of data in the electronic communication sector) and of Article 13(1) of Directive 95/46 (as regards other areas of processing personal data). The Member States are therefore allowed to use these derogations only on limited grounds[86] and only where necessary.[87]

103. As regards, in particular "*national law requiring mass collection of personal data*", Article 15(1) of the e-Privacy Directive expressly mentions, as one of the possible national restrictive measures, that "*Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph*".

104. It is therefore clear that if certain national legislation falls within the scope of Article 15(1) of the e-Privacy Directive or of Article 13(1) of Directive 95/46, such as, for example, legislation on data retention measures in the electronic communications sector, it will have to comply with the Charter, as interpreted in the light of the DRI judgment.

IV. Conclusions

105. In the light of the foregoing, the Legal Service has reached the following conclusions:

General considerations

a) The Court's reasoning in the DRI judgment is based on the provisions of the Charter, and in particular Articles 7, 8 and 52(1) thereof. Consequently, the Court's reasoning in this particular case can only apply to other cases also if the Charter is applicable. In the case of other measures adopted by the EU legislature this will always be the case, but care must be taken in particular as regards other measures adopted by the Member States, given that Article 51(1) of the Charter provides that the Charter applies to the

---

86 According to Article 13(1) of Directive 95/46 these grounds are:
"*(a) national security;*
(b) defence;
(c) public security;
(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);
(g) the protection of the data subject or of the rights and freedoms of others."
The list of grounds justifying the restrictions is similar in Article 15(1) of the e-Privacy Directive. See, as regards the relation between the two provisions: Case C-275/06, *Promusicae, Ibid,* paragraphs 49-53.

87 See, in particular, Case C-473/12, *IPI*, EU:C:2013:715, paragraph 32: "[...][F]*urthermore, it is also apparent from the wording of Article 13(1) that the Member States may lay down such measures only when they are necessary. The requirement that the measures be 'necessary' is thus a precondition for the application of the option granted to Member States by Article 13(1), and does not mean that they are required to adopt the exceptions at issue in all cases where that condition is satisfied.*"

Member States "*only when they are implementing Union law*". It must therefore be established, as a preliminary consideration, whether or not Member States are implementing Union law.

b) The Court has declared that, where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, "*depending on a number of factors*", including, in particular, the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference. As in the DRI judgment, the EU legislature's discretion may then prove to be "*reduced*", in view of the important role played by the protection of personal data in the light of the fundamental right to respect for private life and the extent and seriousness of the interference with that right. If so, there will be a "*strict*" method of judicial review of that exercise of discretion. In such cases, a very careful review of the "*justification*" (including the necessity and proportionality) of any interference, under Article 52(1) of the Charter, will then be required.

c) In order to fully respect the principle of proportionality, the EU legislature must ensure that an interference with fundamental rights is "*precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary*". If this is not the case, then the measure in question may be declared invalid by the Court as being contrary to the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter. In particular, the EU legislature must provide for "*clear and precise rules*" to limit the interference to what is "*strictly necessary*", notably through the inclusion in the EU legislative act of "*minimum safeguards*" and "*sufficient guarantees*".

d) The DRI judgment presents a novel aspect in so far as the Court of Justice refers specifically to a particular body of the case-law of the European Court of Human Rights on the issue of "*general programmes of surveillance*". The Court of Justice has now effectively incorporated the same principles, stemming from this case-law of the European Court of Human Rights, into EU law in this same field. In view of the fact that the cited case-law of the European Court of Human Rights itself relates to a diverse category of surveillance measures (which is not at all limited to data retention issues), it is to be expected that the Court of Justice will, in future, also apply the same reasoning when assessing the validity, under the Charter, of other EU legislative acts in this same field of "*general programmes of surveillance.*"

As regards Union law

e) The DRI judgment itself concerns only the validity of the data retention Directive. It does not therefore have any direct consequences for the validity of any other EU act. Other existing EU acts benefit from a "*presumption*" of legality and so, formally, any other EU act will still remain valid, until such time as it is declared invalid following separate legal proceedings before the Court of Justice. The "*presumption*" of legality of EU acts can though be rebutted.

f) The validity of other EU acts must be assessed on a case-by-case basis, in the light of the particular circumstances of each case. In particular, the specific wording of the provisions of each act must be assessed in each case, in view of the particular objectives of general interest to be attained and the justifications advanced for each measure.

g) Other EU acts which also fall into the same category of "*general programmes of surveillance*" - as envisaged in the case-law of the European Court of Human Rights - will be subject to the same "*strict*" method of judicial review followed by the Court in the DRI judgment.

h) All new and pending EU legislative proposals which concern the special context of "*general programmes of surveillance*" must clearly now take account of the reasoning of the Court of Justice in the DRI judgment. Great care must therefore be taken in such cases to ensure full respect for the Charter.

i) The same considerations will apply also in the case of international agreements under negotiation, given that the EU legislature's discretion, in external relations, to conclude international agreements, under the Treaty and in accordance with the Charter, cannot be wider than the discretion, in internal matters, to adopt EU legislation applying within the EU legal order.

As regards Member States' law

j) The DRI judgment is limited to declaring the invalidity of the data retention Directive, so it does not directly affect the validity of the national measures adopted to implement this Directive. Nevertheless it may produce indirect effects on Member States' laws.

k) Firstly, Member States no longer have any obligation, but an option, to retain data in the electronic communications sector. They may therefore repeal their national legislation in this field.

l) Secondly, if a Member State decides to maintain the rules on data retention, it has to be examined whether or not such rules are in conformity with the Charter, and fulfil the requirements set out by the Court of Justice in the DRI judgment, to the extent that these national rules fall within the scope of application of the Charter, as defined in its Article 51(1).

m) Even if, following the DRI judgment, the data retention Directive is no longer applicable, national measures adopted to implement it now fall within the scope of Article 15(1) of the e-Privacy Directive and have to fulfil all the requirements laid down in this provision. As a result, these national rules are implementing Union law, which entails the applicability of the Charter. In this respect, the DRI judgment could, in principle, have indirect consequences as regards the national measures, given that the same general legal considerations based on the Charter could be invoked to challenge the validity of the national acts too.

n) Following the DRI judgment, Member States run an even higher risk than before of having their legislation annulled by the national courts, in a similar way to what has already happened in a number of Member States.

o) As regards other national measures requiring mass collection of personal data, storage and access of the data for law enforcement purposes, in case these measures fall within the scope of Union law, within the meaning of Article 51(1) of the Charter, national courts might be called upon to examine the compatibility of these measures with the

fundamental rights' standards set out in the Charter as interpreted in the DRI judgment. It is possible, in such cases, that the national courts could make a request for a preliminary ruling to the European Court of Justice.

p) If, on the other hand, the national measures in question are adopted in areas falling outside of the scope of Union law, national courts will rather refer to the fundamental rights' standards resulting from domestic constitutions, as well as from the European Convention of Human Rights, including the relevant case-law of the European Court of Human Rights.

q) A situation where a Member State concludes a bilateral agreement with a third country "*when they are implementing Union law*", would seem to arise in only quite exceptional circumstances. As a result, bilateral agreements concluded by the Member States with third countries requiring mass collection of personal data and exchange of personal data for law enforcement purposes would presumably have been concluded in the exercise of the competence of the Member States. Consequently the Charter would not be applicable to such agreements and so the DRI judgment would not then have any particular consequences in this regard.

r) If certain national legislation falls within the scope of Article 15(1) of the e-Privacy Directive or of Article 13(1) of Directive 95/46, such as, for example, legislation on data retention measures in the electronic communications sector, the Charter would be applicable to it, according to Article 51(1) thereof.

(signed) *(signed)* *(signed)*

Visa:

(signed)

(signed)

Annex: Request for a legal opinion of 27 October 2014