T. Van Canneyt, A. Bertrand, S. Crouzet & L. Vanderdonckt[1, 2]

Artikel

Data Protection: CJEU case law review – 1995-2020

Computerrecht 2021/56

1. Introduction

1. Since the adoption of Regulation 2016/679[3], EU data protection law has gone mainstream. Extensive and continuing media coverage has spiked the awareness about it in the larger public[4].

2. From the data subject's perspective, considering that data protection is a fundamental right in the European Union[5], this evolution is more than welcome and long overdue.

3. However, for controllers and processors, compliance with EU data protection law is not easy. It contains many principles which are *"necessarily relatively general since* [they have] *to be applied to a large number of very different situations"*.[6] What is required exactly to process personal data 'fairly and in a transparent manner' (Art. 5(1)(a) Regulation 2016/679)? What exactly should a controller be doing to meet its obligation to 'facilitate the exercise of data subject rights' (Art. 12(1) Regulation 2016/679)? And which concrete actions are required from a controller to comply with the principle of accountability (Art. 5(2) Regulation 2016/679)?

4. These questions are not always easy to answer. However, with the increased enforcement risk and the high fines introduced by Regulation 2016/679, it has become crucial for controllers and processors to know what is required of them to comply with their legal obligations.

5. The EU legislature certainly had its view regarding the meaning of these concepts, and the recitals of the relevant directives and regulations provide for some clarification. In addition, national supervisory authorities, the Article 29 Working Party ("WP29") and its successor, the European Data Protection Board ("EDPB"), have adopted and are currently adopting guidelines that clarify the obligations that flow from EU data protection law. However, while they have a lot of authoritative value, these guidelines are not legally binding.

6. Therefore, when it comes to the evolution of EU data protection law, it is the Court of Justice of the European Union ("CJEU"), which plays the determining role, and its role is increasingly becoming important.

7. After the adoption of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Directive 95/46")[7], it took five years before a first request for preliminary ruling relating to data protection was referred to the CJEU.[8] In the fifteen years that followed the adoption of Directive 95/46, national courts only referred eleven cases to the CJEU for a preliminary ruling.

8. Yet, in the last decade, we have witnessed a steady increase in the number of cases being referred to the CJEU. The fact that the Charter of Fundamental Rights of the European Union ("Charter")[9] became legally binding on 1 December 2009[10] has definitely been significant in this evolution. Contrary to the European Convention on Human Rights ("ECHR")[11], which only recognises the 'right to respect for private and family life'[12]. It also expressly recognises 'the right to data protection' as a fundamental right.[13]

9. Consequently, the CJEU is shaping more and more the meaning, and therefore also the direction, of EU data protection law. In recent years, it has adopted numerous landmark decisions that have substantially strengthened the rights of data subjects (e.g. the annulment of Directive

1 The authors are lawyers at Fieldfisher and members of the Brussels Bar. Alix Bertrand and Sixtine Crouzet are also members of the Paris bar.

2 This case law review takes into account all preliminary ruling decisions of the CJEU that relate to data protection until 31 December 2020.

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC [2016] OJ L119.

4 A Eurobarometer survey on data protection published one year after Regulation 2016/679 became applicable showed that out of 27.000 respondents in the EU, 67% had heard of the term 'GDPR' and 73% had heard of at least one data subject right guaranteed by Regulation 2016/679. See Special Eurobarometer 487a, https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/survey/getsurveydetail/instruments/special/surveyky/2222.

5 Article 8 of the Charter of Fundamental Rights of the European Union (2016) [2016] OJ C202.

6 Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraph 83. See also, judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 56.

7 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 [1995] OJ L281.

8 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294.

9 Charter of Fundamental Rights of the European Union [2016] OJ C202.

10 The Charter was proclaimed in Nice on 7 December 2000 but only became legally binding with the entry into force of the Lisbon Treaty on 1 December 2009.

11 European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5.

12 Article 8 of the ECHR.

13 Article 8 of the Charter.

2006/24[14] or the recognition of the right to be forgotten[15]), often with global ramifications (e.g. the invalidation of the adequacy decisions regarding Safe Harbour[16] and, more recently, the EU-US Privacy Shield[17]).

10. In this context, it is also striking that data protection decisions in the recent years are often adjudicated by the Grand Chamber. This shows the importance attached to data protection-related matters.[18] The data protection-related decisions of the CJEU have thus become essential for any data practitioner who wishes to interpret EU data protection law.

11. With this case law review, we aim to provide an in-depth analysis of the data protection-related preliminary rulings that the CJEU has adopted until now. Our case law review follows the structure of the main EU legal acts dealing with data protection. We begin with the Charter which is followed by an analysis of cases dealing with what one could call general data protection law. For ease of reference, the division of this chapter is based on the structure of Regulation 2016/679. In the fourth chapter, we analyse cases relating to Directive 2002/58.[19] We eventually conclude our case law review with Directive 2006/24.

2. Charter of fundamental rights of the EU

2.1 *General*

12. The Charter was proclaimed to assert many fundamental rights, freedoms and principles. With the Treaty of Lisbon's entry into force, the Charter has become legally binding. It has "*the same legal value as the Treaties*" according to Article 6 of the Treaty on European Union ("TEU") where it is incorporated by reference. The Charter is therefore part of EU primary law and is at the very top of the hierarchy of norms.

13. The Charter aimed at incorporating, among other rights, the fundamental rights recognised by the CJEU over the years, such as the principle of proportionality and the rights described further in this Chapter. In a series of landmark decisions issued in the early 1970s, the CJEU proactively recognized certain fundamental rights as general principles of law. By doing so, it ensured their observance within the EU legal order.[20] General principles of EU law are inspired either by the international treaties on human rights to which Member States are signatories or on which they have collaborated or by the constitutional traditions common to Member States. Particularly, the CJEU frequently relied on the ECHR signed in Rome on 4 November 1950 by the members of the Council of Europe, which includes the EU Member States. According to the Advocate General Sharpston, the ECHR "*enjoys a special position as a source of such* [fundamental] *rights; and the Court has particular regard to the case-law of the European Court of Human Rights*".[21] Nevertheless, while the fundamental rights guaranteed by the ECHR constitute general principles of EU law, "*the ECHR does not constitute, as long as the European Union has not acceded to it, a legal instrument which has been formally incorporated into EU law*".[22] After the Treaty of Lisbon, general principles of EU law continue to exist in parallel to the Charter.[23]

14. Given that Directive 95/46 predates the Charter, it only referred to fundamental rights guaranteed by the ECHR and by the constitutions of Member States. Therefore, in its decisions relating to Directive 95/46 and prior to the Charter's entry into force, the CJEU referred to the ECHR as interpreted by the case law of the European Court of Human Rights ("ECtHR").[24] In contrast, Regulation 2016/679 mentions the rights, principles and freedoms protected by the Charter, making any references to the ECHR superfluous.[25] However, because of its importance the ECHR continues to have an influence: Article 52(3) of the Charter provides that "*in so far as this Charter contains*

14 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 [2006] OJ L105. See Judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-283/12 and C-594/12, ECLI:EU:C:2014:238.

15 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317.

16 Judgment of 6 October 2015, *Schrems,* C 362/14, ECLI:EU:C:2015:650.

17 Judgment of 16 July 2020, *Facebook Ireland and Schrems,* C-311/18, ECLI:EU:C:2020:559.

18 Between 2018 and 2020, nine out of thirteen data protection related cases were adjudicated by the Grand Chamber: Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388; Judgment of 10 July 2018, *Jehovan Todistajat*, C-25/17, ECLI:EU:C:2018:551; Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788; Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773; Judgment of 24 September 2019, *Google*, C-507/17, ECLI:EU:C:2019:772; Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801; Judgment of 16 July 2020, *Facebook Ireland and Schrems,* C-311/18, ECLI:EU:C:2020:559; Judgment of 6 October 2020, *La Quadrature du Net*, Joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791; Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790.

19 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) [2002] OJ L201, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L337.

20 In this respect, the three most important cases are: (1) Judgment of 12 November 1969, *Erich Stauder v City of Ulm – Sozialamt, Verwaltungsgericht Stuttgart – Germany*, C-29-69, ECLI:ECLI:EU:C:1969:57, paragraph 7, (2) Judgment of 17 December 1970, *Internationale Handelsgesellschaft,* C-11/70, ECLI:EU:C:1970:114, paragraph 4 and (3) Judgment of 14 May 1974, *Nold KG v. Commission*, ECLI:EU:C:1974:51, ECR 491, paragraph 13.

21 Opinion of 17June 2010, *Volker und Markus Schecke GbR v Land Hessen*, Joined cases C-92/09 and C-93/09, ECLI:EU:C:2010:353, paragraph 64.

22 Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15, ECLI:EU:C:2016:970, paragraph 127. The CJEU referred to Article 6(3) TEU which reads as follows: "*Fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, shall constitute general principles of the Union's law*."

23 See Article 6(3) TFEU reproduced in the footnote above.

24 For example, Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, paragraph 71-91.

25 For example, Recital 4 provides a general list of rights, principles and freedoms enshrined in the Charter.

rights which correspond to rights guaranteed by the [ECHR], the meaning and scope of those rights shall be the same as those laid down by the said Convention (…)".

2.2 ***Scope of application limited to EU law***

15. The scope of the Charter is not absolute. In fact, according to Article 51, its provisions apply to "*the institutions, bodies, offices and agencies of the Union with due regard for the principle of subsidiarity and to the Member States only when they are implementing Union law*". It is noteworthy that the Charter does not change the scope of EU law. In other words, the Charter does not add any powers to the EU on top of those already defined in the Treaties.[26]

16. As clearly summarised by the CJEU, "*the fundamental rights guaranteed by the Charter must be respected where national legislation falls within the scope of EU law. In other words, the applicability of EU law entails the applicability of the fundamental rights guaranteed by the Charter*"[27]. For example, in *Willems*, the CJEU considered an EU Regulation as not applicable to the facts of the case that was referred, and therefore there was no need to determine the compatibility of national law provisions with the Charter.[28] In contrast, in *Tele2 Sverige*[29], the CJEU analysed a national law aimed at transposing Directive 2006/24, which it had declared invalid in *Digital Rights Ireland and Others*[30]. Here, the CJEU concluded that such a law fell in any case within the scope of Directive 2002/58. Consequently, the CJEU was authorised to apply the Charter.

17. Therefore, as far as data protection is concerned, if a national law falls under the scope of Directive 95/46, Directive 2002/58 or Regulation 2016/679 (and more generally any other EU legislation)[31], the CJEU has jurisdiction to interpret these directives or this regulation in light of the Charter and to respond to the questions of the referring court.[32]

18. An important consideration is that the extent of the scope of application of the Charter depends on the extent of the scope of EU law. According to the current CJEU President Lenaerts, "*metaphorically speaking, the Charter is the 'shadow' of EU law*".[33] Hence, where the CJEU has broadly interpreted the scope of EU law, this has in turn resulted in a broad applicability of the Charter. Accordingly, the CJEU held that the national measures adopted based on the margins of manoeuvre, exceptions and derogations provided for by EU law continue to fall within the scope of EU law. These must therefore comply with the fundamental rights enshrined in the Charter.[34] Therefore, a national law adopted based on a margin of manoeuvre provided for by Directive 95/46 or by Directive 2002/58 must still comply with the fundamental rights guaranteed by the Charter. This finding also applies to Regulation 2016/679, which, despite being a regulation and thus by definition not requiring to be incorporated into national law, contains a number of instances where Member States have a margin of manoeuvre. More importantly, authorities and courts of Member States must interpret secondary legislation in a manner that does not conflict with the fundamental rights of the EU.

2.3 ***Fundamental rights and the objectives of general data protection law***

19. Fundamental rights are at the core of both Directive 95/46 and Regulation 2016/679. References to fundamental rights appear in the very first recitals and articles, thereby demonstrating their importance.[35]

20. However, fundamental rights are opposed to the free flow of personal data. In fact, the objectives of Directive 95/46 and Regulation 2016/679 are twofold. On the one hand, they aim to ensure the free movement of personal data while on the other hand, they ensure the protection of fundamental rights of the individuals to whom the personal data relate.[36] This dual nature explicitly appears within the legal basis relied upon to enact Regulation 2016/679. The Treaty of Lisbon introduced, within Article 16(2) of the Treaty on the Functioning of the European Union ("TFEU")[37], a specific legal basis to allow the European Parliament and the Council to lay down per-

26 Article 51(2) of the Charter states as follows: "*the Charter does not extend the field of application of Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties*".

27 Judgment of 16 April 2015, *Willems and Others*,Joined cases C-446/12 and C-449/45, ECLI:EU:C:2015:238, paragraph 49. This decision follows the landmark decision: Judgment of 26 February 2013, *Åkerberg Fransson*, C-617/10, ECLI:EU:C:2013:105, paragraphs 20 and 22.

28 Judgment of 16 April 2015, *Willems and Others*, Joined cases C-446/12 and C-449/45, ECLI:EU:C:2015:238, paragraphs 48-50.

29 Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15, ECLI:EU:C:2016:970, paragraph 81.

30 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C-594/12, ECLI:EU:C:2014:238.

31 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559, paragraph 99.

32 For a recent case where the CJEU decided it did not have jurisdiction, see Judgment of 10 December 2020, *J&S Service*, C-620/19, ECLI:EU:C:2020:1011.

33 K. LENAERTS, "The ECHR and the CJEU: Creating Synergies in the Field of Fundamental Rights Protection", Solemn hearing for the opening of the Judicial Year of the ECtHR, 26 January 2018, https://www.echr.coe.int/Documents/Speech_20180126_Lenaerts_JY_ENG.pdf.

34 The landmark case is *ERT*: Judgment of 18 June 1991, *ERT*, C-260/89, ECLI:ECLI:EU:C:1991:254, paragraph 43.

35 Article 1 and Recital 1 of Regulation 2016/679; Article 1 and Recital 3 of Directive 95/46. This objective was restated in Judgment of 6 November 2003, *Lindqvist*, C-101/01, paragraph 96.

36 Recital 3 of Directive 95/46 and Recitals 12 and 166 as well as Article 1 of Regulation 2016/679.

37 Consolidated version of the Treaty on the Functioning of the European Union of 26 October 2012, OJ L. 326/47-326/390.

sonal data protection rules and rules governing the free movement of personal data.[38]

21. The CJEU highlighted in *Österreichischer Rundfunk* that "*Directive 95/46 itself, while having as its principal aim to ensure the free movement of personal data, provides in Article 1(1) that Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data*".[39] As the CJEU noted as early as 2003, "*those* [two] *objectives may of course be inconsistent with one another*".[40] However, the CJEU considered that Directive 95/46 already included mechanisms that reconciled these two objectives to the extent that it determined the conditions and safeguards under which the processing of personal data was lawful.[41] These objectives are essential insofar as they are taken into account by the CJEU when interpreting the provisions of Directive 95/46 and Regulation 2016/679. Hence, national measures stemming from the margins of manoeuvre that Member States have under Directive 95/46 must also comply with the "*objective of maintaining a balance between the free movement of personal data and the protection of private life*".[42]

22. Against this background, the Charter is integral to the CJEU's decisions regarding data protection, even though it is relatively recent.

2.4 *Respect for private and family life and protection of personal data*

2.4.1 *General*

23. Prior to the Charter, the CJEU considered the right to privacy as one of the general principles of EU law in the 80s and 90s.[43] However, according to Advocate General Ruiz-Jarabo Colomer, the case law of the CJEU was "*divergent and delivered on a case-by-case basis*" at the time. Directive 95/46 enabled the CJEU to find a "*more solid foundation on which to base its decisions* (…). *In short, Directive 95/46 develops the fundamental right to privacy in so far as it affects the automatic processing of personal data.*"[44]

24. The right to respect for private and family life is now protected by Article 7 of the Charter, which states that "[e]*veryone has the right to respect for his or her private and family life, home and communications*". The right to protection of personal data is guaranteed by both Article 8(1) of the Charter and Article 16(1) of the TFEU. These Articles state that everyone has the right to protection of personal data concerning them. According to the CJEU's case law, these two fundamental rights are closely connected.[45] The CJEU made it clear that "*the right to respect for private life with regard to the processing of personal data concerns any information relating to an identified or identifiable individual*".[46]

25. However, it is noteworthy that in *Volker and Markus Schecke*, where two EU regulations required the publication of the names of legal persons as beneficiaries of agricultural aid, the CJEU considered that legal persons can benefit from the protection of Articles 7 and 8 of the Charter "*only in so far as the official title of the legal person identifies one or more natural persons*". In this case, the CJEU concluded that the official title of the partnership "*directly identifies*" the partners who are natural persons.[47]

26. The fundamental right enshrined in Article 7 of the Charter is equivalent to that of Article 8 of the ECHR (right to respect for private and family life). However, Article 8 of the Charter *"concerns a fundamental right which is distinct from that enshrined in Article 7 of the Charter and which has no equivalent in the ECHR*".[48] According to Advocate General Sharpston, these two separate rights can be differentiated as follows: "*a classic right (protection of privacy under Article 8 ECHR) and a more modern right (the data protection provisions of Convention No 108)*".[49]

27. These fundamental rights are not absolute. In the CJEU's words, they "*must be considered in relation to* [their] *function in society*".[50] Therefore, they may be limited under the conditions listed by Article 52(1) of the Charter as analysed below. Additionally, Article 8(2) of the Charter authorises processing of personal data, if such data is processed "*fairly for specified purposes and on the basis of the*

38 This Article states: "*The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities*". By contrast, Directive 95/46 was adopted on the basis of Article 114 of the TFEU, known as the legal basis for the internal market.

39 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, paragraph 70.

40 Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraph 79.

41 Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraph 82.

42 Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraph 97.

43 Opinion of 22 December 2018, *Rijkeboer*, C-553/07, ECLI:EU:C:2008:773, paragraph 19 and case law cited.

44 Opinion of 22 December 2018, *Rijkeboer*, C-553/07, ECLI:EU:C:2008:773, paragraphs 20-21.

45 Judgment of 24 November 2011, *ASNEF*, C-468/10, ECLI:EU:C:2011:777, paragraph 41 and case law cited.

46 Judgment of 17 October 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670, paragraph 26.

47 Judgment of 9 November 2010, *Volker und Markus Schecke*, C-92/09 and C-93/09, ECLI:EU:C:2010:662, paragraphs 53-54.

48 Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15, ECLI:EU:C:2016:970, paragraph 129.

49 Opinion of 17June 2010, *Volker und Markus Schecke GbR v Land Hessen*, Joined cases C-92/09 and C-93/09, ECLI:EU:C:2010:353, paragraph 71.

50 Judgment of 5 May 2011, *Deutsche Telekom AG*, C 543/09, ECLI:EU:C:2011:279, paragraph 51 and case law cited.

consent of the person concerned or some other legitimate basis laid down by law".[51] According to Advocate General Kokott, this principle of purpose limitation embodies the "*requirement of foreseeability*".[52]

28. As explained below, the CJEU frequently referenced these two rights to interpret the provisions of Directives 95/46 and 2002/58 and Regulation 2016/679 (Section 2.4.2) and to carry out balancing tests between them and/or other interests or freedoms (Sections 2.4.3 and 2.4.4).

2.4.2 *Interpretation in specific domains*

29. In many decisions, the CJEU has stressed the importance of protecting fundamental rights, specifically the right to privacy.[53] Since *Österreichischer Rundfunk* in 2003, the CJEU has repeatedly held that "*the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights*".[54] In *Schrems,* the CJEU outlined the high threshold of protection that must be afforded to the right to privacy: "*that directive seeks to ensure not only effective and complete protection of the fundamental rights and freedoms (…), in particular the fundamental right to respect for private life with regard to the processing of personal data, but also a high level of protection of those fundamental rights and freedoms. The importance of both (…) Article 7 of the Charter, and (…) Article 8 thereof, is, moreover, emphasised in the case-law of the Court*".[55]

30. The protection of these rights is necessary when an interference or limitation exists. The existence of an interference is broadly understood regardless of whether the concerned data is sensitive or whether the interference causes adverse consequences to the individual in question.[56] Furthermore, the CJEU clarified that any processing of personal data might constitute a threat to Articles 7 and 8 of the Charter.[57]

(a) *Articles 7 and 8 of the Charter and the retention and access to electronic communications data*

31. There are numerous decisions in which the CJEU examined the compatibility with the Charter of legislations imposing on certain entities an obligation to retain data and/or allowing access to communications data by public authorities. These decisions covered both EU and national legislations.

32. In *Digital Rights Ireland and Others*, the CJEU declared Directive 2006/24/EC invalid. This directive required the retention of certain data of subscribers or registered users by providers of electronic communications services. It also allowed competent national authorities to access those data to fight serious crime and ensure public security. The CJEU found that such a retention obligation and access both constituted a "*wide-ranging*" and "*particularly serious*" interference with Articles 7 and 8 of the Charter as the concerned individuals could feel that they were subject to "*constant surveillance*".[58] To assess whether these interferences are justified, the CJEU applied a strict judicial review, analysing whether the conditions of Article 52(1) of the Charter were fulfilled.[59] It found that "*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*". To reach this finding, the CJEU noted that said retention was general and indiscriminate as it affected all persons, means of electronic communications and traffic data with no exception nor limitation[60]. The principle of proportionality, however, required that under EU law, derogations and limitations to the fundamental right of protection of personal data "*must apply only in so far as is strictly necessary*".[61] To that end, "*clear and precise rules*" must be laid down within the EU legislation to define the scope and application of the measure concerned and impose "*minimum safeguards* (…) *to effectively protect [individuals']* (…) *personal data against the risk of abuse and against any unlawful access and use of that data*".[62]

33. In *Tele2 Sverige*[63], the CJEU interpreted Article 15(1) of Directive 2002/58 in light of the rights enshrined

51 Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, paragraph 40.

52 Opinion of 18 July 2007, *Promusicae*, C-275/06, ECLI:EU:C:2007:454, paragraph 53.

53 For example, Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 47 and the case law cited; judgment of 8 April 2014, *Digital Rights Ireland and Others*, C-293/12 and C 594/12, ECLI:EU:C:2014:238, paragraph 53; and *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraphs, 53, 66, 74 and the case law cited.

54 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, paragraph 68; Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 68; Judgment of 17 July 2014, *YS and others*, C-141/12, ECLI:EU:C:2014:208, paragraph 54; Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 38 (with respect to the right to respect for private life).

55 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 39.

56 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 33 and the case law cited; confirmed in Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 87; Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraph 51; Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 116.

57 Judgment of 17 October 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670, paragraph 25.

58 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraphs 34-37.

59 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 48.

60 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraphs 57-58.

61 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 52.

62 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 54.

63 Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15,ECLI:EU:C:2016:970.

in Articles 7, 8 and 11 of the Charter in the context of a retention obligation which was general and indiscriminate. Relying on *Digital Rights Ireland and Others*, the CJEU noted that national laws imposing an obligation to retain traffic and location data and allowing access to the retained data by public authorities for fighting crime caused a serious interference to these rights. This was because the retained data was "*liable to allow very precise conclusions to be drawn concerning the private lives of the persons*".[64] Pursuant to the principle of proportionality, only the purpose of fighting serious crime could justify such a far-reaching interference.[65]

34. In *Ministerio Fiscal*, the CJEU noted that public authorities' access to data relating to SIM cards activated with stolen phones constituted an interference with Articles 7 and 8 of the Charter.[66] However, applying the principle of proportionality, this interference was justified by the objective of fighting crime, and the data did not allow precise conclusions to be drawn concerning the private lives of the SIM card owners.[67]

35. In two recent decisions, the CJEU confirmed *Digital Rights Ireland and Others* and *Tele2 Sverige* by asserting the incompatibility with the Charter of national preventive measures requiring the retention of traffic and location data or its transmission to security and intelligence agencies.[68] However, the CJEU carried out a more nuanced analysis in *La Quadrature du Net*.[69]

(b) *Articles 7 and 8 of the Charter and international transfers of data*

36. The rights enshrined in Articles 7 and 8 of the Charter are essential for assessing the validity of transfers of personal data to third countries outside of the European Economic Area and the level of protection of personal data in third countries[70].

(i) Adequacy decisions

37. Article 25(6) of Directive 95/46 allowed the European Commission to adopt a decision to determine that a third country "*ensures an adequate level of protection* (…) *by reason of its domestic law or of the internal commitments it has entered into* (…) *for the protection of the private lives and basic freedoms and rights of individuals*" ("adequacy decision"). The CJEU viewed the latter provision as an implementation of the right to protection of personal data.[71] The term "*adequate*" requires the level of protection of fundamental rights and freedoms in the third country at issue to be "*essentially equivalent*" – as opposed to identical – to the level of protection guaranteed within the EU by Directive 95/46 read in conjunction with the Charter.[72] Failing this interpretation, the level of protection guaranteed in the EU legal order would be easily circumvented when personal data is transferred to third countries.

38. In *Schrems*, the CJEU declared the first adequacy decision concerning the United States (Decision 2000/520 or "Safe Habour") invalid.[73] It conducted a strict judicial review of the margin of discretion enjoyed by the European Commission when it adopted the Safe Habour, considering "*the important role played by the protection of personal data (…) and, (…)* [of] *the large number of persons whose fundamental rights are liable to be infringed where personal data is transferred to a third country not ensuring an adequate level of protection*".[74] The CJEU found that the Safe Harbour enabled an interference with Articles 7 and 8 of the Charter by allowing the national security and public interest requirements of US laws to prevail over the data protection principles set out therein and with which organisations transferring personal data under the Safe Harbour had to comply. Even though this interference was of "*general nature*", the Safe Harbour failed to include any mechanism to limit it.[75] Referring to the *Digital Rights Ireland and Others* decision, the CJEU recalled that under the protection level of fundamental rights guaranteed in the EU, the EU legislations involving interferences with Articles 7 and 8 of the Charter must "*lay down clear and precise rules*" to define the scope and application of the limitation and must provide sufficient safeguards.[76] Such legislations must be limited to what is strictly necessary, which is not the case of a general authorisation allowing the storage of transferred personal data "*without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subse-*

64 Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15, ECLI:EU:C:2016:970, paragraphs 99-100.
65 Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15, ECLI:EU:C:2016:970, paragraphs 102 and 115.
66 Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraph 51.
67 Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraph 60.
68 Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraphs 81-82.
69 See Section 4.5.2 below. Judgment of 6 October 2020, *La Quadrature du Net*, Joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, paragraphs 168 and 192.
70 See also Recommendations 02/2020 of the EDPB on the European Essential Guarantees for surveillance measures, 10 November 2020 and Recommendations 01/2020 of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 November 2020, version for public consultation.
71 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 72.
72 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 73.
73 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 106.
74 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 75.
75 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraphs 87-88.
76 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 91

quent use, for purposes which are specific, strictly restricted and capable of justifying the interference".[77]

39. Article 45 of Regulation 2016/679 continues to allow the European Commission to adopt adequacy decisions when it concludes that a third country ensures an adequate level of protection. The terms "*essentially equivalent*" have been incorporated in Recital 104 of this Regulation. Following *Schrems*, the European Commission adopted a new adequacy decision (Decision 2016/1250 or "Privacy Shield") for transfers of personal data to the United States.

40. In *Facebook Ireland and Schrems*, the CJEU ruled that the Privacy Shield violated Article 45 of Regulation 2016/679 read in light of the Charter and thus invalidated it. It indeed disagreed with the finding of the European Commission that the US ensured an adequate level of protection.[78] It explained that Articles 7, 8 and 47 of the Charter "*contribute*" to the required level of protection and therefore, the Commission must establish that the concerned third country complies with them.[79] Similarly to *Schrems*, the CJEU found that the Privacy Shield enabled interferences with these fundamental rights on grounds of national security and public interest requirements or based on domestic legislation of the US. Even if these rights are not absolute, the CJEU found that the applicable US legislations allowing US public authorities access to transferred data for surveillance purposes did not comply with the principle of proportionality protected by Article 52(1) of the Charter. In other words, the applicable US surveillance legislations were not limited to what was strictly necessary.[80]

(ii) Standard Contractual Clauses

41. In *Facebook Ireland and Schrems*, the CJEU interpreted Article 46(1) of Regulation 2016/679. This Article states that in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country only if the controller or processor has provided "*appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available*". Among other mechanisms, such appropriate safeguards can be established by adopting the standard contractual clauses issued by the European Commission ("SCC"). According to the CJEU, when it comes to reliance on the SCC, the level of protection required by Articles 46(1) and 46(2)(c)) must be essentially equivalent to the one guaranteed by Regulation 2016/679 read in light of the Charter.[81] The level of protection might result from both the SCC concluded between the exporter and importer of personal data and "*the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2)*"[82].

42. The CJEU examined the validity of the SCC adopted by the Commission (Decision 2010/87) in light of Articles 7, 8 and 47 of the Charter and refused to invalidate it. In fact, the CJEU found that pursuant to this decision, the exporter and importer are required to verify that the level of protection required under EU law is complied with in the concerned third country.[83] Furthermore, if the importer is unable to comply with the SCC, it must inform the exporter which is in turn required to suspend the data transfer and/or terminate the SCC. However, the CJEU found that given the contractual nature of the SCC, they are unable to "*bind the public authorities of third countries*". Therefore, it might be necessary for the exporter and importer to adopt "*supplementary measures*" to ensure an essentially equivalent level of protection.[84]

(c) *Article 8 of the Charter and the right of access*

43. The right of access is expressly set out in Article 8(2) of the Charter. As highlighted by Advocate General Ruiz-Jarabo Colomer, the Charter "*places* [the right of access] *at the very heart of the fundamental right to privacy*".[85]

44. The CJEU construed the right of access favourably for data subjects considering the objective of Directive 95/46. In fact, it invoked the importance of protecting the right to privacy of Article 8 of the Charter to hold that the fees that might be asked by controllers from data subjects exercising their right of access under Article 12(a) might not be set at "*a level likely to constitute an obstacle to the exercise of the right of access guaranteed by that provision*". This would not be applicable to a fee amounting to the cost of communicating personal data.[86] In contrast, in *YS and others*, the CJEU relied on Directive 95/46's objective of protecting data subjects' right to privacy to refuse the extension of the scope of the right of access. In fact, extending the right of access exercised by applicants for a residence permit to the legal analysis drafted during the administrative procedure would imply guaranteeing them

77 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraphs 92-93

78 Judgment of 16 July 2020, *Facebook Ireland and Schrems,* C-311/18, ECLI:EU:C:2020:559, paragraph 185.

79 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559, paragraphs 169 and 186.

80 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559, paragraphs 168-184.

81 Judgment of 16 July 2020, *Facebook Ireland and Schrems,* C-311/18, ECLI:EU:C:2020:559, paragraph 105.

82 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559, paragraph 105.

83 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559, paragraph 142.

84 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559, paragraphs 132 and 133.

85 Opinion of 22 December 2018, *Rijkeboer*, C-553/07, ECLI:EU:C:2008:773, paragraph 23.

86 Judgment of 12 December 2013, *X*, C-486/12, ECLI:EU:C:2013:836, paragraphs 28-30.

the right of access to administrative documents but not the right to privacy.[87]

2.4.3 *Articles 7 and 8 of the Charter and the balancing test regarding legitimate interests*

45. The legitimate interest of the controller or of a third party constitutes one of the lawful grounds listed in both the repealed Directive 95/46 (Article 7(f)) and Regulation 2016/679 (Article 6(f)). In both legislations, "*the fundamental rights and freedoms of the data subject*" need to be considered when determining whether the data controller could rely on its legitimate interest as a legal ground. According to the CJEU, this "*necessitates a balancing of the opposing rights and interests concerned which depends, in principle, on the individual circumstances of the particular case in question and in the context of which the person or the institution which carries out the balancing must take account of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter (…)*".[88]

2.4.4 *Articles 7 and 8 of the Charter and the balancing test regarding the right to erasure*

46. The right to erasure (or right to be forgotten) is another prime example of a balancing exercise in which the right to respect for private life or to the protection of personal data is opposed to other rights or interests.

47. In *Google Spain and Google*, the CJEU considered that an internet search based on a data subject's name provided a "*structured overview of the information relating to that individual*" which corresponds to a "*detailed profile*" of that data subject.[89] Such processing entails a potentially serious interference with Articles 7 and 8 of the Charter given the significant role of search engines and the Internet in making information available.[90] The CJEU ruled that when a data subject requests to be delisted from the results displayed by a search engine operator, "a *fair balance*" should be struck between their fundamental rights and the interest of internet users.[91] The CJEU provided guidance on the outcome of this balancing exercise.[92]

48. Regulation 2016/679 incorporated this balancing test in Article 17(3)(a) by excluding the application of the right to erasure "*for exercising the right of freedom of expression and information*" as analysed in the following section.

49. In *Manni*, the CJEU carried out a balancing exercise between Articles 7 and 8 of the Charter and the economic interests of ensuring the proper functioning of the internal market, which an EU Directive on the disclosure of company documents served. The Directive indeed required that the personal data of certain individuals appear in the companies' register kept by the chamber of commerce. The CJEU ruled that such individuals did not have, as a matter of principle, the right to obtain the erasure or blocking of these data included after a certain period following the dissolution of the concerned company.[93] In the CJEU's opinion, this interpretation did not cause a disproportionate interference with Articles 7 and 8 of the Charter as the economic interests prevailed.[94] First, the relevant EU directive only required a limited volume of personal data to be included in the company register. Furthermore, the disclosure of such data was justified by the risk associated with the companies at issue. However, in certain circumstances, there might be overriding and legitimate reasons that exceptionally justify limiting access to the concerned personal data. That is, national legislatures can limit the access on a case-by-case basis.[95]

2.5 ***Freedom of expression and information***

2.5.1 *General*

50. The freedom of expression and information is protected under Article 11 of the Charter.[96] The freedom of information includes the right to receive and impart information.[97] It is equivalent to Article 10 of the ECHR.[98] This freedom is crucial as it constitutes, in the CJEU's words, "*one of the essential foundations of a pluralist, democratic society, and is one of the values on which, under Article 2 TEU, the Union is founded*".[99]

51. This freedom is often opposed to the rights to privacy and protection of personal data against which it has been balanced as demonstrated below through two different balancing exercises.[100]

87 Judgment of 17 July 2014, *YS and Others*, C-141/12, ECLI:EU:C:2014:208, paragraph 46.
88 Judgment of 24 November 2011, *ASNEF*, C-468/10, ECLI:EU:C:2011:777, paragraph 40; confirmed in Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C 708/18, ECLI:EU:C:2019:1064, paragraphs 32 and 52.
89 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 80.
90 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 80.
91 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 81.
92 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 97. See Section 3.3.5(b) below.
93 Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, paragraph 56.
94 Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, paragraph 57.
95 Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, paragraphs 58-61.
96 Article 11 of the Charter provides that "*1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. 2. The freedom and pluralism of the media shall be respected.*"
97 Judgment of 24 November 2011, *Scarlet Extended SA*, C-70/10, ECLI:EU:C:2011:771, paragraph 50.
98 Recital 37 of Directive 95/46 refers to Article 10 of the ECHR.
99 Judgment of 21 December 2016, *Tele2 Sverige*, C-203/15, ECLI:EU:C:2016:970, paragraph 93 and case law cited.
100 For example, see judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773 and judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C 73/07, ECLI:EU:C:2008:727, as analysed below.

52. However, these rights are not systematically opposed. For instance, in *Scarlet Extended*, the referring court asked the CJEU to interpret the applicable EU legislation with respect to Articles 8 and 11 of the Charter to assess the compatibility of an injunction imposed by a national court on an internet service provider. This provider had to install a filtering system of electronic communications for identifying and blocking the transfer of shared files which infringe copyright.[101] The CJEU balanced these two rights against the right to intellectual property and concluded that the injunction did not strike a fair balance between these rights. Hence, EU law precluded such an injunction.

2.5.2 *Article 11 of the Charter and the balancing test regarding the right to erasure*

53. As explained previously, *in Google Spain and Google*, the CJEU examined a request for delisting and held that there should be a fair balance under Directive 95/46 between the "*interest of the general public in finding that information*" through an internet search and the fundamental rights of the data subject requesting delisting.

54. Regulation 2016/679 incorporated this balancing exercise in Article 17(3)(a). However, instead of referring to a mere "interest" of the general public in finding information online, this provision now refers to the right of freedom of expression and information. The CJEU considered that this provision "*expressly lays down the requirement to strike a balance between (…) Articles 7 and 8 of the Charter, on the one hand, and the fundamental right of freedom of information guaranteed by Article 11 of the Charter, on the other*".[102]

2.5.3 *Article 11 of the Charter and the balancing test regarding processing for journalistic purposes*

55. Article 9 of Directive 95/46 introduced some margins of manoeuvre for Member States with regard to the processing for journalistic purposes. It stated that "*Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression*". This article thus required Member States to reconcile two fundamental rights, namely the rights to privacy and to freedom of expression.[103] The same balancing exercise is foreseen by Regulation 2016/679, with an increased number of articles for which exemptions and derogations can be adopted.[104] For a detailed analysis of the specific provisions relating to the processing for journalistic purposes, refer to Section 3.9.2 below.

In *Satakunnan Markkinapörssi*, the CJEU stressed that to protect the fundamental right to privacy, Member States must adopt only strictly necessary derogations and limitations under Article 9 of Directive 95/46. Simultaneously, the CJEU considered that it was necessary to interpret the "*notions relating to that freedom, such as journalism, broadly*" with respect to the importance of the freedom of expression in a democratic society.[105]

2.6 ***Right to an effective remedy and to a fair trial***

57. The right to an effective remedy and to a fair trial is enshrined in Article 47 of the Charter. Its first two paragraphs state that "[e]*veryone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article*" and "[e]*veryone is entitled to a fair and public hearing within a reasonable time (…)*". According to the CJEU, this right reaffirms the principle of effective judicial protection,[106] intends to ensure compliance with EU law and is "*inherent in the existence of the rule of law*".[107]

58. The CJEU applied this article in the context of Directive 95/46, which also provides for the right to a judicial remedy.[108] In *Puškár*, the CJEU stated that EU Member States must comply with Article 47 when they establish procedural rules for legal actions to ensure protection of the rights conferred by Directive 95/46.[109] This case related to an individual whose right to protection of personal data had been infringed but whose legal action faced two national procedural rules. First, the admissibility of his legal action was made conditional upon the prior exhaustion of other available remedies. Second, a list with personal data produced by the individual was dismissed as evidence because it was obtained without consent of the controller in charge of that list. According to the CJEU, the two procedural rules constituted separate interferences with the right to an effective remedy. The conditions of Article 52(1) of the Charter therefore had to be fulfilled for these two limitations to be justified as explained below.[110] The CJEU ruled that the first procedural rule was provided for by law and respected the essence of the infringed right.

101 Judgment of 24 November 2011, *Scarlet Extended SA*, C-70/10, ECLI:EU:C:2011:771, paragraph not numbered.
102 Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773, paragraph 57.
103 Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122, paragraph 50 and Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraphs 52 to 54.
104 Recital 153 and Article 85 of Regulation 2016/679.
105 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraph 56.
106 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraph 59.
107 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 95.
108 Article 22 of Directive 95/46.
109 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraph 59.
110 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraphs 62 and 87-89.

It also concluded that it served an objective of general interest but left it to the referring court to examine whether it disproportionately affected the right to an effective remedy[111]. Furthermore, it stressed that this procedural rule should suspend the applicable statute of limitation and must not lead to a "*substantial delay in bringing a legal action (…)* [or] *involve excessive costs*".[112] As to the second limitation, the CJEU left it for the referring court to determine whether it was justified under Article 52(1) of the Charter, and particularly whether it did not disproportionately affect the right to an effective remedy.[113]

59. In *Schrems,* a national supervisory authority had rejected an individual's complaint on the ground that his rights and freedoms were violated by the transfer of personal data to the United States as these transfers were based on the adequacy decision of the Safe Harbour. Considering the powers of supervisory authorities[114] and Article 47 of the Charter, the CJEU considered that when national supervisory authorities examine such a claim and reject it on the ground that it is unfounded, the claimant must "*have access to judicial remedies enabling him to challenge such a decision adversely affecting him before the national courts*".[115] Hence, national courts "*must stay proceedings and make a reference to the Court for a preliminary ruling on validity where they consider that one or more grounds for invalidity put forward by the parties or, as the case may be, raised by them of their own motion are well founded*".[116] The European Commission's adequacy decision does not prevent authorities from examining such a claim.[117]

60. Finally, in *Schrems* and then in *Facebook Ireland and Schrems*, the CJEU took into account the interference with the right to an effective remedy when invalidating the relevant provisions of the Safe Harbour and the Privacy Shield.[118] When assessing the validity of the Safe Harbour, the CJEU ruled that a "*legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter*".[119] Furthermore, the CJEU found that under the Privacy Shield, the ombudsperson mechanism set up therein is not sufficient to comply with the requirements of Article 47 of the Charter.[120]

2.7 *Scope of guaranteed rights*

61. Limitations can be imposed on the rights and freedoms guaranteed by the Charter if the four cumulative conditions set out in Article 52(1) are met. Concretely, the limitation at issue must (1) be provided by law, (2) respect the essence of the limited rights and freedoms, (3) pursue objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others and (4) comply with the principle of proportionality. To comply with this principle, the limitation must be appropriate to attain said objective and must not go beyond what is necessary to achieve it.[121]

62. The first condition is typically not problematic.[122] The Court clarified in *Facebook Ireland and Schrems* that this condition implies that "*the legal basis which permits the interference with* [the fundamental] *rights must itself define the scope of the limitation on the exercise of the right concerned*".[123]

63. Regarding the second condition, the *Puškár* and *Digital Rights Ireland* decisions constitute examples of instances in which the Court considered that the limitation respected the essence of the infringed rights and freedoms.[124, 125] However, the Court reached the opposite conclusion in *Schrems* (see our detailed analysis of this case in Section 3.5.2.[126]

64. With respect to the third condition, the CJEU has identified several objectives of general interest in its decisions. For instance, in *Schwarz*, the CJEU was asked about

111 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraph 62-72.
112 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraph 76.
113 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraph 89-93
114 These powers are set out in Article 28(3) of Directive 95/46.
115 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 64.
116 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 64.
117 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 66.
118 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 89.
119 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 95.
120 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559, paragraph 197.
121 Judgment of 17 October 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670, paragraph 40.
122 For example, in *Digital Rights Ireland*, the limitation was provided for by Directive 2006/24. In *Volker und Markus Schecke and Eifert*, EU Regulation 259/2008 allowed for an interference to fundamental rights. In *Puškár*, the limitation was set out in the national code of civil procedure.
123 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559, paragraph 175 and case law cited. See also Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraph 65.
124 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraph 64. Interestingly, the CJEU refers to the "essential content" as a synonym of "essence". Advocate General Kokott clarified the concept of 'essence' of fundamental rights when she held that *"(…) despite the adverse effects associated with [the limitation], those interferences do not meet the threshold of a breach of the essence of those rights, if the principle of proportionality is otherwise respected.*" (Opinion of 30 March 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:253, paragraph 116).
125 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 39.
126 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraphs 94-95.

the validity of Article 1(2) of Regulation 2252/2004, which requires Member States to take and store two digital fingerprints within passports.[127] The CJEU considered that this represents a twofold threat to the rights to respect for private life and the protection of personal data of the passport holders (Art. 7 and 8 of the Charter).[128] However, this interference fulfilled all the cumulative conditions of Article 52(1). Particularly, it did not go beyond what was necessary for the general interest objective of protecting against the use of fraudulent passports.

65. In *Puškár*, the CJEU identified two objectives of general interest: one is the interest of relieving the courts of disputes which can be decided directly before administrative authorities; the other is the interest of increasing the efficiency of judicial proceedings.[129] It also held that the "*objective of avoiding the unauthorised use of internal documents in judicial proceedings* [was] *capable of constituting*" an objective of general interest.[130] Lastly, in *Volker und Markus Schecke and Eifert*, the Court recognised the objective of increasing the transparency of the use of funds in the context of the common agricultural policy of the EU.[131]

66. Furthermore, the CJEU differentiated several objectives of general interest in the context of the retention and access to telecommunications data (for a more detailed analysis, see Section 4.5.2 below).

67. The second element of the 'need to protect the rights and freedoms of others' has been rarely applied in the context of data protection.[132] In *Puškár*, the Court relied on the first element of 'objectives of general interest', while acknowledging that there would be a 'need to protect the rights and freedoms of others' in specific circumstances. Concretely, if the list drawn up by tax authorities was confidential and contained personal data, there would be a need to protect the rights and freedoms of the individuals to whom the personal data relate within the meaning of Article 52(1) of the Charter.[133]

68. Lastly, with respect to the fourth condition, the proportionality test is similar to the one set out under Article 8(2) of the ECHR, which lists the conditions under which an interference to the right to private life can be lawful.[134] The CJEU frequently applied the principle of proportionality, providing factual guidance on what it considered strictly necessary.

69. For instance, the proportionality test under Article 52(1) of the Charter was also used by the CJEU in *Facebook Ireland and Schrems* to conclude that a third country did not provide a level of protection essentially equivalent to the one guaranteed by the EU legal order.[135]

70. Furthermore, the decisions referenced in Section 2.4.2(a), which relate to the obligation to retain communication data or allow access to such data for the purpose of fighting crime or ensuring public security included comprehensive proportionality tests in which the CJEU nuanced the outcome of the balancing exercise (see *inter alia* the *Digital Rights Ireland* decision).[136]

3. General data protection law

3.1 *General provisions*

3.1.1 *Material scope*

(a) *General principle*

71. Article 3(1) of Directive 95/46 set out the material scope of this Directive: it applied to the processing of personal data in two situations: (i) processing carried out wholly or partly by automatic means and (ii) processing otherwise than by automatic means if the personal data are part of a filing system or are intended to form part of it.[137] Article 2(1) of Regulation 2016/679 defines the mate-

127 Judgment of 17 October 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670.

128 Judgment of 17 October 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670, paragraph 30.

129 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraph 67.

130 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraph 92.

131 Judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, joined cases C-92/09 and C-93/09, ECLI:EU:C:2010:662, paragraphs 67-71.

132 In *Scarlet Extended*, Advocate General Cruz Villalón considered that the "need to protect the rights and freedoms of others", which is the second element of the third criterion, was applicable. The Advocate General favoured this condition instead of relying on one of the "objectives of general interest recognised by the EU": "*[a]lthough the protection of intellectual property rights definitely constitutes an objective of general interest,* (…), *the filtering and blocking system requested nevertheless finds its main justification, in the circumstances of the main proceedings, in the need to protect the 'rights and freedoms of others'* (…) *of copyright or related rights*" (Opinion of 14 April 2011, *Scarlet Extended*, C-70/10, ECLI:EU:C:2011:255, paragraphs 89 and 92).

133 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraph 92.

134 Article 8(2) of the ECHR states that "[t]*here shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*".

135 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/18, ECLI:EU:C:2020:559, paragraphs 168-184.

136 See Judgment of 8 April 2014, *Digital Rights Ireland and Others*, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238; Judgment of 21 December; Judgment of 2 October 2018, Ministerio Fiscal, C-207/16, ECLI:EU:C:2018:788 2016, *Tele2 Sverige*, C-203/15, ECLI:EU:C:2016:970; Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790; Judgment of 6 October 2020, *La Quadrature du Net*, Joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791.

137 See in this respect Opinion of 27 September 2018, *Buivids*, C-345/17, ECLI:EU:C:2018:780, paragraphs 32-34; where Advocate General Sharpston rejects the argument of the Latvian government that personal data must always form part of a filing system, even when it is processed by automatic means.

rial scope of Regulation 2016/679 in substantially the same terms.

72. Therefore, to determine whether an activity falls within the material scope of Directive 95/46 or Regulation 2016/679, it must first be established that 'personal data' are being 'processed'.[138] Subsequently, one must determine whether such processing is conducted 'wholly or partly by automatic means'.

73. In *Lindqvist,* the CJEU concluded that loading personal data on an internet page entails "*the operation of loading that page onto a server and the operations to make that page accessible to people who are connected to the internet. Such operations are performed, at least in part, automatically.*"[139]

74. In *Buivids,* the CJEU held that a video recording of persons which is stored on the memory of the digital video camera constitutes processing of personal data by automatic means.[140] In this context, the CJEU clarified that it was irrelevant that the recording was made on only one occasion considering that Directive 95/46 applies to 'any' such processing operation (Art. 2(b) *juncto* Art. 3(1) of Directive 95/46). In a similar case and referring to Recitals 15 and 16 of Directive 95/46, the CJEU decided that surveillance in the form of video recording of persons, which is recorded on a hard disk drive, constitutes processing of personal data by automatic means.[141]

75. In *Satakunnan Markkinapörssi and Satamedia*, the CJEU decided that the collection of data subjects' tax data from publicly available sources and their subsequent alphabetic publication in a newspaper as well as the provision of these data via mobile text-messaging services fall under the material scope of Article 3(1) of Directive 95/46.[142] Interestingly, the CJEU did not specify whether the processing of personal data was carried out wholly or partly by automatic means or whether the personal data was part of a filing system. According to Advocate General Kokott, it was "*probable*" that the different processing activities were "*carried out at least partly by automatic means*".[143] However, the Advocate General did not analyse this point in more detail because she opined that in any event, the publication of tax data in alphabetical order in a printed newspaper constitutes a filing system. Therefore, she concluded that the processing fell within the scope of Article 3(1) of Directive 95/46.
The CJEU also specified that a public authority initially disclosing personal data to the public does not have any bearing on the application of Directive 95/46 to the subsequent processing of these data for other purposes by a controller other than the public authority responsible for the initial disclosure. Indeed, *"a general derogation from the application of the directive in respect of published information would largely deprive the directive of its effect. It would be sufficient for the Member States to publish data in order for those data to cease to enjoy the protection afforded by the Directive."*[144]

76. In the recent *Facebook Ireland and Schrems* case, the CJEU recalled its settled case law that "*the operation of having personal data transferred from a Member State to a third country constitutes, in itself, processing of personal data (…) carried out in a Member State*" as a result of which it falls within the scope of Article 3(1) of Directive 95/46 and Article 2(1) of Regulation 2016/679.[145]

(b) *Exceptions*

77. Article 3(2) of Directive 95/46 contains two important exceptions to the general principle analysed in the previous section. First, Directive 95/46 does not apply to the processing of personal data "*in the course of activities which fall outside of EU law*" (Art. 3(2), first indent of Directive 95/46). Second, Directive 95/46 does not apply to the processing of personal data by a natural person in the course of a "*purely personal or household activity*" (Art. 3(2), second indent of Directive 95/46). Article 2(2) of Regulation 2016/679 has maintained these two exceptions in substantially the same manner.

78. In *Ryneš*,the CJEU held that "*since the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of the fundamental rights set out in the Charter (…), the exception provided for in the second indent of Article 3(2) of that directive must be narrowly construed*".[146] Similarly, the CJEU stated in *Puškár* that these exceptions must be interpreted restrictively "*in so far as it renders inapplicable the system of protection of personal data provided for in Directive 95/46 and thus deviates from the objective*

138 For an analysis of these concepts, see sections 3.1.3(a) and 3.1.3(b) below.
139 Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraphs 26-27 and confirmed in Judgment of 14 February 2019, *Buivids*, C-345-17, ECLI:EU:C:2019:122, paragraphs 37-39 and Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 26; Judgment of 1 October 2015, *Weltimmo,* C-230/14, ECLI:EU:C:2015:639, paragraph 37.
140 Judgment of 14 February 2019, *Buivids*, C-345-17, ECLI:EU:C:2019:122, paragraph 35.
141 Judgment of 11 December 2014, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428, paragraphs 24-25. See also judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraphs 34-35.
142 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia,* C-73/07, ECLI:EU:C:2008:727, paragraphs 35-37.
143 Opinion of 8 May 2008, *Satakunnan Markkin apörssi and Satamedia,* C-73/07, ECLI:EU:C:2008:266, paragraph 34.
144 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia,* C-73/07, ECLI:EU:C:2008:727, paragraphs 48-49.
145 Judgment of 16 July 2020, *Facebook Ireland and Schrems,* C-311/18, ECLI:EU:C:2020:559, paragraph 83; Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 45; Judgment in Parliament v Council and Commission, C-317/04 and C-318/04, ECLI:EU:C:2006:346, paragraph 56.
146 Judgment of 11 December 2014, *Ryneš,* C-212/13, ECLI:EU:C:2014:2428, paragraph 29.

underlying it, namely, to ensure the protection of the fundamental rights and freedoms of natural persons with regard to the processing of personal data".[147]

(c) *Exception 1 – activities outside of the scope of EU law*

79. The first instance in which the CJEU had to interpret the scope of the exception laid down in Article 3(2), first indent of Directive 95/46 was the *Lindqvist* case.[148] Mrs. Lindqvist argued that she had uploaded personal data on an internet page solely for charitable and religious purposes. She defended the view that Directive 95/46 can only apply to processing activities carried out in the context of a professional or commercial activity.

80. Advocate General Tizzano agreed with this interpretation: *"The processing of the personal data in question was (…) carried out in the course of a non-economic activity which had no connection (…) with the exercise of the fundamental freedoms protected by the Treaty and is not governed by any specific rules at Community level."*[149] In his view, concluding that Directive 95/46 applied to processing of personal data carried out in the context of a non-economic activity would require the annulment of Directive 95/46 since it was adopted on a legal ground that solely entailed encouraging the establishment and functioning of the internal market (initial Article 100a of the Treaty establishing the European Community - "EC Treaty", now Article 114 of the TFEU). This led him to conclude that the processing activity in the case at hand fell outside of the scope of Directive 95/46.

81. The CJEU did not follow the Advocate General's Opinion. The fact that the legal basis of Directive 95/46 was Article 100a of the EC Treaty did not imply, according to the CJEU, that every processing activity under Directive 95/46 necessarily required the existence of an actual link with free movement between Member States.[150]

82. Having determined that the material scope of Directive 95/46 also covered the processing of personal data in the context of non-economic activities, the CJEU then clarified the actual scope of the exception laid down in Article 3(2), first indent of Directive 95/46.
In this context, the CJEU paid particular attention to the examples of activities which, according to Article 3(2), first indent of Directive 95/46, fall outside of the scope of EU law: activities "*provided for by and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.*" Considering these examples, the CJEU noted that *"the activities mentioned (…) are in any event, activities of the State or of State authorities and unrelated to the fields of activity of individuals."* Consequently, the CJEU concluded that these examples *"are intended to define the scope of the exception (…), with the result that that exception applies only to the activities which are expressly listed there or which can be classified in the same category (ejusdem generis)."*[151] The CJEU therefore decided that the charitable and religious activities of Mrs. Lindqvist were not covered by the exception of Article 3(2), first indent of Directive 95/46.

83. The CJEU has had the opportunity to clarify the meaning of 'activities outside of the scope of EU law' in several cases. In *Huber*, the CJEU decided that the processing of personal data in a central register of foreign nationals for the purposes of the application of legislation relating to the right of residence and for statistical purposes does not fall within the scope of the exception of Article 3(2), first indent of Directive 95/46. Contrarily, the processing of such data in a central register of foreign nationals for the purpose of fighting crime falls within the scope of this exception.[152]

84. The collection of tax and income data following an initial publication by public authorities and their onward transfer on a CD-ROM to be used for commercial purposes through mobile text-messaging services is not caught by the exception of Article 3(2), first indent of Directive 95/46; this is to the extent that it concerns activities of private companies and not of public authorities.[153]

85. In *Breyer*, the CJEU ruled that public authorities, when processing IP addresses for the purpose of maintaining the security and operation of their websites and of allowing criminal proceedings against the perpetrators of cyberattacks "*act, in spite of their status as public authori-*

147 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraph 38. See also Judgment of 10 July 2018, *Jehovan Todistajat*, C-25/17, ECLI:EU:C:2018:551, paragraph 37.

148 Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraphs 38-45.

149 Opinion of 19 September 2002, *Lindqvist*, C-101/01, ECLI:EU:C:2002:513, paragraphs 35-44. See also Advocate General Tizzano's opinion in *Österreichischer Rundfunk and Others*, in which he adopted the same reasoning. Although the *Lindqvist* decision was issued after the *Österreichischer Rundfunk and Others* decision, the Advocate General's Opinion in the latter predates his Opinion in the former.

150 Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraphs 38-42. See also *Österreichischer Rundfunk and Others*, in which the CJEU analysed this subject extensively by way of preliminary observations, before addressing the actual questions referred - Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, paragraphs 39-47. See also Judgment of 9 July 2020, *Land Hessen*, C-272/19, ECLI:EU:C:2020:535, paragraph 66.

151 Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraphs 43-44. See also Judgment of 9 July 2020, *Land Hessen*, C-272/19, ECLI:EU:C:2020:535, paragraph 66.

152 Judgment of 16 December 2008, *Huber,* C-524/06, ECLI:EU:C:2008:724, paragraphs 44-45. For the sake of completeness, we add that the CJEU ruled that the use of this register for the purpose of fighting crime was viewed to be violating the principle of non-discrimination on grounds of nationality, as set out in Article 12 of EC Treaty.

153 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia,* C-73/07, ECLI:EU:C:2008:727, paragraphs 40-42.

ties, as individuals and outside the activities of the State in the area of criminal law".[154] In his opinion, Advocate General Campos Sánchez-Bordona added that the reference to 'allowing criminal proceedings' in the case at hand should be understood as relating to a *"person's entitlement to initiate the State's exercise of ius puniendi, through appropriate proceedings"* and not to the exercise of the State's *ius puniendi* as such.[155] Therefore, the processing of IP addresses by a public authority in the case at hand did not constitute an activity of the State in the area of criminal law.

86. In the recent case *Land Hessen,* the CJEU ruled that "[w]*hile the activities of the Petitions Committee of the Parliament of Land Hessen are incontestably public and are activities of that Land, that committee contributing indirectly to the parliamentary activity, the fact remains that not only are those activities political as much as administrative, but it is also not clear from the documents available to the Court that those activities correspond, in this instance, to the activities mentioned in Article 2(2)(b) and (d) of Regulation 2016/679 or that they can be classified in the same category as those activities.*"[156]

87. Moreover, the recording and publishing of a video recording of police officers on *YouTube* by an individual does not fall within the scope of the exception of Article 3(2), first indent of Directive 95/46 as it does not constitute an activity of the State or of State authorities.[157]

88. Finally, in *Jehovan Todistajat*, the CJEU ruled that personal data processing in the context of door-to-door preaching carried out by individuals is not an activity of the State authorities and therefore does not benefit from the exception of Article 3(2), first indent of Directive 95/46.[158]

(d) *Exception 2 - Household exemption*

89. Regarding the household exemption, Recital 12 of Directive 95/46 cites two examples of processing activities which are to be considered exclusively personal or domestic: "*correspondence and the holding of records of addresses*". Referring to these examples, in *Lindqvist*, the CJEU held that the household exemption must therefore be interpreted as *"relating only to activities which are carried out in the course of private or family life of individuals"*.[159] In *Ryneš,* the CJEU recalled the need for a strict interpretation, as Article 3(2), second indent of Directive 95/46 refers to processing carried out 'purely' in the context of a personal or household activity and not those which are 'simply' carried out in that context.[160]

90. On several occasions, the CJEU also stated that the words 'personal or household' *"refer to the activity of the person processing the personal data and not to the person whose data are processed"*.[161]

91. Based on the aforementioned considerations, the CJEU has held that the following activities do not fall within the scope of the household exemption: the publication of personal data on the internet such that they are made accessible to an indefinite number of individuals[162]; making accessible tax and income data to an unrestricted number of individuals via mobile text-messaging services[163]; the installation of a camera system by an individual in their family home for the purpose of protecting the property, health and life of the home owners such that the camera also partially monitors a public space[164]; the collection of personal data by members of the Jehovah's Witnesses Community in the course of door-to-door preaching[165] or the publishing of a video on *YouTube*[166].

3.1.2 *Territorial scope*

92. Article 4 of Directive 95/46 set out the rules regarding its territorial scope. Considering the nature of the legal instrument which required Member States to transpose it into national law, this Article was vital to determine which Member States' national data protection law applied to situations of cross-border data processing. Additionally, Article 4 of Directive 95/46 also covered the extra-territorial scope of Directive 95/46.

93. In a world where cross-border data processing has become omnipresent, it is not surprising that the CJEU

154 Judgment of 19 October 2016, *Breyer,* C-582/14, ECLI:EU:C:2016:779, paragraphs 50-53.
155 Opinion of 12 May 2016, *Breyer,* C-582/14, ECLI:EU:C:2016:339, paragraphs 85-92. A similar reasoning can be found in the CJEU's *Puškár* decision, Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraphs 39-40.
156 Judgment of 9 July 2020, *Land Hessen*, C-272/19, ECLI:EU:C:2020:535, paragraph 71.
157 Judgment of 14 February 2019, *Buivids*, C-345-17, ECLI:EU:C:2019:122, paragraph 40-42.
158 Judgment of 10 July 2018, *Jehovan Todistajat*, C-25/17, ECLI:EU:C:2018:551, paragraph 39.
159 Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraphs 46-47.
160 Judgment of 11 December 2014, *Ryneš,* C-212/13, ECLI:EU:C:2014:2428, paragraphs 30-32. See also judgment of 10 July 2018, *Jehovan Todistajat*, C-25/17, ECLI:EU:C:2018:551, paragraph 40.
161 Judgment of 10 July 2018, *Jehovan Todistajat*, C-25/17, ECLI:EU:C:2018:551, paragraph 41 and judgment of 11 December 2014, *Ryneš,* C-212/13, ECLI:EU:C:2014:2428, paragraph 30.
162 Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraph 47.
163 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia,* C-73/07, ECLI:EU:C:2008:727, paragraphs 43-45.
164 Judgment of 11 December 2014, *Ryneš,* C-212/13, ECLI:EU:C:2014:2428, paragraph 33.
165 Judgment of 10 July 2018, *Jehovan Todistajat*, C-25/17, ECLI:EU:C:2018:551, paragraphs 40-49. The CJEU notably based its conclusion on the fact that the preaching activity, by its very nature, intends to spread the faith to people who do not belong to the Jehovah's Witnesses faith. According to the CJEU, this implies that the activity is *"directed outwards from the private setting of the members who engage in preaching"*. Furthermore, the CJEU referred to the fact that the individual members share data collected during their preaching activities with the community, thus making it accessible *"to a potentially unlimited number of persons"*.
166 Judgment of 14 February 2019, *Buivids*, C-345-17, ECLI:EU:C:2019:122, paragraph 43.

has been asked to clarify the territorial scope in several cases.[167]

94. These cases related to Article 4(1)(a) of Directive 95/46, which stated that a Member State's law applies to the processing of personal data carried out in the context of an establishment of the controller on the territory of that Member State. This criterion is commonly referred to as the 'establishment test'.

95. *Google Spain and Google* is best known for the recognition of the right to be forgotten.[168] However, this landmark decision was equally important because of the manner in which the CJEU interpreted the establishment test in a context of extra-territorial application of Directive 95/46.

96. Google Inc., a company established in the United States, operates the search engine Google Search. Before considering the existence of a possible right for data subjects to be forgotten, the CJEU first had to establish that Directive 95/46 applied to Google Inc. as controller of the processing carried out in the context of its search engine – *i.e.* that Google Inc. met the criteria of the establishment test.

97. Having established that Google Spain constituted an establishment of Google Inc. in Spain[169], the Grand Chamber had to examine whether Google Inc.'s processing activities related to its search engine were carried out 'in the context of the activities of' Google Spain.

98. In response to Google's defence that Google Spain did not intervene in the operation of the search engine at all, the CJEU noted that Article 4(1)(a) of Directive 95/46 did not require the processing to be carried out 'by' Google Spain itself, "*but only that it be carried out 'in the context of the activities' of* [Google Spain]".[170] These words cannot be interpreted restrictively as the CJEU recalled.[171]

99. The Grand Chamber then confirmed that the objective of Article 4(1)(a) of Directive 95/46 was to *"prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope*".[172]

100. On that basis, it concluded that "*the processing of personal data for the purposes of (…) a search engine (…)*", which is operated by an undertaking that has its seat outside of the EU but has an establishment in a Member State, *"is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable*".[173] This resulted from the fact that the activities of Google and Google Spain were *"inextricably linked*".[174]

101. In *Wirtschaftsakademie Schleswig-Holstein*, the CJEU adopted the same reasoning to conclude that the activities of Facebook Germany, which were intended to *"ensure the promotion and sale in Germany of advertising space that makes Facebook's services profitable"* are inextricably linked with the processing of personal data in the context of Facebook Inc.'s operation of its social network.[175]

102. In *Weltimmo* and in *Verein für Konsumenteninformation*[176], the CJEU further extended the application of the establishment test under Article 4(1)(a) of Directive 95/46 by broadening the interpretation of the notion of 'establishment', as explained in Section 3.1.3(e) below, which deals with the definition of '(main) establishment'.[177]

103. With its broad interpretation of the establishment test, the CJEU has stretched territorial application to the maximum extent possible. This seems linked to the fact that Directive 95/46, as Advocate General Jääskinen indicated, was adopted *"before the large-scale provision of on-line services on the internet started*".[178] Article 4(1) of Directive 95/46 was indeed not fit to deal with the increasing number of controllers based outside of the EU who were processing huge amounts of data of EU-based data subjects. At the time of these CJEU decisions, the European Commission had already issued its proposal for

167 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317; Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388; Judgment of 28 July 2016, *Verein für Konsumenteninformation,* C-191/15, ECLI:EU:C:2016:612; Judgment of 24 September 2019, *Google*, C-507/17, ECLI:EU:C:2019:772.

168 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317. On the right to be forgotten, see section 3.3.5 below.

169 See our analysis of the concept of 'establishment' in section 3.1.3(e) below.

170 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 52. Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, paragraph 35; Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, paragraph 57.

171 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 53. Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, paragraph 25; Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, paragraph 56.

172 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 54. Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, paragraphs 26-27.

173 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 55.

174 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 56.

175 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, paragraphs 58-61.

176 Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639 and Judgment of 28 July 2016, *Verein für Konsumenteninformation,* C-191/15, ECLI:EU:C:2016:612.

177 See our analysis of the concept of 'establishment' in section 3.1.3(e) below.

178 Opinion of 25 June 2013, *Google Spain and Google,* C-131/12, ECLI:EU:C:2013:424, paragraphs 60-61.

Regulation 2016/679 which added two new criteria, the 'offering of goods or services' and the 'monitoring of behaviour' tests, to deal with the extra-territorial situation.[179] The CJEU therefore seemed determined to prevent EU-based data subjects from losing the protection of their fundamental right to data protection in instances in which the controller was based outside of the EU.

104. After the adoption of Regulation 2016/679, one might therefore have expected that the CJEU would start relying on the two new tests of Article 3(2)(a) and (b) of Regulation 2016/679 when addressing these situations.[180] However, in *Google,* it confirmed its previous case law relating to the establishment test in the context of Article 3 of Regulation 2016/679.[181]

3.1.3 *Definitions*

105. Both Directive 95/46 and Regulation 2016/679 set out a list of definitions whose meaning and scope have been clarified by the CJEU over the years. These definitions relate to fundamental concepts that have shaped the scope of EU data protection law, such as 'personal data', 'controller' and 'processor'. As explained below, relying on the purpose of Directive 95/46 and then of Regulation 2016/679 as well as on the protection of individuals' fundamental rights, the CJEU has often interpreted such definitions broadly, providing an extensive scope to EU data protection law and thereby ensuring the full protection of personal data.

106. It is noteworthy that some definitions set out in Directive 95/46 and Regulation 2016/679 also appeared under Regulation 45/2001[182], which applied to data processing carried out by EU institutions and agencies. For instance, this is the case of the concepts of 'personal data', 'processing', 'controller' and 'processor' which are defined in almost the same terms. The CJEU has developed another body of case law to apply Regulation 45/2001 and its definitions. The corresponding decisions can therefore shed some light on the case law of the CJEU under Directive 95/46 and Regulation 2016/679 and are thus included in the following sections.

(a) *Personal data*

(i) General

107. The notion of 'personal data' under Article 2(a) of Directive 95/46 is defined as "*any information relating to an identified or identifiable natural person*". This notion does not cover legal persons.[183]

108. This definition allows the following test to determine whether a natural person is identifiable: "*an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*". Recital 26 of Directive 95/46 described the identification test to use, whereby "*to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person*".

109. It is noteworthy that Article 4(1) of Regulation 2016/679 keeps the same first part of the definition of personal data as in the repealed Directive 95/46. Considering the second part of the definition relating to the identification test, it replaces the terms "*identification number*" by "*identifier, such as a name, an identification number, location data, an online identifier*" and adds a reference to the "*genetic*" identity.[184] Recital 26 of Regulation 2016/679 also describes in more detail the 'reasonable means' method to use by referring to objective factors such as time, cost and available technology.[185, 186]

110. As we will see below, the CJEU has had the opportunity to interpret the notion of 'personal data' multiple times. Some referring courts have explicitly asked the

179 Article 3(2)(a) and (b) of Regulation 2016/679.

180 See EDPB, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), 12 November 2019.

181 Judgment of 24 September 2019, *Google*, C-507/17, ECLI:EU:C:2019:772, paragraphs 48-52.

182 Regulation (EC) 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2001] OJ L 8. It is worth noting that Regulation 45/2001 was subsequently repealed by Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC [2018] OJ L 295.

183 Judgment of 30 May 2006, *Bank Austria Creditanstalt AG v. Commission of the European Communities*, T-198/03, ECLI:EU:T:2006:136, paragraph 95: "*Regulation No 45/2001 seeks to protect individuals with regard to the processing of personal data. The applicant, which is a legal person, does not belong to the circle of persons which the regulation is intended to protect.*"

184 Article 4(1) of Regulation 2016/679 provides that "'*personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*".

185 Recital 26 of Regulation 2016/679 states that "(…) *To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments* (…)".

186 See also Opinion 4/2007 on the concept of personal data of WP29, which has provided additional guidance on the four elements set out in the definition of 'personal data' under Directive 95/46, namely: (1) "any information", (2) "relating to", (3) "identified or identifiable" and (4) "natural person". This opinion is still relevant, albeit not officially endorsed by the EDPB upon its establishment.

CJEU to interpret it in relation to specific piece(s) of information.[187] However, the CJEU often interpreted the notion on its own initiative as a preliminary consideration to determine whether Directive 95/46 is applicable without any such question being referred to it.[188]

111. Often as an introductory remark in its rulings in this context, the CJEU has asserted the "*very wide*" scope of Directive 95/46 and the varied nature of the personal data covered by it.[189] Furthermore, it has not restricted the content of personal data. In fact, in the landmark case *Nowak*, the CJEU viewed the use of the terms "*any information*" in the definition of personal data as reflecting "*the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it 'relates' to the data subject*".[190] Concretely, for information to "*relate*" to an individual, the CJEU considered that this criterion is fulfilled "*where the information, by reason of its content, purpose or effect, is linked to a particular person*".[191]

112. The decisions delivered by the CJEU represent many examples of sets of information qualifying as 'personal data'. In the CJEU's own words, "[p]*ersonal data would therefore include, for example, surname and forenames, postal address, e-mail address, bank account number, credit card numbers, social security number, telephone number or driving licence number.*"[192]

113. The CJEU clarified that the "*concepts of 'personal data' and of 'data relating to private life' are not to be confused. Consequently, the claim made* (…) *that the information at issue does not fall within the scope of the private life of the experts concerned* [and hence does not constitute personal data] *is ineffective*"[193]. In other terms, information does not necessarily have to fall into the private sphere of an individual to qualify as 'personal data'.[194] The latter distinction triggers significant consequences with respect to the scope of 'personal data'.

114. For example, it is settled case law that the data provided "*as part of a professional activity*" can constitute personal data.[195] The CJEU has concretely held that the records of working time with the daily work and rest periods for each worker need to be categorized as personal data.[196] The list of participants in a meeting who were representatives of a business organisation was also found to constitute 'personal data'[197]. Similarly, information that makes it possible to identify the author of each comment made by a pool of experts on a document represents 'personal data'.[198] The same conclusion was reached for the name and professional income of employees and pension-

187 Judgment of 19 October 2016, *Breyer*, C-582/14, ECLI:EU:C:2016:779, paragraph 30; Judgment of 17 July 2014, *YS and Others*, C-141/12, ECLI:EU:C:2014:208, paragraph 22; Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, paragraph 26.

188 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, paragraph 64; Judgment of 6 November 2003, *Lindqvist*, C-101/01, paragraph 24; Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, paragraph 34; Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraph 34; Judgment of 16 December 2008, *Heinz Huber v Bundesrepublik Deutschland*, C-524/06, ECLI:EU:C:2008:724, paragraph 40; Judgment of 11 December 2014, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428, paragraph 18; Judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:336, paragraph 24; Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122, paragraphs 30-32.

189 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 59; and affirmed in Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, paragraph 33.

190 Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, paragraph 34.

191 Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, paragraph 35. See also Opinion 4/2007 on the concept of personal data of WP29, 20 June 2007, 01248/07/EN, WP 136.

192 Judgment of 8 November 2007, *Bavarian Lager v Commission*, Case T-194/04, ECLI:EU:T:2007:334, paragraph 104, which was upheld on appeal by Judgment of 29 June 2020, *Commission v. Bavarian Lager Co.*, C-28/08, ECLI:EU:C:2010:378, paragraphs 68-70. The latter *Bavarian Lager* decision was also referenced in the Judgment of 7 July 2011, *Gregorio Valero Jordana*, T-161/04, ECLI:EU:T:2011:337, paragraph 91, where the Court held that the names and family names relating to individuals who passed European competitive exams and to individuals nominated to certain positions constitute 'personal data' within the meaning of Regulation 45/2001, which sets out the same definition of 'personal data' as in Directive 46/95.

193 Judgment of 16 July 2015, *ClientEarth and PAN Europe v EFSA*, C-615/13, ECLI:EU:C:2015:489, paragraph 31.

194 Judgment of 11 June 2015, *Colin Boyd McCullough*, T-496/13, ECLI:EU:T:2015:374, paragraph 66.

195 This principle was asserted in Judgment of 16 July 2015, *ClientEarth and PAN Europe v EFSA*, C-615/13, ECLI:EU:C:2015:489, paragraph 30, which confirms Judgment of 13 September 2013, *ClientEarth and PAN Europe v EFSA*, T-214/11, ECLI:EU:T:2013:483, paragraphs 44-46. In this decision, the CJEU applied the definition of personal data set out in Article 2(a) of Regulation 45/2001. It must be noted that said definition was identical to the definition set out in Directive 95/46. It is worth noting that Recital 7 of Regulation 45/2001 explicitly stated that "*The persons to be protected are those whose personal data are processed by Community institutions or bodies in any context whatsoever, for example because they are employed by those institutions or bodies*". This finding was however then confirmed in Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, paragraph 34, which relates to Directive 95/46.

196 Judgment of 30 May 2013, *Worten*, C-342/12, ECLI:EU:C:2013:355, paragraphs 19 and 22.

197 Judgment of 8 November 2007, *Bavarian Lager v Commission*, Case T-194/04, ECLI:EU:T:2007:334, paragraph 104, which was upheld on appeal by Judgment of 29 June 2020, *Commission v. Bavarian Lager Co.*, C-28/08, ECLI:EU:C:2010:378, paragraphs 68-70.

198 Judgment of 13 September 2013, *ClientEarth and PAN Europe v EFSA*, T-214/11, ECLI:EU:T:2013:483, paragraphs 41-46. This finding was confirmed in Judgment of 16 July 2015, *ClientEarth and PAN Europe v EFSA*, C-615/13, ECLI:EU:C:2015:489, paragraph 29.

ers who are recipients of public funds[199] and for the names as well as the amount of earned and unearned incomes of individuals whose income exceeds certain thresholds.[200] Similarly, tax data constitutes personal data.[201] In *IPI*, the CJEU found that the data collected by private detectives relating to estate agents constitutes personal data as they concern identified or identifiable natural persons.[202] Finally, the surnames of the members of EU agencies participating in agency meetings constitute personal data even if the meetings of these agencies are linked to the exercise of public duties.[203]

115. The CJEU has generally rejected many arguments of those – be it applicants or defendants – who have attempted to limit the scope of the concept of 'personal data'. Hence, the fact that some data were made public – either on the internet or in the *Official Journal of the European Union* – does not necessarily mean that such data can no longer amount to personal data.[204] Moreover, the characterization of information as 'personal data' can be carried out regardless of whether the data subject to which it relates has first objected to the disclosure of said data.[205]

116. However, the CJEU clarified that the concept of 'personal data' does not extend to legal analyses as such.[206] While the CJEU recognised that the data relating to an individual set out in a legal analysis constitute personal data, the legal analysis in itself cannot amount to personal data.

117. Finally, the qualification of certain information as 'personal data' triggers the application of a number of principles established in the repealed Directive 95/46 and in Regulation 2016/679. However, the CJEU recalled that the determination of the qualification of 'personal data' cannot be affected by the fact that certain principles will apply following such a legal qualification.[207]

199 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, paragraph 64.

200 Judgment of 16 December 2008 *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraph 35.

201 Judgment of 1 October 2015, *Bara and Others*, C 201/14, ECLI:EU:C:2015:638, paragraph 29; Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraph 41.

202 Judgment of 7 November 2013, *IPI*, C-473/12, ECLI:EU:C:2013:715, paragraph 26.

203 Judgment of 11 June 2015, *Colin Boyd McCullough*, T-496/13, ECLI:EU:T:2015:374, paragraph 66.

204 This finding was confirmed in Judgment of 16 July 2015, *ClientEarth and PAN Europe v EFSA*, C-615/13, ECLI:EU:C:2015:489, paragraph 31; Judgment of 11 June 2015, *Colin Boyd McCullough*, T-496/13, ECLI:EU:T:2015:374, paragraph 66.

205 Judgment of 13 September 2013, *ClientEarth and PAN Europe v EFSA*, T-214/11, ECLI:EU:T:2013:483, paragraphs 57-59. This finding was confirmed in Judgment of 16 July 2015, *ClientEarth and PAN Europe v EFSA*, C-615/13, ECLI:EU:C:2015:489, paragraph 33.

206 Judgment of 17 July 2014, *YS and others*, C-141/12, ECLI:EU:C:2014:208, paragraphs 39-41.

207 Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, paragraphs 46-47 (with respect to the application of the rights of access and rectification).

(ii) Information relating to an identified natural person

118. In most cases, the CJEU has readily concluded that the information related to the preliminary questions of the referring court constitutes personal data as it is information "*concerning an identified or identifiable natural person*".[208] For instance, as soon as 2003, the CJEU considered in the *Lindqvist* decision that the concept of personal data "*undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies*".[209] In *Rīgas satiksme*, the CJEU stated that "*it is common ground that that the identity document number and the address of the taxi passenger, (…) constitute information concerning an identified or identifiable natural person and, therefore, 'personal data'*".[210]

119. Another example of direct identification is the *Huber* decision in which the CJEU ruled that the data contained in a central register of foreign nationals constituted personal data. This included the name, given name, date and place of birth, nationality, marital status, sex, a record of entries and exits, residence status, particulars of passports, a record of previous statements as to domicile and particulars of the authorities who supplied the data and the reference numbers used by those authorities.[211] The same finding was reached for the surname and given name of the natural persons whose income exceeded certain thresholds as well as the amount of their income.[212] The CJEU concluded that the same was also the case for the identity document number and the address of a taxi passenger[213] and the names and addresses of certain internet users.[214] Finally, in *Schwarz*, the CJEU ruled that "*fingerprints constitute personal data, as they objectively con-*

208 See judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, paragraph 64; judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, paragraph 45; Judgment of 16 December 2008 *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraph 35; Judgment of 30 May 2013, *Worten*, C-342/12, ECLI:EU:C:2013:355, paragraph 19; Judgment of 16 December 2008, *Heinz Huber v Bundesrepublik Deutschland*, C-524/06, ECLI:EU:C:2008:724, paragraphs 31 and 43; Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 42 (where the CJEU states that the name and address of a person constitute "*basic data*"); Judgment of 17 July 2014, *YS and Others*, C-141/12, ECLI:EU:C:2014:208, paragraph 38 ("*there is no doubt that the data relating to the applicant for a residence permit and contained in a minute, such as the applicant's name, date of birth, nationality, gender, ethnicity, religion and language, are information relating to that natural person, who is identified in that minute in particular by his name, and must consequently be considered to be 'personal data'*"); Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 27; Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725. paragraph 33.

209 Judgment of 6 November 2003, *Lindqvist*, C-101/01, paragraph 24.

210 Judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:336, paragraph 24.

211 Judgment of 16 December 2008, *Heinz Huber v Bundesrepublik Deutschland*, C-524/06, ECLI:EU:C:2008:724, paragraph 43.

212 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraph 35.

213 Judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:336, paragraph 24.

214 Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, paragraph 45.

tain unique information about individuals which allows those individuals to be identified with precision".[215]

(iii) Information relating to an identifiable natural person

120. The definition of personal data also covers information that allows for the indirect identification of data subjects. In practice, this implies that individuals can be identified by combining at least two pieces of information. According to the CJEU, the use of the term "*indirectly*" in Article 2(a) of Directive 95/46 demonstrates that "*in order to treat information as personal data, it is not necessary that that information alone allows the data subject to be identified*".[216]

121. Relying on the terms "*means likely reasonably to be used*" and the reference to "*any other person*", the CJEU ruled that the definition of personal data does not require that "*all the information enabling the identification of the data subject must be in the hands of one person*".[217] The CJEU further explained that the fulfilment of the criterion "*reasonably likely means to be used*" would not be met "*if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant*".[218] As mentioned above, the cost and time factors have now been incorporated in Recital 26 of Regulation 2016/679.

122. In some instances, the CJEU conducted a factual analysis to determine whether certain pieces of information amount to 'personal data'. For instance, when applying Regulation 45/2001, the CJEU held that the information included in a press release constituted personal data. In the same document, the European Anti-Fraud Office recommended that competent public authorities prosecute an individual. Although the press release did not explicitly name the individual to prosecute, the CJEU relied on the factual circumstances of the case to conclude that the plaintiff was 'identifiable' within the meaning of the above definition. In fact, reading the press release in conjunction with other press articles covering the same topic made it possible to identify the individual since the press articles gave the name of the plaintiff. As highlighted by the CJEU, "*it should be noted that the fact that the press release did not explicitly name the applicant was not sufficient to protect her identity (…). A reader of the press release who had read those articles would have had no difficulty in understanding that the investigation to which the press release related concerned the applicant. It must therefore be considered that the press release contained factual elements that made it possible to identify the applicant, even if it did not name her.*"[219]

123. IP addresses also provide a good example of indirect identification. In *Scarlet Extended*, the CJEU first held that IP addresses of users' computers amount to personal data as they allow users "*to be precisely identified*".[220] It is noteworthy that in this decision, the CJEU did not specify whether the concerned IP address was dynamic or static. While the CJEU did not justify this finding at the time, it subsequently clarified it in *Breyer* that its previous analysis considered that the internet service provider collected and processed users' IP addresses.[221] In *Breyer*, the CJEU analysed the nature of dynamic IP addresses.[222] These are assigned to devices for each internet connection and are replaced when subsequent connections are made.[223] In *Breyer*, the media services provider could not identify users from the IP addresses directly without additional information. Therefore, the CJEU concluded that it was possible for the media services provider to combine the IP address with the additional information held by the internet service provider as a "*means likely reasonably to be used*" for identification.[224] However, this would not be the case if the identification of individuals was prohibited by law. In this case, the media service provider had "*legal channels*" at its disposal to have the competent authority request additional information from the internet service provider.[225] Consequently, the CJEU found that dynamic IP addresses also constitute personal data. Regulation 2016/679 incorporates these findings as the definition of personal data now explicitly refers to online identifiers (Art. 4(1)). Furthermore, Recital 30 provides examples of online identifiers in the context of devices and applications, such as IP addresses and cookie identifiers.

124. In line with the *Breyer* decision, the CJEU found in *Nowak* that the written answers submitted by a candidate at a professional examination and any examiner's comments with respect to them would constitute personal

215 Judgment of 17 October 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670, paragraph 27.

216 Judgment of 19 October 2016, *Breyer*, C-582/14, ECLI:EU:C:2016:779, paragraph 41. See also Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 171.

217 Judgment of 19 October 2016, *Breyer,* C-582/14, ECLI:EU:C:2016:779, paragraph 43; and confirmed in Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, paragraph 31.

218 Judgment of 19 October 2016, *Breyer*, C-582/14, ECLI:EU:C:2016:779, paragraph 46.

219 Judgment of 21 September 2007, *Kalliopi Nikolaou*, T-259/03, ECLI:EU:T:2007:254, paragraphs 181, 202-203 and 222 (translation from French to English; this is not an official translation).

220 Judgment of 24 November 2011, *Scarlet Extended SA*, C-70/10, ECLI:EU:C:2011:771, paragraph 51.

221 Judgment of 19 October 2016, *Breyer*, C-582/14, ECLI:EU:C:2016:779, paragraph 34.

222 Judgment of 19 October 2016, *Breyer*, C-582/14, ECLI:EU:C:2016:779, paragraph 36.

223 Static IP addresses, on the other hand, are IP addresses that do not change.

224 Judgment of 19 October 2016, *Breyer*, C-582/14, ECLI:EU:C:2016:779, paragraphs 42-49.

225 Judgment of 19 October 2016, *Breyer*, C-582/14, ECLI:EU:C:2016:779, paragraphs 46-47.

data even if the concerned examiner could not identify the candidate when reviewing the examination. The reason is that candidates are ultimately "*easily and infallibly*" identifiable by the examination body through their examination number.[226]

125. In the context of video surveillance, the CJEU found that the image of a person recorded by a camera constitutes personal data "*inasmuch as it makes it possible to identify the person concerned*".[227] When citing the definition of 'personal data', the CJEU refers to the 'physical' identity of an individual which enables their indirect identification[228]. In *Ryneš*, the CJEU did not concretely apply this test to the video recording at issue. However, the facts of the decision highlighted that the video recording made it possible to identify two suspects in the course of the criminal proceedings.[229] In *Buivids*, the CJEU considered that it was possible to hear and see the police officers displayed in the video recording, which therefore constituted personal data.[230]

(iv) Special categories of data, personal data concerning health, and data relating to offences and criminal convictions

126. Article 8(1) of Directive 95/46 and Article 9(1) of Regulation 2016/679 contain a subcategory of personal data, namely the special categories of data which include personal data concerning health. In *Lindqvist*, the CJEU relied on the purpose of the Directive to argue that this subcategory of personal data needs to be interpreted broadly. Essentially, personal data concerning health must include "*information concerning all aspects, both physical and mental, of the health of an individual*". Therefore, for instance, according to the CJEU, the information according to which an individual has injured his or her foot and is on half time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46.

127. Regulation 2016/679 incorporated this decision and further completed it through a new definition of data concerning health. According to Article 4(15), it refers to "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*". Recital 35 further extends the scope of this definition by clarifying that it encompasses "*information relating to the past, current or future physical or mental health status of the data subject*". Numerous non-exhaustive examples are also provided, such as information derived from the testing or examination of a body part or bodily substance and any information on a disease or disease risk.

128. In *GC and Others*, the CJEU clarified that information relating to a judicial investigation and a trial constitutes data relating to offences and criminal convictions within the meaning of Article 8(5) of Directive 95/46 and Article 10 of Regulation 2016/679 "*regardless of whether or not, in the course of those legal proceedings, the offence for which the individual was prosecuted was shown to have been committed*".[231]

(b) *Processing*

129. Article 2(b) of Directive 95/46 defines the processing of personal data as "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*". It is noteworthy that Regulation 2016/679 has substantially kept the same definition of controller as in the repealed Directive 95/46 (Art. 4(2)).[232]

130. The notion of processing is relevant to determine the material scope of Directive 95/46 and Regulation 2016/679 (see Section 3.1.1 above).

131. Soon after the adoption of Directive 95/46, the CJEU was asked to interpret the aforementioned definition in the context of personal data made available on the internet. It ruled that loading personal data on an internet page constitutes personal data processing as it relates to the operations of "*transmission, dissemination or otherwise making data available*" that are examples listed in the above definition. This finding was first affirmed in *Lindqvist*[233] and is now settled case law, after its confirmation in *Google Spain and Google* (with respect to the publication of content by third parties on web pages)[234] and *Weltimmo*.[235]

226 Judgment of 20 December 2017, *Peter Nowak v Data Protection Commissioner*, C-434/16, ECLI:EU:C:2017:994, paragraph 31.

227 Judgment of 11 December 2014, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428, paragraph 22 and confirmed in Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122, paragraph 31.

228 Judgment of 11 December 2014, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428, paragraph 21; Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122, paragraph 30.

229 Judgment of 11 December 2014, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428, paragraph 15.

230 Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122, paragraph 32.

231 Judgment of 24 September 2019, *GC and Others*, C-136/17; ECLI:EU:C:2019:773, paragraph 72.

232 Article 4(2) of Regulation 2016/679 now provides that the notion of processing "*means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*".

233 Judgment of 6 November 2003, *Lindqvist*, C-101/01, paragraph 25.

234 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 35.

235 Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, paragraph 37.

132. Otherwise, the decisions delivered by the CJEU have provided an extensive array of concrete examples of processing activities. For instance, the CJEU clarified that the processing of personal data includes *"any operation performed upon such data by a third party, such as the collecting, recording, storage, consultation or use thereof*".[236] Additionally, the CJEU held that communication of the names and addresses of certain internet users by a telecom operator or an internet service provider to a third party constitutes processing of personal data.[237] Similarly, the communication of the names and surnames of individuals to a person who requested access to documents containing the same amounts to 'processing'.[238] The collection and use of personal data by tax authorities also fall within the aforementioned definition.[239] Similarly, the recording and use of personal data by an entity, their transmission to the court of audit and inclusion in a report are all processing operations.[240] Most importantly, the CJEU ruled that transferring personal data from an EU Member State to a third country is "*in itself*" processing of personal data as it involves "*disclosure by transmission, dissemination or otherwise making available*".[241] Other processing activities of "*disclosure by transmission, dissemination or otherwise making available*" include the communication of personal data to a journalist by a person who has necessarily had access to such data (i.e. the leak of said information) and the publication of a press release that included personal data[242]. Furthermore, in *Satakunnan Markkinapörssi and Satamedia*, the CJEU considered that the list of activities carried out on the personal data at issue all constitute personal data processing (e.g. collection from the public domain, publication, transfer on a CD-ROM, sending text messages).[243] Finally, the collection, storage and transmission of personal data by a regulated body or by private detectives acting for the latter also constitute personal data processing.[244]

133. The CJEU concluded that the operations carried out by a search engine need to be classified as processing of personal data given that the activity entails finding personal data published on the internet, indexing it automatically, storing it and making it available to internet users according to a particular preferential order.[245] In fact, such an activity involves several operations that are "*expressly and unconditionally*" listed under Article 2(b) such as retrieval, recording, organisation, making available and disclosure. The fact that the operator of a search engine does not differentiate between the categories of data and carries out the same operations with respect to non-personal data does not affect this previous finding. Finally, the fact that such an operator does not alter personal data that have already been published by third parties on the internet has no influence over the qualification of processing either.

134. In the context of a video-surveillance system, the CJEU considered that a "*video recording of persons which is stored on a continuous recording device*" constitutes automatic processing.[246] Additionally, publishing a video recording that includes personal data on a video-sharing and streaming website also constitutes processing of that data.[247]

(c) *Controller*

(i) General

135. Article 2(d) of Directive 95/46 defined a 'controller' as the "*natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law*".[248] Article 4(7) of Regulation 2016/679 has retained the same definition of controller as in the repealed Directive 95/46.

136. In *Google Spain and Google,* the Grand Chamber asserted that the broad definition of "controller' aims at ensuring "*effective and complete protection of data sub-*

236 Judgment of 17 October 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670, paragraphs 28-29. In this case, the CJEU considered that taking and storing digital fingerprints on the individuals' passport constitutes processing of personal data.

237 Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, paragraph 45; Judgment of 12 April 2012, *Bonnier Audio AB et Perfect Communication Sweden AB*, C-461/10, ECLI:EU:C:2012:219, paragraph 52.

238 Judgment of 7 July 2011, *Gregorio Valero Jordana*, T-161/04, ECLI:EU:T:2011:337, paragraph 91; similarly Judgment of 8 November 2007, *Bavarian Lager v Commission*, Case T-194/04, ECLI:EU:T:2007:334, paragraph 105, which was upheld on appeal by Judgment of 29 June 2020, *Commission v. Bavarian Lager Co*., C-28/08, ECLI:EU:C:2010:378, paragraph 23.

239 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraph 34. A similar processing was examined Judgment of 16 December 2008, *Huber*, C-524/06, ECLI:EU:C:2008:724, paragraph 43.

240 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, ECLI:EU:C:2003:294, paragraph 64.

241 Judgment of 6 October 2015, *Schrems I*, C-362/14, ECLI:EU:C:2015:650, paragraph 45. This analysis was confirmed in judgment of 16 July 2020, *Schrems II*, C-311/18, ECLI:EU:C:2020:559, paragraph 83.

242 In this case, the CJEU applied Regulation 45/2001, whose Article 2(b) provided for an identical definition of 'processing' as in Directive 95/46. Judgment of 21 September 2007, *Kalliopi Nikolaou*, T-259/03, ECLI:EU:T:2007:254, paragraphs 204 and 222.

243 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraphs 36-37.

244 Judgment of 7 November 2013, *IPI*, C-473/12, ECLI:EU:C:2013:715, paragraph 26.

245 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 28.

246 The storage was carried out on the memory of the camera in Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122, paragraph 35, and on the hard disk drive of the video-surveillance system in Judgment of 11 December 2014, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428, paragraphs 23 and 25.

247 Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122, paragraph 39.

248 See also Guidelines 07/2020 on the concepts of controller and processor in the GDPR of the EDPB, 2 September 2020.

jects".[249] This has become settled case law since the CJEU later confirmed this broad definition in *Wirtschaftsakademie Schleswig-Holstein*[250] and *Fashion ID*[251]. In fact, the CJEU considered in *Google Spain and Google* that excluding search engine operators from the scope of the definition of controller would violate both the wording of the definition and its objective. The fact that such operators do not exercise any control on the personal data published on third-party websites and that they automatically index it to make it available to users does not affect this finding.[252]

137. In *Jehovan todistajat*, the CJEU considered that the aforementioned definition does not require controllers to determine the purposes and means of processing through "*written guidelines or instructions*". In fact, the determination of the purposes and means might occur when a person "*exerts influence over the processing of personal data, for his own purposes*".[253]

138. Finally, regarding the processing of personal data by public bodies, the CJEU recently asserted in *Land Hessen* that the notion of 'controller' is "*not confined to public authorities, but (…) is sufficiently wide to include any body which, alone or jointly with others, determines the purposes and means of the processing of personal data*".[254] For instance, the Petitions Committee of the parliament of a Federated State of a Member State acts as a controller if it determines the purposes and means of data processing.[255] Furthermore, in *Ryneš*, the CJEU examined processing operations executed by a controller who was a natural person.[256]

(ii) Joint controllership

139. The definition of 'controller' distinguishes between a person who determines the purpose and means of processing "*alone*" and a person who does so "*jointly with others*". Directive 95/46 did not elaborate further on the concept of joint controllership. In fact, it did not mention this concept in its recitals and provisions either. Regulation 2016/679, on the other hand, has introduced a specific Article 26 dedicated to joint controllers which restates the definition "*Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers*".[257]

140. According to the CJEU, the terms "*alone or jointly*" imply that the concept of the controller "*may concern several actors taking part in that processing, with each of them then being subject to the applicable data protection provisions*".[258] In three recent landmark decisions, the CJEU has held that several persons must be qualified as controllers jointly responsible for processing.[259]

141. In all these decisions, the CJEU ruled that for persons to be joint controllers, it is not necessary that all of them have access to the personal data processed. Additionally, when joint controllers are responsible for a specific processing activity within a chain of processing activities, they do not act as controllers for preceding or subsequent processing if they do not determine either the purposes or the means of the same.[260]

142. Interestingly, the CJEU specified that "*the existence of joint responsibility does not necessarily imply equal responsibility of the various operators*" involved in the processing of personal data.[261] In fact, "*those operators may be involved at different stages of that processing of personal data and to different degrees*", as a result of which, "*the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case*".[262] However, the CJEU did not clarify ways of determining the respective level of responsibility of joint controllers and particularly how this finding interacts with Article 26 of the GDPR which requires the latter to 'determine their respective responsibilities for compliance'.

143. In *Wirtschaftsakademie Schleswig-Holstein*, the Grand Chamber analysed the processing of personal data associated with a fan page hosted on Facebook and created by an organisation (the administrator).[263] The administrator can request Facebook to provide statistical data on the visitors of its fan page in accordance with the parameters it

249 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 34.
250 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, paragraph 28.
251 Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 66.
252 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 34; confirmed in Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773, paragraph 35.
253 Judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:551, paragraphs 67-68.
254 Judgment of 9 July 2020, *Land Hessen*, C-272/19, ECLI:EU:C:2020:535, paragraph 65.
255 Judgment of 9 Jul 2020, *Land Hessen*, C-272/19, ECLI:EU:C:2020:535, paragraph 73.
256 Judgment of 11 December 2014, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428, paragraph 13. In this case, Mr. Ryneš set up a camera system next to his family home.
257 See also Guidelines 07/2020 on the concepts of controller and processor in the GDPR of the EDPB, 2 September 2020.
258 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, paragraph 29.
259 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388; Judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:551; Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629.
260 Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 74.
261 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, paragraph 43; Judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:551, paragraph 66; Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 70.
262 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, paragraph 43; Judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:551, paragraph 66; Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 70.
263 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388.

can define, such as the characteristics of the target audience. To that end, Facebook drops cookies on the visitors' devices to collect information and report to the administrator. According to the CJEU, the creation of the fan page by the administrator "*gives Facebook the opportunity*" to place such cookies.[264] Moreover, by defining specific parameters for compiling the statistical data, the administrator helps determine the purposes and means of the processing. Therefore, the CJEU asserted that the administrator of the fan page acts as a controller jointly with the social media provider for this processing. In contrast, the CJEU considered that the mere use of a social network does not make social network users joint controllers with the social network.[265]

144. In *Jehovan todistajat*, the CJEU considered that the members of the Jehovah's Witnesses Community who engage in door-to-door preaching jointly act as controllers with their Community for the processing of personal data relating to the persons visited.[266] Indeed, in this decision, while the Community organises, coordinates and encourages door-to-door preaching from its members to spread their faith, the members determine the circumstances of collection of personal data, the category of data collected and its subsequent processing.

145. In *Fashion ID*, the CJEU analysed the legal qualification of a website publisher who embeds a social plugin, such as the Facebook "Like" button.[267] Social plugins cause the automatic transmission of personal data relating to the website's visitors to the corresponding social network. The website publisher does not directly exercise control over the data thereby transmitted. The automatic transmission occurs regardless of whether users click on the social plugin or whether they hold an account with the social network. Therefore, the CJEU stated that the website publisher acts as a controller jointly with the social network with respect to the collection and transmission of the personal data relating to the website's visitors. In fact, by embedding the social plugin, the website publisher has "*made it possible*" for the social network to automatically obtain personal data relating to all the website's visitors.[268] By doing so, the website publisher "*exerts a decisive influence over the collection and transmission*" of the concerned personal data. However, the CJEU held that the website operator does not determine the purposes and means of subsequent operations involving the processing of personal data carried out by the social network after its transmission to the latter. Therefore, the website operator cannot be considered to be a joint controller with respect to those subsequent processing operations.[269]

(d) *Filing system*

146. Article 2(c) of Directive 95/46 defined filing systems as "*any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis*". The CJEU has deemed that filing systems correspond to "*manual processing*" as opposed to automatic processing.[270]

147. The notion of 'filing system' is relevant to determine the material scope of Directive 95/46 and Regulation 2016/679, as explained in Section 3.1.1. Both apply to personal data processed by automatic means and *"otherwise than by automatic means"* that forms part of a filing system or which is intended to form part of a filing system (Art. 3(1) of Directive 95/46 and Art. 4(6) of Regulation 2016/679).

148. In *Jehovan todistajat*, the CJEU applied this definition to a set of personal data comprising names, addresses and other information relating to the individuals contacted in the course of door-to-door preaching by the Jehovah Community's members.

149. The CJEU concluded that the concerned set of personal data represents a filing system, "*if those data are structured according to specific criteria which, in practice, enable them to be easily retrieved for subsequent use*".[271] In this decision, the CJEU noted that the members of the Jehovah Community used the name, address, beliefs of the persons contacted as well as their wish not to receive further visits as criteria to easily retrieve these persons. Additionally, since the aforementioned definition does not specify any practical means or requirements to structure filing systems or their form, filing systems do not necessarily include "*data sheets, specific lists or other search methods*".[272]

150. Finally, it is noteworthy that while Recitals 15 and 27 of Directive 95/46 both stated that the structure of filing systems must allow "*easy access*" to the corresponding personal data, Regulation 2016/679 does not expressly refer hereto. The accessibility of personal data structured in filing systems is still included in the definition of filing systems, which is identical to the one in Directive 95/46.[273] However, it is likely that the lack of reference to the "*ease*"

264 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, paragraph 35.
265 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, paragraph 35.
266 Judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:551.
267 Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629.
268 Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 75.
269 Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 76.
270 Judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:551, paragraph 53.
271 Judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:551, paragraph 62.
272 Judgment of 10 July 2018, *Jehovan todistajat*, C-25/17, ECLI:EU:C:2018:551, paragraph 58.
273 Article 4(6) of Regulation 2016/679.

of accessibility broadens the definition of filing systems even further.

(e) *(Main) establishment*

(i) Importance of the concept of establishment

151. The concept of 'establishment' is present in both Directive 95/46 and Regulation 2016/679.[274]

152. In fact, Recital 19 of Directive 95/46 stated that an establishment on the territory of a Member State "*implies the effective and real exercise of activity through stable arrangements; (…) the legal form of such an establishment, whether simply* [a] *branch or a subsidiary with a legal personality, is not the determining factor in this respect*". This concept was used to identify the applicable national laws. According to Directive 95/46, Member States shall apply the national provisions adopted pursuant to the Directive when "*the processing is carried out in the context of the activities of an establishment*" in the concerned Member States.[275]

153. Regulation 2016/679 has substantially retained the definition of 'establishment' in Recital 22.[276] It however introduced the new definition of 'main establishment' for controllers and processors (Art. 4(16), as clarified by Recital 36). The concept of 'main establishment' applies to controllers and processors with an establishment in more than one Member State. It is differentiated from the situation in which a controller or processor has a 'single' establishment in the European Union. Under Regulation 2016/679, these notions are the cornerstone of enforcement. In fact, the existence of a main or single establishment for a controller or processor will influence the determination of the enforcement authority for the supervision of cross-border processing carried out by that controller or processor (i.e. the lead supervisory authority as detailed in Article 56 of Regulation 2016/679). Specifically, the location of the main or single establishment determines the location of the competent supervisory authority. That authority is in charge of coordinating with the concerned supervisory authorities of other Member States.[277]

(ii) Interpretation of the concept under Directive 95/46

154. The CJEU has interpreted the concept of 'establishment' under Directive 95/46 in several cases to determine whether national laws applied to the processing carried out by a controller.

155. In the landmark decision *Google Spain and Google*, the Grand Chamber held that although not located in the EU, the search engine provider Google Inc. had an 'establishment' in Spain since it met the condition of an "*effective and real exercise of activity through stable arrangements*" on the basis of its subsidiary there.[278]

156. The CJEU applied a very similar reasoning in *Wirtschaftsakademie Schleswig-Holstein* in which it considered that Facebook Inc. and Facebook Ireland had a permanent establishment in Germany through a subsidiary.[279]

157. The CJEU further extended the concept of 'establishment' in *Weltimmo* and *Verein für Konsumenteninformation*.[280] In *Weltimmo*, the CJEU viewed this concept as "*a flexible definition* (…) *which departs from a formalistic approach whereby undertakings are established solely in the place where they are registered*". As subsequently confirmed in *Verein für Konsumenteninformation*, even a "*minimal*" activity exercised through stable arrangements needs to be considered an establishment.[281] To apply such a concept concretely, "*both the degree of stability of the arrangements and the effective exercise of activities in that other Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet*".[282] According to this reasoning, the existence of a representative in a Member State might constitute an establishment if "*that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned*".[283] However, the CJEU specified that "*such an establishment cannot exist merely because the undertaking's website is accessible*" in the concerned Member State.[284]

274 See also the Guidelines for identifying a controller or processor's lead supervisory authority of WP29, 5 April 2017, 16/EN, WP 244 rev.01.

275 Article 4(1)(a) of Directive 95/46 provides that "1. *Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable*".

276 Recital 22 of Regulation 2016/679 states that "(…) *Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect*."

277 The coordination procedure is set out in Article 60 of Regulation 2016/679.

278 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraphs 48-49.

279 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, ECLI:EU:C:2018:388, paragraphs 59-61.

280 Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, paragraphs 29 to 31; Judgment of 28 July 2016, *Verein für Konsumenteninformation*, C-191/15, ECLI:EU:C:2016:612, paragraphs 74-77.

281 Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, paragraph 31; Judgment of 28 July 2016, *Verein für Konsumenteninformation*, C-191/15, ECLI:EU:C:2016:612, paragraph 75.

282 Judgment of 1 October 2015, *Weltimmo*., C-230/14, ECLI:EU:C:2015:639, paragraph 29; confirmed in.Judgment of 28 July 2016, *Verein für Konsumenteninformation*, C-191/15, ECLI:EU:C:2016:612, paragraph 77

283 Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, paragraph 30.

284 Judgment of 28 July 2016, *Verein für Konsumenteninformation*, C-191/15, ECLI:EU:C:2016:612, paragraph 76.

158. The consequences of the broad interpretation of the notion of establishment are explained in Section 3.1.2 above, which deals with the territorial scope of Directive 95/46.

3.2 *Principles*

3.2.1 *Principles relating to processing of personal data*

159. The principles relating to data quality (Article 6 of Directive 95/46) and to processing of personal data (Article 5 of Regulation 2016/679) are a quintessential aspect of the lawfulness of processing of personal data. As the CJEU has recalled in many instances, *"all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the directive"*.[285]

160. They reflect the fundamental nature of the right to privacy and the right to data protection[286] and have their origins in Convention 108, which was the first international legally binding text on data protection.[287]

(a) *Lawfulness, fairness and transparency*

161. Article 6(1)(a) of Directive 95/46 required personal data to be processed 'fairly and lawfully'. Article 5(1)(a) of Regulation 2016/679 slightly expands the concept by adding the obligation to process personal data in a transparent manner with respect to the data subject.

162. The CJEU has currently received only one request for preliminary ruling that dealt with this principle. In *Bara and Others*, the CJEU ruled that 'fair processing' requires a public authority to inform the data subjects of the transfer of their personal data to another public authority that would process these data for its own purposes.[288]

(b) *Purpose limitation*

163. According to Article 6(1)(b) of Directive 95/46 and Article 5(1)(b) of Regulation 2016/679, personal data must be "*collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*".

164. In the first data protection-related request for a preliminary ruling, *Österreichischer Rundfunk and Others,* the CJEU had to assess whether the requirement for certain public bodies to disclose the identity and the amount of the salaries or pensions of individuals exceeding a certain threshold to the national Court of Audit was compatible with Article 6(1)(b) of Directive 95/46. The CJEU ruled that the purposes of this legal requirement, which was *"to exert pressure on the public bodies concerned to keep salaries within reasonable limits"* could be considered a "*specified, explicit and legitimate purpose*".[289]

165. In *Worten,* the CJEU held that the requirement to collect personal data for 'specified, explicit and legitimate purposes' as set out in Article 6(1)(b) of Directive 95/46 is complied with when a controller keeps a record of working time for its employees, where this processing activity is intended to ensure compliance with the national working conditions regulations.[290]

166. The CJEU has also examined the purpose limitation principle in two cases relating to the processing of biometric data on passports or identify cards. In *Schwarz,* the CJEU took the view that the storage of fingerprints in a passport *"does not go beyond what is necessary in order to achieve the aim of protecting against the fraudulent use of passports"*.[291] It did recognise a certain risk that public authorities might be tempted to store the fingerprints centrally to use it for other purposes (e.g. in the context of a criminal investigation). However, the CJEU insisted that this did not affect in itself the validity of Regulation 2252/2004[292] insofar as it does not provide a legal basis for such centralised storage. In other words, it appears that the CJEU held that the mere possibility of further processing in a manner incompatible with the initial purpose does not constitute in itself an infringement of the principle of purpose limitation.

167. The issue of a central database containing fingerprints was also at stake in *Willems and Others.*[293] Several Dutch citizens feared the so-called 'function creep'[294], i.e. the fact that their biometric data might be used for judicial purposes or by the intelligence and security services.

285 In this context, the CJEU also specified that compliance with one of the legal bases for the processing of personal data set out in Article 7 of Directive 95/46 or in Article 6 of Regulation 2016/679 only comes second. See e.g. Judgment of 20 May 2003, *Österreichischer Rundfunk e.a,* C-465/00, ECLI:EU:C:2003:294, paragraph 65, Judgment of 16 December 2008, *Huber,* C-524/06, ECLI:EU:C:2008:724, paragraph 48; Judgment of 24 November 2011, *ASNEF,* joined cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, paragraph 26; Judgment of 30 May 2013, *Worten,* C-342/12, ECLI:EU:C:2013:355, paragraph 33; Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 71; Judgment of 1 October 2015, *Bara and Others*, C-201/14, ECLI:ECLI:EU:C:2015:638, paragraph 30.

286 See Section 2 above.

287 Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, ETS No.108.

288 Judgment of 1 October 2015, *Bara and Others*, C-201/14, ECLI:EU:C:2015:638, paragraph 34.

289 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, paragraph 81.

290 Judgment of 30 May 2013, *Worten,* C-342/12, ECLI:EU:C:2013:355, paragraphs 34-35.

291 Judgment of 17 October 2013, *Schwarz,* C-291/12, ECLI:EU:C:2013:670, paragraph 63.

292 Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States (OJ 2004 L 385, p. 1), as amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 6 May 2009 (OJ 2009 L 142, p. 1; corrigendum: OJ 2009 L 188, p. 127.

293 Judgment of 16 April 2015, *Willems and Others*, joined cases C-446/12-C-449/12, ECLI:EU:C:2015:238.

294 See also, Article 29 Working Party, Opinion 3/2005 on Implementing the Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, 30.9.2005, WP112, pp. 8-9.

Unfortunately, due to the legal technicalities of the manner in which the question had been asked, the CJEU did not provide an answer on the merits of this particular issue.

(c) *Data minimisation*

168. According to Article 6(1)(c) of Directive 95/46, personal data must be "*adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*".[295] As the CJEU recalled in *Asociația de Proprietari bloc M5A-ScaraA*, this 'principle of data minimisation' relates to the requirement of proportionality: is the processing of personal data proportionate to the purpose pursued?[296] Consequently, the principle of data minimisation is crucial when assessing the necessity of the processing of personal data for the purposes of an identified legitimate interest (Art. 7(f) of Directive 95/46 – Art. 6(1)(f) or Regulation 2016/679).

169. In *Österreichischer Rundfunk and others*, it is interesting to note that the CJEU based most of its reasoning on Article 8 of the ECHR to assess whether there was compliance with principle of data minimisation of Article 6(1)(c) of Directive 95/46.[297] If this proportionality test was not met, according to the CJEU, the processing activity would also not satisfy the principle of data minimisation set out in Article 6(1)(c) of Directive 95/46.[298] The CJEU added, however, that it was for the national courts to ascertain whether this was the case.
Furthermore, the CJEU decided that Article 6(1)(c) of Directive 95/46 was directly applicable. Therefore, individuals could rely on it before national courts *"to oust the application of rules of national law which are contrary to those provisions"*.[299]
We believe that this two-tiered approach, with a significant emphasis on the ECHR, should be seen considering the fact that this was the first request for a preliminary ruling concerning data protection. In later cases, the CJEU appears to have adopted an approach whereby it referred to the ECHR or the Charter more in a general context, following which it based its reasoning directly on the provisions of Directive 95/46.[300]

170. In *Worten*, the CJEU concluded that the communication of a record containing the working hours' begin and end, as well as the breaks in between, to the employment inspector does not violate the principle that data must be 'adequate, relevant and not excessive' if the processing is necessary to allow the employment inspector to monitor the application of working time legislation.[301]

171. In its landmark decision *Google Spain and Google*[302], the CJEU clarified how the principles relating to processing of personal data[303] are crucial in the interpretation of other data protection obligations and rights.
In this case, the referring court essentially wanted to understand whether Articles 12(b) and 14(b) of Directive 95/46 allow a data subject to order the operator of a search engine to remove links to web pages published lawfully by a newspaper and containing true information about the data subject from the list of results.[304]
In this context, the CJEU stressed that the requirement to ensure that the processing of personal data is 'adequate, relevant and not excessive' must not only be examined when the processing was initially started but also at any moment in time, and especially at the time when a data subject exercises their rights. As the CJEU stated, *"(…) even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed"*.[305]

172. In relation to video surveillance in an apartment building, the CJEU opined that the principle of data minimisation notably requires the controller to consider alternative measures that are less invasive to privacy (e.g. a security system using magnetic access cards and an intercom) and that the controller should seek to limit the processing of personal data to certain areas (e.g. only the entrance and common parts of a building) and during certain periods (e.g. only at night or outside normal working hours).[306]

(d) *Accuracy*

173. According to Article 6(1)(d) of Directive 95/46, personal data must be "*accurate and, where necessary, kept*

295 Article 5(1)(c) Regulation 2016/679 contains the same principle, albeit phrased slightly differently: 'Personal data shall be adequate, relevant and *limited to what is necessary* in relation to the purpose for which they are processed ('data minimisation').
296 Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraphs 30-31.
297 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, paragraphs 64-90. We add that the CJEU referred to principle of data minimisation as the 'requirement of proportionality'.
298 See Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, paragraph 91.
299 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, paragraphs 99-101.
300 See also chapter 2 above on the Charter, for a more detailed analysis of this topic.
301 Judgment of 30 May 2013, *Worten*, C-342/12, ECLI:EU:C:2013:355, paragraphs 34-35.
302 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317.
303 Or 'principles relating to data quality' as they were referred to under Directive 95/46.
304 See our analysis in Section 3.3.5 below.
305 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 93; Judgment of 24 September 2019, *GC and Others*, C-136/17; ECLI:EU:C:2019:773, paragraph 42.
306 Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraphs 48-51.

up to date". This article further states that reasonable steps must be taken to erase or delete inaccurate or incomplete data.[307]

174. In *Puškár*, the CJEU ruled that the creation by public authorities of a list containing individuals who are suspected to act as 'fronts' in company director roles can be proportionate if there are "*sufficient indications to assume that the data subjects are rightly included in that list*".[308]

175. In *Nowak*, the CJEU decided that "*it is apparent from Article 6(1)(d) of Directive 95/46 that the assessment of whether personal data is accurate and complete must be made in the light of the purpose for which that data was collected. That purpose consists, as far as the answers submitted by an examination candidate are concerned, in being able to evaluate the level of knowledge and competence of that candidate at the time of the examination. That level is revealed precisely by any errors in those answers. Consequently, such errors do not represent inaccuracy (…)*".[309]

176. However, according to the CJEU, there might be situations in which the answers of a candidate are inaccurate, e.g. if, following a mix-up of the examination scripts, answers of another candidate were attributed to the candidate concerned. Similarly, there might be situations where the examiner's comments are inaccurate because they do not accurately record the evaluation of the candidate's answers.

(e) *Storage limitation*

177. The storage limitation principle set out in Article 6(1)(e) of Directive 95/46 is phrased in a relatively general manner: "*personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed*".[310] Consequently, data retention periods must be determined by each controller individually, on a case-by-case basis, with regard to the purpose and the specific circumstances of the processing.

178. When dealing with the storage limitation principle, many controllers typically seek to establish the maximum retention period that can be justified for a given processing activity. It is therefore noteworthy that the first case referred to the CJEU in relation to this principle, *Rijkeboer*[311], entailed a data subject arguing that personal data concerning him were deleted too quickly.

179. In this case, the data subject had requested a Dutch local authority to notify him of all instances in which his personal data had been disclosed to third parties. On the basis of Dutch national law, such data was automatically erased after one year. The local authority had therefore only notified the data subject of the disclosures in the year preceding his request.

180. Therefore, the CJEU had to assess the relation between Articles 6(1)(e) (storage limitation) and 12(a) (right of access) of Directive 95/46.[312] The CJEU indicated that cases in which national rules limit the storage of information to relatively short periods of time (*e.g.* one year), it must be ensured that these short retention periods present "*a fair balance*" between "*the interest of the data subject in protecting his privacy*", particularly in exercising his rights under Directive 95/46 on the one hand and *"the burden which the obligation to store that information represents for the controller"* on the other.[313]

181. Adopting a similar reasoning as it did with the principle of data minimisation[314], in *Google Spain and Google,* the CJEU clarified that processing of personal data, which was initially lawful, might become incompatible with the principle of storage limitation *"where those data are no longer necessary in the light of the purposes for which they were collected or processed"* considering the time elapsed.[315]

182. In *Nowak*, the CJEU stated that considering a candidate's examination answers and the examiner's comments with respect to them, *"their retention in a form permitting the identification of the candidate is, a priori, no longer necessary as soon as the examination procedure is finally closed and can no longer be challenged, so that those answers and comments have lost any probative value"*.[316]

(f) *Accountability*

183. Article 5(2) of Regulation 2016/679 introduced the principle of accountability in EU data protection law.

184. In *Orange Romania*, the CJEU briefly mentioned this principle for the first time. When assessing whether the conditions for valid consent were met, the CJEU indicated that according to Article 5(2) of Regulation 2016/679, the controller must be able to demonstrate the lawfulness

307 Article 5(1)(2) Regulation 2016/679 phrases this principle in substantially the same terms.

308 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraphs 114 and 117.

309 Judgment of 20 December 2017, *Nowak*,C-434/16, ECLI:EU:C:2017:994, paragraph 53.

310 The principle is stated in virtually the same terms in Article 5(1)(e) of Regulation 2016/679.

311 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293.

312 For an analysis of the CJEU's findings regarding the right of access, see 3.3.3 below.

313 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 64.

314 See paragraph 36 above.

315 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 93; See also, Judgment of 24 September 2019, *GC and Others*, C-136/17; ECLI:EU:C:2019:773, paragraph 74.

316 Judgment of 20 December 2017, *Nowak*, C-434/16, ECLI:EU:C:2017:994, paragraph 55.

of the processing. Therefore, the controller bears the burden of proof relating to the existence of valid consent.[317]

3.2.2 *Lawfulness of processing*

185. It is the settled case law of the CJEU that all processing of personal data must comply with one of the criteria for lawful data processing.[318]

186. On several occasions, in relation to the implementation of Directives 95/46, the CJEU has had the opportunity to point out that Member States were neither allowed to add new principles relating to the lawfulness of processing to Article 7 of Directive 95/46 nor to impose additional requirements that can potentially amend the scope of these principles.[319] The CJEU justified its position by referring to the fact that Directive 95/46 intended to achieve harmonisation which is generally complete.

(a) *Consent*

(i) General

187. Before analysing the different conditions that constitute valid consent in the sense of Articles 7(a) and 2(h) of Directive 95/46 and of Articles 6(1)(a), 7 and 4(11) of Regulation 2016/679, it is important to know who should provide consent and who should seek it.

188. In *Deutsche Telekom*, the CJEU underlined that there is no provision in Directive 2002/58 allowing the telecommunications network operator to consent. The right of prior consent is "*conferred solely on subscribers*".[320] Although this conclusion was adopted in the specific context of Directive 2002/58, it seems to suggest that consent must always be obtained from the data subject whose personal data will be processed.[321]

189. In *Fashion ID*, with respect to the embedding of the Facebook "Like" button on a website, the CJEU, having determined that a website operator and the social network are joint controllers for the personal data transferred from the website to the social network[322], had to clarify which of them has the duty to obtain consent from the data subject.

190. Considering the fact that consent must be given prior to the processing of personal data, the CJEU ruled that "*it is for the operator of the website (…) to obtain consent, since it is the fact that the visitor consults that website that triggers the processing of the personal data.*"[323] Accordingly, Advocate General Bobek had observed that "[i]*t would obviously not be in line with efficient and timely protection of data subjects' rights if the consent were to be given only to the joint controller that is involved later (if at all), once the collection and transmission has already taken place.*"[324]

191. It can obviously not be contested that consent must be obtained by the joint controllers before the processing, i.e. the collection and subsequent transmission of personal data to the social network, begins. However, we find it strange that the CJEU only held the website operator responsible for collecting that consent. In our view, assuming it is technically possible, it would be more logical, that the social network designs its "Like" button with an embedded consent mechanism.

192. We opine that under Regulation 2016/679, in light of its Article 26(1), it should be for the joint controllers to decide who will be responsible for obtaining the data subject's consent.

(ii) Freely given

193. Unsurprisingly, in *Schwarz*, the CJEU ruled that "*persons applying for passports cannot be deemed to have consented to* [the] *processing of* [their] *fingerprints*" to the extent that it is essential for EU citizens to have a passport

317 Judgment of 11 November 2020, *Orange Romania*, C-61/19, ECLI:EU:C:2020:901, paragraph 42.

318 Article 7 of Directive 95/46 and Article 6 of Regulation 216/679. See notably, Judgment of 20 May 2003, *Österreichischer Rundfunk e.a*, C-465/00, ECLI:EU:C:2003:294, paragraph 65, Judgment of 16 December 2008, *Huber,* C-524/06, ECLI:EU:C:2008:724, paragraph 48; Judgment of 24 November 2011, *ASNEF,* joined cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, paragraph 26; Judgment of 30 May 2013, *Worten,* C-342/12, ECLI:EU:C:2013:355, paragraph 33; Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 71; Judgment of 1 October 2015, *Bara and Others*, C-201/14, ECLI:ECLI:EU:C:2015:638, paragraph 30, Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraph 36.

319 Judgment of 24 November 2011, *ASNEF*, Joined cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, paragraphs 24-32; Judgment of 19 October 2016, *Breyer,* C-582/14, ECLI:EU:C:2016:779, paragraph 57; Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraphs 37-38; Judgment of 11 November 2020, *Orange Romania*, C-61/19, ECLI:EU:C:2020:901, paragraph 34.

320 Judgment of 5 May 2011, *Deutsche Telekom*, C-543/09, ECLI:EU:C:2011:279, paragraph 56.

321 This is also the position adopted by the Dutch DPA in the WhatsApp decision and that of the Belgian DPA in its decision 25/2020. See College bescherming persoonsgegevens, Decision of 15 January 2013, Z2011-00987, https://autoriteitpersoonsgegevens.nl/sites/default/files/downloads/rapporten/rap_2013-whatsapp-cbp-definitieve-bevindingen-nl.pdf, p. 32 and Geschillenkamer van de Gegevensbeschermingsautoriteit, Decision of 14 May 2020, 25/2020; https://www.gegevensbeschermingsautoriteit.be/publications/beslissing-ten-gronde-nr.-25-2020.pdf, p. 17.

322 For a more detailed assessment of how the CJEU came to this conclusion, see 3.1.3(c) above.

323 Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 102.

324 Opinion of 19 December 2018, *Fashion ID,* C-40/17, ECLI:EU:C:2018:1039, paragraph 132.

to travel to non-member countries.[325] This reflects the requirement that consent must be 'free', although the CJEU oddly stated that EU citizens are not free to object – rather than to consent – to the processing of their fingerprints.[326]

194. The CJEU also underlined that "*in order to ensure that the data subject enjoys genuine freedom of choice, the contractual terms must not mislead him or her as to the possibility of concluding the contract even if he or she refuses to consent to the processing of his or her data*".[327]

195. In *Planet49*, the CJEU appears to have suggested that there is an issue regarding the requirement of 'freely given consent' when a data subject is required to consent to the processing of their personal data for advertising purposes as a prerequisite to their participation in a promotional lottery. However, as the referring court did not expressly refer a question in this regard, the CJEU unfortunately did not take a decision on the issue and only examined whether the consent provided was 'unambiguous' and 'specific (see Sections 3.2.2(a)(iii) and 3.2.2(a)(iv) below).[328]

(iii) Unambiguous

196. Regarding the requirement that consent must be 'unambiguous', in *Planet49* the CJEU ruled that reliance on a pre-ticked checkbox is compatible with neither Articles 2(h) and 7(a) of Directive 95/46 nor Articles 4(11) and 6(1)(a) of Regulation 2016/679. According to the CJEU, "*consent given in the form of a preselected tick in a checkbox does not imply active behaviour on the part of the website user*".[329] Since consent must be given 'unambiguously', "*it would appear impossible in practice to ascertain objectively whether a website user had actually given his or her consent to the processing of his or her personal data by not deselecting a pre-ticked checkbox*".[330]

(iv) Specific

197. In *Planet49*, regarding the requirement of 'specific consent', the CJEU set out that the indication of wishes of the data subject "*must relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes*".[331]

198. An interesting case in this context is *Deutsche Telekom*[332]. The facts of the case were as follows: Deutsche Telekom, a telecommunications network operator, operated a telephone directory enquiry service in the context of the Universal Service Directive[333]. Based on Article 12(2) of Directive 2002/58, inclusion in this directory is conditional upon the subscriber's consent. According to the principle in Article 25(2) of the Universal Service Directive, Deutsche Telekom also made the data in its telephone directory available to other undertakings publishing a telephone directory in return for payment. The referring court essentially wanted to understand whether Article 12(2) of Directive 2002/58 made the passing on of this data to other undertakings conditional upon the consent of the telecommunications network operator or of that of its subscribers.

199. In its judgment, the CJEU developed a reasoning, which today appears odd in light of Regulation 2016/679. The CJEU recalled that Article 12(1) of Directive 2002/58 and its Recital 38 provide the subscriber "*the opportunity to give free, specific and informed consent, for the purposes of Articles 2(h) and 7(a) of Directive 95/46, to the publication of his personal data in public directories*".[334] However, it then went on to state that this provision "*does not support the inference that the subscriber has a selective right to decide in favour of certain providers of publicly available directory enquiry services and directories*".[335] Therefore,the CJEU concluded that "[t]*he consent given (…) by a subscriber (…) to the publication of his personal data in a public directory relates to the purpose of that publication and thus extends to any subsequent processing of those data by third-party undertakings active in the market for publicly available directory enquiry services and directories, provided that such processing pursues that same purpose.*"[336]

200. Considering the evolution of the notion of consent triggered by Articles 4(11), 6(1)(a) and 7 of Regulation 2016/679, we are unsure whether this interpretation of the CJEU is still valid. The notion that the subscriber's consent for publication in the public directory of their

325 Judgment of 17 October 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670, paragraph 32.
326 Judgment of 17 October 2013, *Schwarz*, C-291/12, ECLI:EU:C:2013:670, paragraph 32.
327 See also Judgment of 11 November 2020, *Orange Romania*, C-61/19, ECLI:EU:C:2020:901, paragraph 41.
328 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 64.
329 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 52.
330 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 55. See also Judgment of 11 November 2020, *Orange Romania*, C-61/19, ECLI:EU:C:2020:901, paragraphs 35-37.
331 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraphs 58-59; Judgment of 11 November 2020, *Orange Romania*, C-61/19, ECLI:EU:C:2020:901, paragraphs 38-39. See also in the context of the inclusion of search results on a search engine, Judgment of 24 September 2019, *GC and Others*, C-136/17; ECLI:EU:C:2019:773, paragraph 62.
332 Judgment of 5 May 2011, *Deutsche Telekom*, C-543/09, ECLI:EU:C:2011:279.
333 Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services, OJ 2002 L 108, p. 51.
334 Judgment of 5 May 2011, *Deutsche Telekom*, C-543/09, ECLI:EU:C:2011:279, paragraph 58.
335 Judgment of 5 May 2011, *Deutsche Telekom*, C-543/09, ECLI:EU:C:2011:279, paragraph 62.
336 Judgment of 5 May 2011, *Deutsche Telekom*, C-543/09, ECLI:EU:C:2011:279, paragraph 65.

electronic communications operator also necessarily implies their consent to publication in a public directory operated by other undertakings appears incompatible with the requirement for specific and granular consent.[337]

(v) Informed

201. In *Orange Romania,* the CJEU indicated that the information that the controller is required to provide on the basis of Article 2(h) of Directive 95/46 and Article 4(11) of Regulation 2016/679, "*must enable the data subject to be able to determine easily the consequences of any consent he or she might give*".[338] Consequently, according to the CJEU, in situations where the data subject is misled regarding the possibility of concluding a contract even if they refuse to consent to the processing of their data, not only is the consent not freely given but also it is not given in an informed manner.[339] In our view, in the scenario described by the CJEU, the validity of the consent would indeed be affected because it was not freely given. We opine however that in this particular scenario, the consent would still be given in an informed manner if the controller informed the data subject about their identity and the purposes of processing (see also Recital 42 of Regulation 2016/679).

202. In *Planet49,* interestingly, the CJEU considered that reliance on a pre-ticked checkbox might also be problematic considering the requirement that the consent be 'informed'. According to the CJEU, "[i]*t is not inconceivable that a user would not have read the information accompanying the preselected checkbox, or even would not have noticed that checkbox, before continuing with his or her activity on the website visited*".[340] This position is also slightly surprising in our view. If the requirement of 'informed consent' would not be met because the data subject did not read the information provided by the controller, there would be many instances, even outside the context of pre-ticked checkboxes, in which a controller is unable to validly rely on consent. We believe that the requirement of 'informed consent' does not go beyond the obligation for the controller to make the information available to the data subject in a transparent and easily accessible manner.[341] If this obligation is fulfilled, it becomes irrelevant whether the data subject actually reads the information before giving consent.

(b) *Legal obligation*

203. Article 7(c) of Directive 95/46 stated that personal data may be processed if that "*processing is necessary for compliance with a legal obligation to which the controller is subject*.[342] The judgment in *Österreichischer Rundfunk and Others* clarified that the existence of a legal obligation is not sufficient in itself. Insofar as such a legal obligation interferes with fundamental rights[343], the interference is only justified if it is both necessary for and appropriate to the aim pursued by that legislation.[344]

204. As Advocate General Poiares Maduro recalled in his Opinion in *Huber*, the concept of necessity implies that "*the authority adopting a measure which interferes with a right protected by Community law in order to achieve a legitimate interest aim must demonstrate that the measure is the least restrictive for the achievement of this aim*".[345]

205. In *Worten,* the CJEU therefore decided that a national law that requires an employer to make a record of the working time available to the employment inspector is not incompatible with Article 7(c) of Directive 95/46 if the processing is necessary to allow the employment inspector to monitor the application of working time legislation.[346]

(c) *Performance of a task of public interest or official authority*

206. On the basis of Article 7(e) of Directive 95/46 and Article 6(1)(e) of Regulation 2016/679, personal data may also be processed if it is 'necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed'.

207. When assessing this legal ground, the CJEU typically adopted a similar approach to the one applied when assessing the 'necessity to comply with a legal obligation' criterion (Art. 7(c) of Directive 95/46).[347] In *Huber*, the CJEU examined the processing of personal data in a central register of foreign nationals for the purposes of the application of legislation relating to the right of residence. It ruled that this processing only satisfied the requirement of necessity laid down by Article 7(e) of Directive 95/46 if the register only contained the data which were necessary for the application of that legislation and if the centralised

337 See e.g. EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2002, paragraphs 55-61.

338 Judgment of 11 November 2020, *Orange Romania*, C-61/19, ECLI:EU:C:2020:901, paragraph 40.

339 See also Judgment of 11 November 2020, *Orange Romania*, C-61/19, ECLI:EU:C:2020:901, paragraph 41.

340 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 55.

341 In its Guidelines on Consent, in the context of 'informed consent' the EDPB also focuses on the obligation to provide information. It does not address the obligation to ensure that the data subject has also read the information. EDPB, Guidelines 05/2020 on consent under Regulation 2016/679, 4 May 2020, paragraphs 62-74.

342 See also Article 6(1)(c) of Regulation 2016/679.

343 In *Österreichischer Rundfunk and Others,* reference was made only to Article 8 of the ECHR, as the judgment preceded the effective date of the Charter. Today, the reasoning of the CJEU obviously also applies in relation to Articles 7 and 8 of the Charter.

344 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, paragraph 90.

345 Opinion of 3 April 2008, *Huber,* C-524/06, ECLI:EU:C:2008:194, paragraph 27, and the CJEU case law referred to in footnote 17.

346 Judgment of 30 May 2013, *Worten,* C-342/12, ECLI:EU:C:2013:355, paragraphs 34-35.

347 See paragraphs 171-172 above.

nature of the register allowed authorities to apply that legislation more effectively. On the other hand, the processing of the personal data in a central register for statistical purposes did not meet the 'necessity' requirement. Following the view of Advocate General Poiares Maduro, the CJEU indicated that this purpose can be attained by processing only anonymous data.[348]

208. In *Worten,* the CJEU therefore decided that a national law that requires an employer to make a record of the working time available to the employment inspector is not incompatible with Article 7(e) of Directive 95/46 if the processing is necessary to allow public authorities to monitor the application of working time legislation. However, the necessity requirement also implies that access shall be limited to those the authorities having such monitoring powers.[349]

209. In *Puškár*, the CJEU ruled that the creation of a list by public authorities of individuals who are suspected to act as 'fronts' in company director roles can be based on Article 7(e) of Directive 95/46 provided that these authorities have been assigned with such a task by national legislation in the public interest, that the processing is necessary to attain the objectives pursued and that "*all of the conditions for the lawfulness of that processing of personal data imposed by Directive 95/46 be satisfied*".[350]
Regarding the necessity requirement, building on its previous case law in this context[351], the CJEU indicated that the assessment of the necessity implies ascertaining whether the processing of the personal data is "*suitable for achieving the objectives pursued (…) and whether there is no other less restrictive means in order to achieve these objectives*".[352]

(d) *Legitimate interest*

(i) General

210. The legitimate interest is a legal ground that controllers often rely on. However, it is also a legal ground with somewhat of a negative connotation. It is therefore not surprising that several requests for preliminary rulings were referred to the CJEU that relate to Article 7(f) of Directive 95/46.[353] It is also a topic in which the case law of the CJEU has evolved over the years.

211. On two occasions, the CJEU has had the opportunity to point out that Member States were neither allowed to add new principles relating to the lawfulness of processing to Article 7(f) of Directive 95/46 nor to impose additional requirements that can amend the scope of these principles.[354] For instance, in *ASNEF,* the CJEU recalled that the national law stating that a controller can only rely on its legitimate interest or on that of third parties if the personal data appear in public sources is not compatible with Article 7(f) of Directive 95/46.[355]

212. The CJEU also confirmed that Article 7(f) of Directive 95/46 had direct effect.[356]

213. The most interesting cases relating to the legitimate interest however deal with its conditions. As we will see below, the position of the CJEU in relation to these conditions has slightly evolved over the years.

214. Initially, the CJEU indicated that Article 7(f) of Directive 95/46 contained two cumulative conditions. First, the processing of personal data must be necessary for the purposes of the legitimate interest pursued by the controller or by the third party or parties to whom the data are disclosed. Second, such interest must not be overridden by the fundamental rights and freedoms of the data subject.[357] However, it specified that the second condition implied "*a balancing of the opposing rights and interests concerned*".[358]

215. Since *Rīgas satiksme*, the CJEU has changed its consideration of the balancing exercise and now refers to three cumulative conditions: "*first, the pursuit of a legitimate interest by the data controller or by a third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the fundamental rights and freedoms of the person concerned by the data protection do not take precedence*".[359]

348 Judgment of 16 December 2008, *Huber,* C-524/06, ECLI:EU:C:2008:724, paragraphs 62-68. Opinion of 3 April 2008, *Huber,* C-524/06, ECLI:EU:C:2008:194, paragraph 23.
349 Judgment of 30 May 2013, *Worten,* C-342/12, ECLI:EU:C:2013:355, paragraphs 34-36.
350 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraphs 115 and 117.
351 See paragraph 171 and further above.
352 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraphs 111-113. See also Opinion of 30 March 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:253, paragraphs106-111.
353 See also WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 9 April 2014, WP217.
354 Judgment of 24 November 2011, *ASNEF*, Joined cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, paragraphs 24-32; Judgment of 19 October 2016, *Breyer,* C-582/14, ECLI:EU:C:2016:779, paragraph 57.
355 Judgment of 24 November 2011, *ASNEF*, Joined cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, paragraph 49.
356 Judgment of 24 November 2011, *ASNEF*, Joined cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, paragraph 50-55.
357 Judgment of 24 November 2011, *ASNEF*, Joined cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, paragraph 38.
358 Judgment of 24 November 2011, *ASNEF*, Joined cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, paragraph 40. See also, Judgment of 13 May 2014, *Google Spain and Google,* C-131/12, ECLI:EU:C:2014:317, paragraph 74 and Opinion of 10 July 2014, *Ryneš*, C-213/13, ECLI:EU:C:2014:2072, paragraph 64.
359 Judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:43, paragraph 28-32. See also, Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 95; Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraph 40.

(ii) Condition 1 – legitimate interest

216. In *Ryneš* and *Asociația de Proprietari bloc M5A-ScaraA,* the CJEU held that in the context of a camera system installation, the protection of the property, health and life of the controller and that of their family might constitute a legitimate interest.[360] Although the CJEU did not expressly address it, the foregoing obviously does not release the controller from the obligation to conduct this balancing act.

217. Similarly, there is no doubt, according to the CJEU, that the interest of a third party in obtaining the personal information of a person who damaged their property to sue that person for damages can be qualified as a legitimate interest.[361]

218. In a situation of joint controllership, the CJEU held that each controller "*should pursue a legitimate interest (…) through the processing operations in order for those operations to be justified in respect of each of them*".[362]

219. However, the most important clarification was added in the *Asociația de Proprietari bloc M5A-ScaraA* decision. According to the CJEU, the legitimate interest of the controller or third party to whom the personal data will be disclosed "*must be present and effective as at the date of the data processing and must not be hypothetical at that date.*"[363] However, in the context of a processing activity that aims to protect the property or life of the controller and that of others, it is not "*necessarily required, at the time of examining all the circumstances of the case, that the safety of property and individuals was previously compromised*".[364]

(iii) Condition 2 – necessity

220. According to the settled case law of the CJEU regarding the condition of necessity of processing, "*it should be borne in mind that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary*".[365]

221. In *Asociația de Proprietari bloc M5A-ScaraA*, the CJEU added that when verifying whether the processing of personal data is 'necessary' for the purpose of the legitimate interests pursued, "*Article 6(1)(c) of Directive 95/46* [i.e. the principle of data minimisation] *must be taken into account*".[366] It must be ascertained that the "*legitimate interest pursued, cannot reasonably be as effectively achieved by other means less restrictive of the fundamental rights and freedoms of data subjects*".[367]

(iv) Condition 3 – Balancing exercise

222. In several decisions, the CJEU has made it clear that the condition of balancing the opposing rights and interests at issue "*depends in principle on the specific circumstances of the particular case*".[368] Furthermore, it specified that in conducting the balancing exercise, the controller "*must take account of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter of Fundamental Rights of the European Union ('the Charter')*".[369]

223. In several decisions, the CJEU indicated the elements to be taken into account to assess the seriousness of the infringement of the data subject's rights and freedoms.

224. In *ASNEF,* the CJEU stated that the public nature of the personal data might be a relevant element when conducting the balancing exercise as it might reduce the seriousness of the infringement of the data subject's fundamental rights.[370]

225. On the other hand, the processing of personal data from non-public sources "*implies that information relating to the data subject's private life will thereafter be known by the data controller and, as the case may be, by the third party or parties to whom the data are disclosed. This more serious infringement of the data subject's rights enshrined in Articles 7 and 8 of the Charter must be taken into account and be balanced against the legitimate interest pur-*

360 Judgment of 11 December 2014, *Ryneš,* C-212/13, ECLI:EU:C:2014:2428, paragraph 34. See also, Opinion of 10 July 2014, *Ryneš*, C-213/13, ECLI:EU:C:2014:2072, paragraph 63-67 and Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA,* C-708/18, ECLI:EU:C:2019:1064, paragraph 42.

361 Judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:43, paragraph 29; Judgment of 29 January 2008, *Promusicae,* C-275/06, ECLI:EU:C:2008:54, paragraph 53-54.

362 Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraphs 96-97

363 Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraph 44.

364 Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraph 44.

365 Judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:43, paragraph 30; Judgment of 11 December 2014, *Ryneš,* C-212/13, ECLI:EU:C:2014:2428, paragraph 28; Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraph 46. See also the similar reasoning about the necessity requirement in the context Article 7(c) of Directive 95/46, as set out in paragraph 51.

366 Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraph 30.

367 Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraph 47.

368 Judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:43, paragraph 31; Judgment of 24 November 2011, *ASNEF*, Joined cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, paragraph 40; Judgment of 19 October 2016, *Breyer,* C-582/14, ECLI:EU:C:2016:779, paragraph 62, Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraph 52.

369 Judgment of 24 November 2011, *ASNEF*, Joined cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, paragraph 40. See also, Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 74 and Opinion of 10 July 2014, *Ryneš*, C-213/13, ECLI:EU:C:2014:2072, paragraph 64.

370 Judgment of 24 November 2011, *ASNEF*, Joined cases C-468/10 and C-469/10, ECLI:EU:C:2011:777, paragraph 44; See also Judgment of 4 May 2017, *Rīgas satiksme*, C-13/16, ECLI:EU:C:2017:43, paragraph 32 and Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraph 54.

sued by the data controller or by the third party or parties to whom the data are disclosed."[371]

226. Similarly, the age of the data subject might be a factor which should be considered in the context of balancing of interests. However, the fact that the data subject is a minor does not automatically imply that the data subject's fundamental rights prevail over the legitimate interest of the controller.

227. In *Asociația de Proprietari bloc M5A-ScaraA,* the CJEU also referred to the following elements: the nature of the personal data and especially their potentially sensitive nature, the specific methods of processing, the number of people that might access the data and the reasonable expectations of the data subject.[372]

228. In *Google Spain and Google,* regarding the publication of a piece of personal data on a website which is subsequently indexed on a search engine, the CJEU opined that "*the outcome of the weighing of the interests at issue to be carried out (…) may differ according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of the web page is at issue, given that, first, the legitimate interests justifying the processing may be different and, second, the consequences of the processing for the data subject, and in particular for his private life, are not necessarily the same*".[373] The CJEU rightfully held that the inclusion of the personal data in the list of results of a search engine "*makes access to that information appreciably easier for any internet user (…)* [I]*t is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page*".[374]

3.2.3 *Processing of special categories of personal data and data relating to criminal convictions and offences*

(a) *Principle*

229. Articles 8(1) and (5) of Directive 95/46 and Articles 9(1) and 10 of Regulation 2016/679 lay down a general prohibition for processing special categories of personal data and data relating to criminal convictions and offences or related security measures.[375]

230. In *GC and Others*, the CJEU, dismissing Google's arguments, ruled that this prohibition applies to every kind of processing of such data and to all controllers carrying out such processing including an operator of a search engine.[376]

However, the CJEU specified that the operator of a search engine is "*responsible not because* [special categories of personal data] *appear on a web page published by a third party but because of the referencing of that page and in particular the display of the link to that web page in the list of results*".[377] Consequently, the CJEU held that the prohibition in Articles 8(1) and (5) of Directive 95/46 only applied to the operator of a search engine "*on the occasion of a verification performed by that operator, under the supervision of the competent national authorities, following a request by the data subject*".[378]

(b) *Exception – Reasons of substantial public interest*

231. In *GC and Others*, the CJEU indicated that the freedom of expression, protected by Article 11 of the Charter might constitute a reason of substantial public interest[379] that a search engine operator may rely on, when displaying a link in the list of results with information relating to offences and criminal convictions.

(c) *Exception – Manifestly made public by the data subject*

232. When a data subject has manifestly made public special categories relating to them, not only is the publisher of a web page allowed to process that data on the basis of Article 8(2)(e) of Directive 95/46 and Article 9(2)(e) of Regulation 2016/679 but also the operator of a search engine who subsequently indexes this web page in the search results.[380]

3.3 ***Rights of the data subject***

3.3.1 *General*

233. Under Directive 95/46, data subjects benefitted from several rights related to their personal data. Throughout the years, the CJEU has played an important role in clarifying the practical implications of these rights. With Regulation 2016/679, the European legislator has consolidated the case law of the CJEU and has strengthened and broadened the rights of data subjects.

3.3.2 *Information to be provided*

(a) *General*

234. Articles 10 and 11 of Directive 95/46 imposed a duty on controllers to provide certain information to data

371 Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraph 55.
372 Judgment of 11 December 2019, *Asociația de Proprietari bloc M5A-ScaraA*, C-708/18, ECLI:EU:C:2019:1064, paragraphs 57-59.
373 See also, Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraphs 86.
374 See also, Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 86.
375 For an analysis of the CJEU's interpretation of these notions, see section 3.1.3(a) above.
376 Judgment of 24 September 2019, *GC and Others*, C-136/17; ECLI:EU:C:2019:773, paragraph 42.
377 Judgment of 24 September 2019, *GC and Others*, C-136/17; ECLI:EU:C:2019:773, paragraph 46.
378 Judgment of 24 September 2019, *GC and Others*, C-136/17; ECLI:EU:C:2019:773, paragraph 48.
379 Article 8(4) of Directive 95/46 or Article 9(2)(g) of Regulation 2016/679.
380 Judgment of 24 September 2019, *GC and Others*, C-136/17; ECLI:EU:C:2019:773, paragraphs 63-64.

subjects about the processing of their personal data. Under Regulation 2016/679, a similar but more detailed obligation is imposed by Articles 12 to 14. These Articles are included in Chapter III of this Regulation which signifies that Regulation 2016/679 now officially grants data subjects a right to be informed regarding the processing of their personal data.

235. The right to be informed is crucial and might in fact be considered one of the most important rights granted to data subjects by EU data protection law. Indeed, only when data subjects are aware that a controller is processing their data will they be able to exercise their other data subject rights.[381]

236. In *Rijkeboer,* the CJEU also clarified that the requirement to inform data subjects regarding the processing of their personal data (Art. 10 and 11 of Directive 95/46) and the right of access to information about a processing activity (Art. 12(a) of Directive 95/46) imposed two distinct obligations on a controller.[382] Compliance with one of these two similar obligations does not authorise a controller to ignore the other.

237. The CJEU has had the opportunity to clarify certain points regarding the manner in which controllers should comply with this duty to inform.

(b) *Timing of the provision of information*

238. Article 10 of Directive 95/46 did not specify when the controller should provide the information to the data subject in situations where the data are obtained directly from data subjects. The CJEU clarified on several occasions that this information must be provided "*immediately, that is to say, when the data are collected*".[383]

239. In contrast, when data are not obtained directly from the data subjects, the information may be provided at a later stage, particularly "*when the data are registered or, possibly, when the data are disclosed to a third party*"[384] in accordance with Article 11 of Directive 95/46.

240. It is noteworthy that Regulation 2016/679 has expressly incorporated the position of the CJEU in its Articles 13 and 14.

(c) *Person responsible for the provision of information*

241. In *Fashion ID*[385], the CJEU clarified who must provide the required information when dealing with a situation of joint controllership.

242. Having found that Fashion ID and Facebook were joint controllers in the collection and disclosure of a user's personal data by transmission to Facebook, the CJEU had to consider who was responsible for providing the information required by Article 10 of Directive 95/46. Advocate General Bobek noted in his Opinion that in a situation of joint controllership, one could think that the obligation of information will be fulfilled by either one of the joint controllers.[386] However, the Advocate General opined that the factual circumstances of the case should be taken into account to guarantee an efficient and timely protection of the data subject's rights.[387] Particularly, since the processing of personal data was triggered by the fact that a user visited Fashion ID's website, the Advocate General considered that the duty to inform the data subject should be incumbent on Fashion ID.[388]

243. The CJEU followed the Advocate General's reasoning. Since the data were collected at the moment when the data subject consulted Fashion ID's website, the CJEU concluded that Fashion ID was best placed to provide the information required by Article 10 of Directive 95/46 in a timely manner.[389]

244. As we did in relation to the CJEU's position on who is responsible to obtain consent[390], we opine that under Article 26(1) of Regulation 2016/679, it should be for the joint controllers to decide between them as to who will be responsible to provide the required information.

(d) *Nature of the information to be provided*

245. Both Directive 95/46 and Regulation 2016/679 contain a list of the information that a controller must provide to data subjects regarding the processing of their personal data. Nonetheless, the CJEU has had to answer questions regarding the nature of the information to be provided to data subjects on several occasions.

246. In the more recent *Planet49* case[391], the CJEU highlighted that it is clear "*from the words 'at least' in Article 10 of Directive 95/46 that that information is not listed*

381 Judgment of 1st October 2015, *Bara and Others*, C-201/14, ECLI:EU:C:2015:638, paragraph 33.
382 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraphs 67-69.
383 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 68; Judgment of 7 November 2013, *IPI*, C-473/12, ECLI:EU:C:2013:715, paragraph 23 and Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 104.
384 See Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 68; Judgment of 7 November 2013, *IPI*, C-473/12, ECLI:EU:C:2013:715, paragraph 23.
385 Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629.
386 Opinion of 19 December 2018, *Fashion ID*, C-40/17, ECLI:EU:C:2018:1039, paragraphs 132-133 and 141.
387 Opinion of 19 December 2018, *Fashion ID*, C-40/17, ECLI:EU:C:2018:1039, paragraphs 132-133.
388 Opinion of 19 December 2018, *Fashion ID*, C-40/17, ECLI:EU:C:2018:1039, paragraph 141.
389 Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraphs 102-103.
390 See paragraph 182 above.
391 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801.

exhaustively".[392] Although the duration of processing is not included in Article 10 of Directive 95/46, the CJEU held that "*information on the duration of the operation of cookies must be regarded as meeting the requirement of fair data processing*".[393] The CJEU considered that such interpretation was supported by Article 13(2)(a) of Regulation 2016/679, which specifically mentions that the controller must provide the data subject with information relating to the retention period to ensure fair and transparent processing.

247. In *Bara and Others,* the CJEU also referred to the requirement of fair processing of personal data laid down in Article 6 of Directive 95/46, when deciding that a public administrative body transferring personal data to another public administrative body is required to inform the data subjects of this transfer.[394]

248. Regarding the extent of the duty to inform, the CJEU clarified that a controller's duty to inform, as set out in Article 10 of Directive 95/46, is limited to those processing activities "*in respect of which it actually determines the purposes and means*".[395] In doing so, the CJEU followed Advocate General Bobek's Opinion that the extent of the obligation to inform data subjects imposed on a website operator who acts as a joint controller "*shall correspond with that operator's joint responsibility for the collection and transmission of the personal data*".[396] Therefore, a website operator cannot be expected to provide any information on further processing activities carried out by a third party and over which the website operator had no control. Although Fashion ID, in its capacity of joint controller, was indeed required to provide information to the users of its website pursuant to Article 10 of Directive 95/46, the CJEU held that such information needed only to relate to the processing of personal data for which Fashion ID actually determined the purposes and means. Fashion ID was not required to provide information regarding further processing activities implemented by Facebook once Facebook received the data as the former did not determine the purposes and means of such activities.[397]

249. In *Rijkeboer,* Advocate General Ruiz-Jarabo Colomer acknowledged that Directive 95/46 did not expressly impose any obligation on controllers to communicate the time-limit to request access to information to data subjects. However, the Advocate General opined that unless the data subject was provided with such information, "*it would be difficult to find a period as short as one year to be compatible with the principle of proportionality and, accordingly, with Directive 95/46*".[398] The CJEU however did not include this consideration in its judgment. Had this case been adjudicated under Regulation 2016/679, perhaps the CJEU would have decided to address it given that Regulation 2016/679 now requires data subjects to be informed of "*the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period*".[399]

250. In *Planet49*,[400] the CJEU was also asked to clarify whether Planet49, as a controller serving cookies on its website, was expected to provide information regarding third parties who could access the data related to cookies. On this issue, the CJEU first highlighted that regarding cookies, "*Article 5(3) of Directive 2002/58 requires that the user concerned has given his or her consent, having been provided with clear and comprehensive information, 'in accordance with Directive* [95/46]*', inter alia, about the purposes of the processing*".[401]

251. According to the CJEU, such clear and comprehensive information "*must be clearly comprehensible and sufficiently detailed so as to enable the user to comprehend the functioning of the cookies employed*".[402] The CJEU went on to clarify that "*in a situation (…) in which (…) cookies aim to collect information for advertising purposes relating to the products of partners of the organiser of the promotional lottery, (…) whether or not third parties may have access to those cookies form part of the clear and comprehensive information which must be provided to the user in accordance with Article 5(3) of Directive 2002/58*".[403]

3.3.3 *Right of access*

252. The right of access has been the subject of several questions before the CJEU, and as a result, the CJEU's case law has provided interesting clarifications regarding the application of this right in practice.

(a) *Objective and scope*

253. The CJEU had the opportunity to clarify the objective and the scope of the right of access in several cases, starting with the *Rijkeboer* case.[404]

392 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 78.
393 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 78.
394 Judgment of 1st October 2015, *Bara and Others*, C-201/14, ECLI:EU:C:2015:638, paragraphs 32-34.
395 Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraph 105.
396 Opinion of 19 December 2018, *Fashion ID*, C-40/17, ECLI:EU:C:2018:1039, paragraph 141.
397 See Section 3.1.3(c)(ii) on joint controllership.
398 Opinion of 22 December 2008, *Rijkeboer*, C-553/07, ECLI:EU:C:2008:773-paragraph 66.
399 See Art. 13(2)(a) and 14(2)(a) of Regulation 2016/679.
400 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801.
401 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 73.
402 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 74.
403 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 75.
404 See Section 172 above for a reminder of the facts of this case.

254. In this case, the CJEU noted that two categories of data were involved: first, the actual personal data relating to Mr Rijkeboer (the "basic data"), and second, information about the processing of such basic data (e.g. information on the recipients to whom the basic data were sent).[405] According to the CJEU, Article 12(a) of Directive 95/46 provided a right of access to both categories of data.

255. The CJEU drew this conclusion considering the objective of the right of access, which it examined with respect to the purposes of the Directive itself. The CJEU essentially found that the right of access was intended to serve the Directive's purposes of guaranteeing the individuals' right to privacy by enabling data subjects to carry out the necessary checks to ensure that their personal data are processed in a correct and lawful manner.[406] In light of this objective, the CJEU determined that a right of access to both the basic data and to the information about the processing of such basic data was "*necessary to enable the data subject to exercise the rights set out in Article 12(b) and (c) of the Directive*"[407].

256. This view on the objective of the right of access was reiterated in *YS and Others*[408]and *Nowak*[409]. In *Nowak*, the CJEU ruled that providing an examination candidate the right of access to the answers they had submitted to the examination and to any comments made by an examiner with respect to those answers, pursuant to Article 12(a) of Directive 95/46, did serve the purpose of Directive 95/46.

257. In *YS and Others*, the facts of the case led the CJEU to a different conclusion. As the CJEU had ruled that the legal analysis drafted by a case officer regarding a residence permit application did not constitute personal data relating to the concerned applicant[410], it determined that "*extending the right of access of the applicant (…) to that legal analysis would not in fact serve the directive's purpose (…), but would serve the purpose of guaranteeing him a right of access to administrative documents, which is not however covered by Directive 95/46*"[411].

(b) *Setting a time limit on the right of access to information about a processing activity*

258. *Rijkeboer* also provided an opportunity for the CJEU to address the issue of time limit on the right of access to information about the processing of personal data. In this case, the CJEU clarified that data subjects have a right of access to information about the processing of their personal data "*not only in respect of the present, but also in respect of the past*".[412] If the CJEU considered that setting a time limit to the right to access information about a processing conducted in the past could be envisaged, it highlighted that such time limit should still "*allow the data subject to exercise his different rights laid down in the Directive*".[413] Therefore, the information about the processing of personal data implemented in the past should be stored for a period determined to strike "*a fair balance*" between, on the one hand, the interest of the data subject in protecting their privacy and exercising their rights and, on the other hand, the burden which the obligation to store such information represents for the controller.[414]

(c) *Form of the access to the data*

259. Another issue that the CJEU had to address was related to the form in which the information requested by a data subject pursuant to Article 12(a) of Directive 95/46 should be communicated to the data subject.

260. In *YS and Others*, three third country nationals had applied for lawful residence in the Netherlands. Each of them had requested access to a document ("the minute") containing a legal analysis in the form of internal advice on whether to grant resident status on the basis of Article 12 of Directive 95/46. In this context, the CJEU was asked to clarify whether Article 12(a) of Directive 95/46 granted the data subject a right to obtain a copy of the minute or whether it would be sufficient to provide the data subject a full summary of any personal data relating to him in an intelligible form.

261. Advocate General Sharpston opined that "*Directive 95/46 did not require personal data covered by the right of access to be made available in the material form in which they exist or were initially recorded*"[415]. Furthermore, according to the Advocate General, "*the fact that personal data are contained in a document such as a minute does not imply that the data subject automatically has the right to that material form, that is to say, a copy or extract of that document*"[416].

262. Following the same logic, the CJEU ruled that Article 12(a) of Directive 95/46 did not confer on data subjects "*a right to obtain a copy of the document or the origi-*

405 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraphs 41-43.
406 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 49.
407 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 51; see also Recital 41 of Directive 95/46.
408 Judgment of 17 July 2014, *YS and Others*, C-141/12 and C-372/12, ECLI:EU:C:2014:2081, paragraph 44.
409 Judgment of 20 December 2017, *Nowak*, C-434-16, ECLI:EU:C:2017:994, paragraph 57.
410 See Section 3.1.3(a) above.
411 Judgment of 17 July 2014, *YS and Others*, C-141/12 and C-372/12, ECLI:EU:C:2014:2081, paragraph 46.
412 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 54 and paragraph 70.
413 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 57.
414 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 64.
415 Opinion of 12 December 2013, *YS and Others*, C-141/12 and C-372/12, ECLI:EU:C:2013:838, paragraph 74.
416 Opinion of 12 December 2013, *YS and Others*, C-141/12 and C-372/12, ECLI:EU:C:2013:838, paragraph 79.

nal file" in which their data appeared.[417] In fact, the CJEU held that the provision of a full summary of the personal data related to the data subject in an intelligible form was sufficient to comply with the right of access.[418]

263. This notion of 'intelligible form' must be interpreted as a "*form allowing the data subject to become aware of the personal data relating to him and to check that they are accurate and processed in compliance with* [the] *Directive, so that that person may, where relevant, exercise the rights conferred on him by* [the] *Directive*"[419]. Article 15(3) of Regulation 2016/679 now expressly confers on a data subject the right to obtain a copy of the personal data undergoing processing.

264. Finally, the CJEU indicated that the controller may redact information in the document that is not related to the data subject.[420]

(d) *Levying a fee for the exercise of the right of access*

265. In *X*, a woman had asked her municipality of residence to grant her access to her personal data. The municipality provided her a certified transcript of her personal data and demanded a fee of twelve euros and eighty cents for the same. The woman contested that request for payment.[421] In the context of this case, the CJEU had to consider whether Article 12(a) of Directive 95/46 should be interpreted as precluding the levying of fees with respect to the communication of personal data by a public authority.

266. Having examined the wording of Article 12(a) of Directive 95/46 in various European languages, the CJEU found that nothing in the wording of this provision suggested that the Member States were required to communicate the information referred to in the provision free of charge.[422] Therefore, the CJEU clarified that this provision should be interpreted as neither requiring Member States to levy fees when the right to access personal data was exercised nor prohibiting the levying of such fees so long as they were not excessive.[423]

267. On what constitutes 'excessiveness', the CJEU noted that Article 12(a) of Directive 95/46 did not list any criteria for assessing the fees levied when the right of access was exercised. In this context, Member States ultimately remained responsible for setting any fee (if any) at a level which was not excessive. According to the CJEU which followed an analogous reasoning as the one previously developed in *Rijkeboer*[424], when setting such fees, Member States should seek to strike a "*fair balance*" between the data subject's interests to exercise their data protection rights and the burden imposed on the controller. However, the CJEU added that in any event, the level of the fee should not constitute an obstacle to the exercise of the right of access and "*should not exceed the cost of communication of the data*"[425].

268. Deviating from the CJEU's position, Article 12(5) of Regulation 2016/679 states that this access must be provided free of charge and subject to the exceptions stated in the article.[426]

3.3.4 *Right of rectification*

269. Under Article 12(b) of Directive 95/46, a data subject was granted the right to obtain from the controller, *inter alia*, the rectification of personal data processed in a manner that was not compliant with Directive 95/46, "*in particular because of the incomplete or inaccurate nature of the data*". Currently, this right of rectification is enshrined in Article 16 of Regulation 2016/679 and is also very briefly mentioned under Article 8(2) of the Charter.

270. The *Rijkeboer* case emphasized, among other things, the close relationship between the right of access and the right of rectification. The CJEU stated that the right of access was "*necessary to enable the data subject to exercise his (…) right of rectification*"[427]. Indeed, as mentioned previously [428], the right of access enables the data subject to check whether their personal data are processed in a compliant manner or contrarily, whether there exists an incompatibility that could trigger the exercise of the right of rectification.

271. The *Nowak* case enabled the CJEU to address some concerns specifically relating to the right of rectification. The facts underlying the *Nowak* case were straightforward. After having failed an examination, a candidate submitted a data access request seeking all personal data relating to him held by the examiner.

417 Judgment of 17 July 2014, *YS and Others*, C-141/12 and C-372/12, ECLI:EU:C:2014:2081, paragraph 58.
418 Judgment of 17 July 2014, *YS and Others*, C-141/12 and C-372/12, ECLI:EU:C:2014:2081, paragraph 59.
419 Judgment of 17 July 2014, *YS and Others*, C-141/12 and C-372/12, ECLI:EU:C:2014:2081, paragraph 57.
420 Judgment of 17 July 2014, *YS and Others*, C-141/12 and C-372/12, ECLI:EU:C:2014:2081, paragraph 58.
421 Judgment of 12 December 2013, *X*, C-486/12, ECLI:EU:C:2013:836.
422 Article 12(a) of Directive 95/46 stated that data subjects should be able to exercise their right of access "*without excessive delay or expense*".
423 Judgment of 12 December 2013, *X*, C-486/12, ECLI:EU:C:2013:836, paragraph 22.
424 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 64.
425 Judgment of 12 December 2013, *X*, C-486/12, ECLI:EU:C:2013:836, paragraphs 29-31.
426 Article 12(5) of Regulation 2016/679 provides that the data controller may charge a "*reasonable fee taking into account the administrative cost of providing the information or communication or taking the action requested* (…) *where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character*". It should be noted that this Article 12(5) also specifies that the burden of demonstrating the manifestly unfounded or excessive character of the request is on the controller.
427 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 51.
428 On the right of access, see section 3.3.3 above.

272. In the context hereof, the CJEU clearly stated that "*the right of rectification provided for in Article 12(b) of Directive 95/46 cannot enable a candidate to 'correct', a posteriori, answers that are 'incorrect*'"[429].

273. Regarding the answers submitted by an examination candidate, the CJEU stated that it should be kept in mind that these answers were collected precisely to evaluate the candidate's level of knowledge and competence at the time of the examination. Any errors made by the candidate would precisely reflect such level and could therefore not be deemed 'inaccurate' within the meaning of Directive 95/46.[430] Therefore, the candidate would not be able to request that such errors be rectified under Article 12(b) of Directive 95/46.

274. However, the CJEU specified that there could still be some situations in which the answers given by the candidate could prove to be inaccurate, for instance, if examination scripts were mixed by mistake, causing the answers submitted by another candidate to be ascribed to the candidate concerned.

3.3.5 *Right to erasure*

275. Article 12(b) of Directive 95/46 also conferred on data subjects the right to obtain from the controller the erasure of personal data processed in a manner not compliant with Directive 95/46, "*in particular because of the incomplete or inaccurate nature of the data*". The CJEU has greatly contributed to clarifying the scope and application of the right of erasure under Directive 95/46. As a result, this right has been further detailed under Regulation 2016/679 where it is also referred to as the 'right to be forgotten'.

(a) *The origins of the right to be forgotten – The Google Spain decision*

276. The CJEU has also been involved in establishing a 'right to be forgotten' for data subjects based on the right of erasure under Article 12(b) of Directive 95/46 and on the right to object to the processing under Article 14(a) of the same Directive. Particularly, the CJEU first unveiled its arguments in favour of such a right to be forgotten in the landmark decision of *Google Spain and Google*.

277. It is noteworthy that pursuant to the CJEU case law, it seems that the right to be forgotten can have a legal basis in both the right to erasure and the right to object to the processing. Nonetheless, the right to erasure is commonly considered to be the primary legal basis for this right. In fact, Article 17 of Regulation 2016/679 is specifically entitled 'Right to erasure ('right to be forgotten')'. This section will thus primarily focus on the points made by the CJEU in relation to the right to erasure. Clarifications relating to the right to object to the processing can be found in Section 3.3.8 below.

278. The case of *Google Spain and Google* arose after a data subject lodged a complaint with the Spanish data protection authority against the publisher of a newspaper and against Google in 2010. The complaint was based on the fact that when an internet user entered his name in Google's search engine, the user would obtain links to pages of the publisher's newspaper dating back to 1998 on which the data subject's name appeared connected with attachment proceedings for the recovery of social security debts. Through this complaint, the data subject, who stated that the attachment proceedings concerning him had been fully resolved for years, requested two things. First, he asked that the publisher of the newspaper be required to remove or alter the newspaper pages so that the personal data relating to him would no longer appear on the same. Second, he requested that Google, as the operator of the search engine, be required to remove or conceal the personal data relating to him so that they would no longer be included in the search results nor appear in links to the publisher's newspaper (i.e. a request for de-referencing).

279. The facts of this case presented an extra complexity since the personal data relating to the data subject was involved in two separate processing activities.[431] The data was first processed by the publisher that published the data on its website. The data was subsequently processed by Google to reference the same in the list of results displayed following a search made on the basis of the data subject's name. Therefore two separate controllers, respectively the publisher and Google, carried out these two separate processing activities.

280. Having made this distinction, the CJEU focused on the obligations of the search engine operator instead of on those of the publisher in *Google Spain and Google*. In this context, the CJEU clarified the extent of the responsibility of the operator of a search engine with particular regard to the data subject's right of erasure.

(i) Responsibility of the operator of a search engine in the context of a request for erasure

281. The distinction between the two processing activities carried out by the publisher on the one hand and by the operator of the search engine on the other implied that each controller would be responsible for ensuring that their respective processing was compliant with Directive 95/46. Thus, the CJEU specified that a search engine operator, as the controller with respect to the data processing carried out as part of the activity of such a search engine,"*must ensure, within the framework of its re-*

429 Judgment of 20 December 2017, *Nowak*, C-434-16, ECLI:EU:C:2017:994, paragraph 52.

430 On the principle of accuracy, see section 3.2.1(d) above.

431 For an analysis of the definition of 'processing', see Section 3.1.3(b) above.

sponsibilities, powers and capabilities, that that processing meets the requirements of Directive 95/46, in order that the guarantees laid down by the directive may have full effect."[432]

282. In relation to a data subject's request to exercise the right of erasure (and right to object to the processing), the CJEU recalled that a search engine operator, as a controller, had an obligation to "*duly examine*" the merits of any such request, and where appropriate, end the processing of the personal data in question.[433] Such obligation would apply to the operator of the search engine directly regardless of whether or not the publisher who had initially published the data is required to erase its publication under Directive 95/46.

283. In fact, the CJEU noted that in some cases, the publication by a publisher on its web page of information relating to a data subject might benefit from one of the derogations from the requirements of Directive 95/46 laid out in Article 9 of said Directive (e.g. the derogation provided for processing carried out 'solely for journalistic purposes') and thus be lawful. The search engine operator would however most likely be unable to benefit from the same exemption. In such circumstances, the data subject would therefore be able to exercise their rights under Article 12(b) and 14(a) of Directive 95/46 against the operator of the search engine but not against the publisher of the web page.[434]

284. The CJEU also pointed out that the processing performed in the context of the activity of a search engine was "*liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet (…) and thereby to establish a more or less detailed profile of him*". The CJEU further added that the interference of such processing with the data subjects' rights was heightened by the importance of the role played by the internet and search engines in our society.[435]

285. In light of the aforementioned, the CJEU clarified that when examining the merits of a request made by a data subject under Article 12(b) of Directive 95/46, a search engine operator should seek a fair balance between the data subject's fundamental rights to privacy and to the protection of personal data on the one hand and the legitimate interest of internet users in having access to the information on the other. Accordingly, the CJEU considered that the data subject's rights to privacy and to protection of personal data would, as a general rule, override the interest of internet users to access information. However, there could be instances in which this would not be the case, particularly depending on the data subject's role in public life.[436] Consequently, the operator of a search engine will have to examine each request on a case-by-case basis.

286. Regarding the operator's responsibility in relation to a data subject's right to erasure, the CJEU thus concluded that to comply with such right and in so far as the conditions laid down in Article 12(b) of Directive 95/46 are met, "*the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful*."[437]

(ii) Scope of the right to erasure

287. Another issue addressed by the CJEU in *Google Spain and Google* concerned the scope of the data subject's right to erasure. More specifically, the CJEU provided some clarity on the conditions that should be met to enable a data subject to obtain the erasure of their personal data pursuant to Article 12(b) of Directive 95/46.

288. Under Directive 95/46, the application of the right of erasure (Art. 12(b)) was subject to the condition that the processing of personal data be incompatible with the directive. The wording of Article 12(b) referred to the situation in which the personal data would be incomplete or inaccurate. However, the CJEU clarified that such reference was only made "*by way of example*" and that "*the non-compliant nature of the processing (…) may also arise from non-observance of the other conditions of lawfulness that are imposed by the directive upon the processing of personal data*".[438] In other words, a data subject should have a right to obtain the erasure of their personal data such that the processing of such data did not comply with at least one of the data protection principles laid down in Article 6 of Directive 95/46.

432 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 83.
433 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 77.
434 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 85.
435 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 80.
436 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 81.
437 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 88.
438 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 70.

289. Although *Google Spain and Google* showed that the right to erasure might apply in many different situations, the CJEU illustrated in *Manni* that this right to erasure was in fact not an absolute right. Mr Manni, , the sole director and liquidator of a company that had been dissolved in 2005, appeared in the public companies register and had requested that his personal data be erased or blocked from said register in 2007. The CJEU was asked, in essence, "*whether the authority responsible for keeping the register should, after a certain period had elapsed since a company ceased to trade, and on the request of the data subject, either erase or anonymise that personal data, or limit their disclosure*".[439]

290. The CJEU noted that such registers were established pursuant to EU law in order, inter alia, to protect the interests of third parties with respect to joint stock companies and limited liability companies by enabling such third parties to inform themselves on these matters. In this regard, Advocate General Bot pointed out that it might be necessary to keep the data included in these registers even after the dissolution of the company, for instance, in order to "*assess the legality of an act carried out on behalf of that company during the period of its activity*" or "*so that third parties can bring an action against the liquidators of that company*"[440]. The CJEU further held that considering the different limitation periods in place in the different Member States, it was "*impossible (…) to identify a single time limit, as from the dissolution of a company, at the end of which the inclusion of such data in the register and their disclosure would no longer be necessary*"[441].

291. Considering the aforementioned, the processing of personal data carried out in the context of the companies register did not necessarily appear to be violating the principle of storage minimisation. The CJEU therefore decided that it could not be guaranteed that all the individuals listed in such public companies registers would have a right, "*as a matter of principle*", to obtain the erasure of their data from these registers after a certain period of time from the dissolution of the company to which their name was linked.[442]

(b) *Other illustration of a possible application of the right to erasure – The Nowak case*

292. The CJEU first provided an example of when the data subject could request the erasure of their personal data, even where such data was neither incomplete nor inaccurate, in the *Nowak* case. Indeed, *Nowak* illustrated that an examination candidate could "*have the right to ask the data controller to ensure that his examination answers and the examiner's comments with respect to them are, after a certain period of time, erased, that is to say, destroyed*"[443].

293. The CJEU's reasoning behind this example particularly relied on the principle of storage limitation (as mentioned in Art. 6(1)(e) of Directive 95/46) according to which personal data should not be kept in a form which permits the identification of data subjects for longer than necessary for the purposes for which the data was collected. In the context of an examination, the CJEU found that the answers submitted by a candidate and any comments made by the examiner with respect to such answers would no longer be relevant as soon as the examination procedure was closed and no longer subject to challenge. Consequently, the data subject could then request the answers and comments to be erased not because such answers were incomplete or inaccurate but because they would no longer be necessary considering the purposes for which they were collected and processed.

294. Article 17(1)(a) of Regulation 2016/679 now specifically mentions the situation in which "*personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed*" as one of the grounds enabling a data subject to request the erasure of their personal data.

(c) *The right to be forgotten applied to sensitive personal data*

295. The findings of *Google Spain and Google* were reiterated and refined in the case of *GC and Others* to address the specific issue of requests for de-referencing relating to special categories of personal data and to personal data relating to criminal offences (Art. 8(1) and (5) of Directive 95/46 and Art. 9(1) and 10 of Regulation 2016/679).

(i) Special categories of personal data

296. With regard to special categories of personal data, the CJEU clarified how the general prohibition of processing such data influenced the handling of a request for de-referencing by a search engine operator. According to the CJEU, when requested to de-reference links to web pages containing special categories of personal data, a search engine operator would be required, by way of principle, to accede such request unless one of the exceptions provided for under Directive 95/46 applied.[444]

439 Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, paragraph 44.
440 Opinion of 8 September 2016, *Manni*, C-398/15, ECLI:EU:C:2016:652, paragraphs 73-74.
441 Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, paragraph 55.
442 Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, paragraph 56.
443 Judgment of 20 December 2017, *Nowak*, C-434-16, ECLI:EU:C:2017:994, paragraph 55.
444 Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773, paragraph 69.

297. The CJEU clarified that such exception could in particular apply where the processing of special categories of personal data "*relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims*" (Art. 8(2)(e) of Directive 95/46). In such circumstances, the operator of a search engine can refuse to grant the requested de-referencing provided that the processing met all the other conditions of lawfulness laid down in Directive 95/46 and that the data subject would not be able to exercise their right to object to the processing under Article 14(a) of Directive 95/46.[445]

298. Finally, the CJEU took into account the fact that Regulation 2016/679 has now clarified through the exemptions listed under Article 17(3) that the right of erasure cannot be seen as an absolute right.[446] It considered that the operator should in any event seek to strike a balance between the data subject's rights to privacy and the protection of personal data on the one hand and the fundamental right of freedom of information on the other.[447] When balancing out these rights, the operator would need to consider "*all the relevant factors of the particular case*" and take into account "*the seriousness of the interference with the data subject's rights to privacy and protection of personal data*" with respect to the sensitive nature of the data at hand. As in *Google Spain and Google*, the CJEU ruled that the data subject's fundamental rights would, "*as a general rule*", override the public's right to freedom of information although this balance might vary depending on the specific circumstances of the case (*e.g.* the nature and sensitivity of the information in question or the role played by the data subject in public life).[448] In this context, the operator could refuse to accede the data subject's request for de-referencing relating to web pages containing special categories of personal data if the operator could establish that the referencing of such pages was "*strictly necessary for protecting the freedom of information of internet users*".[449]

(ii) Personal data relating to criminal offences

299. With regard to the requests for de-referencing of links to web pages including information relating to criminal proceedings brought against the data subject, concerning an earlier stage of the proceedings and no longer corresponding to the current situation, the CJEU considered that it was for the operator to assess whether the data subject had a right to the information no longer being linked with their name in a list of search results of their name.

300. The CJEU clarified that this assessment should be made "*in the light of all the circumstances of the case, such as, in particular, the nature and seriousness of the offence in question, the progress and the outcome of the proceedings, the time elapsed, the part played by the data subject in public life and his past conduct, the public's interest at the time of the request, the content and form of the publication and the consequences of publication for the data subject*".[450]

301. If this assessment revealed that the data subject did have a right for the information to be no longer linked with their name, the operator should grant the data subject's request for de-referencing. However, this would not be the case where the operator found that "*the inclusion of the link in question is strictly necessary for reconciling the data subject's rights to privacy and protection of personal data with the freedom of information of potentially interested internet users*"[451]. Interestingly, even in this scenario, the CJEU decided to impose an obligation on the operator to"*adjust the list of results on its search engine in such a way that the overall picture it gives the internet user reflects the current legal position (…)*", meaning that the web pages including the most up-to-date information should appear first.[452] The operator would be required to make such adjustment "*at the latest on the occasion of the request for de-referencing*".[453]

(d) *Territorial scope of the right to be forgotten*

302. In *Google*[454], another case brought before the CJEU following a request for de-referencing, the CJEU highlighted the territorial scope of the right to be forgotten. The CJEU was asked to clarify the territorial scope of the right to be forgotten on search engines (i.e. national, European or global); and particularly, whether the right to de-referencing has an extra-territorial effect outside the EU.

303. In this context, the CJEU started by reminding that "*the right to the protection of personal data is not an absolute right*" and that "*it must be balanced against other fundamental rights*", including the right to freedom of information of internet users. The CJEU further acknowl-

445 Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773, paragraph 69.
446 Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773, paragraph 57.
447 Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773, paragraph 59.
448 Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773, paragraph 66.
449 Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773, paragraph 69.
450 Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773, paragraph 77.
451 The necessity to balance out an individual's right to privacy (and more specifically, his or her right to be forgotten) against other fundamental rights, such as freedom of expression and freedom to access information, has also been highlighted by the ECtHR. See for instance, Judgment of the ECtHR of 28 June 2018, *M.L. and W.W. v. Germany*, ECLI:CE:ECHR:2018:0628JUD006079810).
452 Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773, paragraph 78.
453 Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773, paragraph 78.
454 Judgment of 24 September 2019, *Google*, C-507/17, ECLI:EU:C:2019:772.

edged that the balance between the right to privacy and to the protection of personal data on the one hand and other fundamental rights such as the right to freedom of information "*may vary significantly around the world*".[455]

304. According to the CJEU, there was no evidence that the EU legislator specifically intended for EU data protection rights to have an extra-territorial scope and thus to apply the same beyond the territorial limits of the EU.

305. According to the above considerations, the CJEU concluded that EU law did not impose any obligation on search engine operators to carry out a de-referencing on all the versions of their search engines (i.e. at a global level).

306. However, the CJEU stated that de-referencing should be carried out for all Member States as the EU legislator's intention, when adopting Regulation 2016/679, was clearly to ensure a consistent level of protection throughout all Member States. Therefore, the operator of a search engine could not limit the de-referencing only to the Member State in which the individual making the request was located but had to grant the request consistently across the entire European Union. The CJEU clarified that when required to carry out a de-referencing, search engine operators should take "*sufficiently effective measures*" to ensure the "*effective protection*" of the individual's fundamental rights. The CJEU did not provide any further details about such measures other than outlining that they must "*have the effect of preventing or, at the very least, seriously discouraging internet users in the Member States from gaining access to the links in question*".[456]

307. As a last comment on this territoriality issue, the CJEU mentioned that although EU law did not impose an obligation on search engine operators to grant any request for de-referencing at a global level, it did not "*prohibit such a practice*". Therefore, the CJEU left it to national supervisory or judicial authorities to assess whether, after weighing a data subject's right to privacy and the protection of personal data concerning them and the right to freedom of information "*in the light of national standards of protection of fundamental rights*", it would be appropriate to order the search engine operator to perform a de-referencing concerning all versions of that search engine.[457] This consideration derives from the acknowledgement that balance between the various fundamental rights at stake might indeed vary even from one Member State to another. The CJEU thus leaves the possibility for national authorities to require a global de-referencing on the basis of "*national standards of protection of fundamental rights*" even though such requirement for a global de-referencing could not be derived directly from EU law. In practice, however, this last comment from the CJEU raises some concerns as it might be expected to pose a challenge for the consistency of the application of the right to be forgotten throughout the EU.

3.3.6 *Right to restriction of processing*

308. Under Directive 95/46, Article 12(b) granted the data subject a right to obtain from the controller, inter alia, the "*blocking of data the processing of which does not comply with the provisions of* [Directive 95/46]*, in particular because of the incomplete or inaccurate nature of the data*". Under Regulation 2016/679, the wording has been changed so that this right to the blocking of data is now referred to as the right to 'restriction of processing'.

309. Unfortunately, there have not been many occasions for the CJEU to clarify how this right should apply in practice so far.

310. This right was briefly mentioned in *Rijkeboer* only for the CJEU to illustrate that "*the right of access is necessary to enable the data subject to exercise the rights set out in Article 12(b) and (c) of Directive 95/46*", including the right for the data subject to have the controller "*block his data*".[458]

311. In *Manni*, the CJEU also made a quick reference to the right to block personal data when it considered whether or not the authority responsible for keeping the companies register pursuant to EU laws should, after some time had elapsed following the dissolution of a company, limit the disclosure of personal data linked to this company. Following the same reasoning as the one under Section 3.3.5, the CJEU ruled that as a matter of principle, data subjects whose personal data was included in the companies register could not be guaranteed a right to obtain the blocking of that data from the public under Article 12(b) of Directive 95/46.[459]

3.3.7 *Notification obligations to recipients*

312. Under Directive 95/46, Article 12(c) stated that the data subject could require that the controller notify any third parties to whom the personal data have been disclosed of any rectification, erasure or blocking of data carried out in compliance with Article 12(b), "*unless this proves impossible or involves a disproportionate effort.*" A similar provision has been included in Regulation 2016/679 under Article 19.

455 Judgment of 24 September 2019, *Google*, C-507/17, ECLI:EU:C:2019:772, paragraph 60.
456 Judgment of 24 September 2019, *Google*, C-507/17, ECLI:EU:C:2019:772, paragraph 70.
457 Judgment of 24 September 2019, *Google*, C-507/17, ECLI:EU:C:2019:772, paragraph 72.
458 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 51. See also for a similar comment, Judgment of 20 December 2017, *Nowak*, C-434-16, ECLI:EU:C:2017:994, paragraph 57.
459 Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, paragraph 56.

313. In the context of the *Rijkeboer* case, the CJEU was asked to rule, inter alia, on the proportionality of the setting of a time limit to the right to access information for the recipients or categories of recipients of personal data.

314. This case prompted the CJEU to make a few comments regarding the controller's obligation to notify third parties to whom personal data have been disclosed in case the data subject requested that such data be rectified, erased or blocked.

315. Indeed, the CJEU recognised that the time limit set on the right to access information for the recipients of the data "*must allow the data subject to exercise the different rights laid down in the Directive*".[460] Such rights particularly included the right to have third parties to whom the data have been disclosed notified in the event of a rectification, erasure or blocking of the data.

316. However, the CJEU noted the following: "*Accordingly, Article 12(c) of the Directive expressly provides for an exception to the obligation on the controller to notify third parties to whom the data have been disclosed of any correction, erasure or blocking, namely, where this proves impossible or involves a disproportionate effort.*" Accordingly, considering that the obligation to keep the information on the recipients of the personal data for a long period "*could represent an excessive burden on the controller*", the CJEU determined that the Directive did not require such a burden to be imposed on the controller.[461]

317. On this last point, the CJEU did not clarify the situation that would enable a controller to leverage the exception provided in Article 12(c) of Directive 95/46 (i.e. when the notification obligation would *"prove impossible"* or be considered to *"involve a disproportionate effort"*).

318. Since Article 19 of Regulation 2016/679 still refers to the same exception that was included in Article 12(c) of Directive 95/46, the CJEU might have an opportunity to clarify this issue in the future.

3.3.8 *Right to object*

319. Article 14(a) of Directive 95/46 stated that a data subject should be granted the right "*to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him (…)*". It was clear from the Directive's wording that this right might not always be applicable. Article 14(a) stated that "*where there is a justified objection, the processing instigated by the controller may no longer involve those data*", thereby implying that the right to object to the processing should in fact only be binding on the controller "*where there is a justified objection*". However, a very strict interpretation did not seem in place either as Article 14(a) specified that this right should apply "*at least*" in the cases in which the processing was based on the public interest or on the legitimate interests pursued by the controller or by third parties.

320. The wording of Article 14(a) of Directive 95/46 evidently left room for interpretation, and the CJEU helped clarify the circumstances in which this right to object should apply.

321. First, in *Nowak*, the CJEU exemplified a situation in which a data subject would have a legitimate interest to object to a processing activity. Indeed, the CJEU found that "*an examination candidate has, inter alia, a legitimate interest, based on the protection of his private life, in being able to object to the processing of the answers submitted by him at that examination and of the examiner's comments with respect to those answers outside the examination procedure, and in particular, to their being sent to third parties, or published, without his permission.*"[462]

322. The CJEU also found that a data subject might rely on Article 14(a) of Directive 95/46 to object to the referencing of links to web pages containing personal data relating to them by a search engine.[463] In this regard, the CJEU clarified in *Google Spain and Google* that to assess whether the data subject's request should then actually be granted, "*it should in particular be examined whether the data subject has a right that the information relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name*".[464] More specifically, the CJEU explained that such examination was required to balance out the data subject's rights to privacy and protection of personal data on the one hand and other fundamental rights such as the internet users' right to information on the other. Where the data subjects' fundamental rights override the interest of the general public to access the information, the data subject would then indeed have a right to obtain the requested de-referencing.

323. In the context of requests for de-referencing, the CJEU held that "*as a general rule*", the data subject's rights would indeed override the public's right to information although the specific circumstances of a case could occasionally indicate otherwise.[465] The circumstances in *Google*

460 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 57.

461 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 61.

462 Judgment of 20 December 2017, *Nowak*, C-434-16, ECLI:EU:C:2017:994, paragraph 50.

463 See Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 98 and Judgment of 24 September 2019, *GC and Others*, C-136/17, ECLI:EU:C:2019:773, paragraph 51.

464 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 96.

465 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 97.

Spain and Google illustrated a situation in which the data subject's rights overrode the public's right to information. Indeed, the CJEU noted that the information in relation to which the data subject requested a de-referencing concerned facts that had taken place sixteen years earlier and that there did not appear to be *"particular reasons substantiating a preponderant interest of the public*" in having access to that information for a search made on the data subject's name. Consequently, the CJEU found that the data subject had a right to require the litigious links to be removed from the list of results displayed by the search engine.[466]

324. In *Manni*, the CJEU applied the same exercise of weighing the data subject's fundamental rights against the public's fundamental rights. However, the circumstances at hand were very different.[467] The CJEU seemed to consider that in that case, the third parties' right to access the information included in the companies register would most likely prevail over the data subject's rights to privacy and protection of personal data, particularly considering the need to "*protect the interests of third parties in relation to joint-stock companies and limited liability companies and to ensure legal certainty, fair trading and thus the proper functioning of the internal market take precedence*".[468] Nonetheless, the CJEU specified again that the result of the balancing exercise might have been different had the factual circumstances of the case been different. Therefore, the CJEU acknowledged that "*there may be specific situations in which the overriding and legitimate reasons relating to the specific case of the person concerned justify exceptionally that access to personal data entered in the register is limited, upon expiry of a sufficiently long period after the dissolution of the company in question, to third parties who can demonstrate a specific interest in their consultation*".[469]

325. In conclusion, the CJEU has clarified both in *Google Spain and Google* and in *Manni* that when receiving a data subject's objection to a given processing activity, the controller must weigh out the data subject's rights against the public's rights on a case-by-case basis to determine whether the data subject's request should be granted.

326. In *Manni*, the CJEU highlighted that national laws would also have to be taken into account in the context of that exercise, particularly to ensure that such national laws do not preclude the data subject to object to the processing at hand.[470]

327. Finally, the CJEU clarified in *Google Spain and Google* that when assessing whether a data subject's objection to a processing should be granted, it was not necessary to consider whether the processing had caused prejudice to the data subject.[471]

328. The EU legislature duly noted the CJEU's findings regarding the right to object to processing. Particularly, Article 21(1) of Regulation 2016/679 now explicitly refers to the balancing test detailed in particular in *Google Spain and Google* as it states that "[t]*he controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims*".

3.3.9 *Restrictions*

329. Under the conditions set out in Article 13 of Directive 95/46 and Article 23 of Regulation 2016/679, Member States are allowed to adopt restrictions to the data protection rights or obligations. The CJEU has played an important role to clarify how such exceptions should be understood and applied.

(a) *Article 13(1) of Directive 95/46*

330. The CJEU has interpreted the application of Article 13(1) of Directive 95/46 on multiple occasions. In *Puškár*, the CJEU outlined that any limitation imposed on a data subject's rights should be "*necessary for the protection of an interest referred to in Article 13(1), such as, inter alia, an important economic and financial interest in the field of taxation and be based on legislative measures*".[472] Thus, it was clarified that two conditions should be satisfied before a controller could rely on Article 13(1) of Directive 95/46.

(i) First condition: Measure necessary for the protection of an interest listed in Article 13(1)

331. Article 13(1) of Directive 95/46 contained seven 'interests' that could potentially justify the restriction of some of the obligations and rights laid down in Articles 6(1), 10, 11(1), 12 and 21 of Directive 95/46.

332. In *IPI*, the CJEU had the opportunity to shed some light on the application of Article 13(1) of Directive 95/46. This case arose as the Institut professionnel des agents immobiliers ("IPI"), a body responsible for ensuring compliance with the conditions of access to and the proper practice of the regulated profession of estate agent in Belgium, had requested a Belgian court to declare that some indi-

466 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 98.
467 See Section 3.3.5(b)(ii) above for a reminder of the facts underlying this case.
468 Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, paragraph 60.
469 Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, paragraph 60.
470 Judgment of 9 March 2017, *Manni*, C-398/15, ECLI:EU:C:2017:197, paragraph 61.
471 Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 96.
472 Judgment of 27 September 2017, *Puškár*, C-73/16, ECLI:EU:C:2017:725, paragraph 116.

viduals had infringed the rules of the profession based on facts gathered by private detectives. The Belgian court questioned the value to be given to such evidence as it had been obtained without respecting the obligation to inform data subjects set out in Directive 95/46.

333. First, the CJEU clarified that Article 13(1) of Directive 95/46 merely offered Member States the option to provide for one or more exceptions set out in this Article but did not compel them to do so.[473] Simultaneously, the CJEU also highlighted that the Member States could only provide for exceptions pursuant to Article 13(1) of Directive 95/46 if such measures were necessary. However, even where this condition of 'necessity' would be satisfied, Member States could still choose not to provide an exemption under their local law.[474] It is apparent from the wording of Article 23(1) of Regulation 2016/679[475] that this margin of manoeuvre granted to Member States still exists today.

334. Then, the CJEU had to rule on whether the activity of a private detective acting for a regulated body could fall within the scope of Article 13(1)(d) of Directive 95/46. As a reminder, this provision offered the possibility for Member States to implement exceptions, *inter alia*, to the duty to inform data subjects where they deemed it necessary to safeguard "*the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions*".

335. The CJEU concluded that the activity of a regulated body or of a private detective acting for a regulated body to investigate possible breaches of the rules of ethics of a regulated profession was covered by the exception in Article 13(1)(d) of Directive 95/46.

336. In *Ryneš*, the CJEU referred to the protection of the property, health and life of the controller and their family as an interest that was covered by Article 13(1)(d) and (g) of Directive 95/46.[476]

(ii) Second condition: Exception based on legislative measures

337. This condition was illustrated in *Bara and Others* in which the CJEU observed that "*Article 13 expressly requires that such restrictions are imposed by legislative measures*".[477] In the circumstances at hand, the national law did not specifically provide any exemption regarding the duty to inform data subjects from which the controller could have benefitted. The CJEU concluded that "*the conditions laid down in Article 13 of Directive 95/46 permitting a Member State to derogate from the rights and obligations*" flowing from Articles 10 and 11 of the Directive were not complied with.[478]

(iii) Additional requirement: Compatibility with the fundamental right to privacy

338. As already specified in Section 2 above, the CJEU has consistently considered that the provisions of Directive 95/46 should be interpreted with respect to fundamental rights.[479] This statement also applies in relation to Article 13 of Directive 95/46. In *Österreichischer Rundfunk and Others*, the CJEU clarified that where a national legislation is incompatible with Article 8 of the ECHR, "*that legislation is also incapable of satisfying the requirement of proportionality in Articles 6(1)(c) and 7(c) or (e) of Directive 95/46*". In this context, such legislation could not "*be covered by any of the exceptions referred to in Article 13 of that directive, which likewise requires compliance with the requirement of proportionality with respect to the public interest objective being pursued*".[480]

(b) *Incorporation of the CJEU findings in Regulation 2016/679*

339. The EU legislature has clearly taken into account the CJEU's case law when drafting Article 23(1) of Regulation 2016/679. Indeed, this provision now clarifies that any restriction to the rights granted to data subjects within Regulation 2016/679 "*respects the essence of the fundamental rights and freedoms*" and "*is a necessary and proportionate measure in a democratic society*". The CJEU applied these new elements of Article 23(1) of Regulation 2016/679 for the first time in *La Quadrature du Net*.[481] For a detailed analysis of this case, see Section 4 on E-privacy below.

473 Judgment of 7 November 2013, *IPI*, C-473/12, ECLI:EU:C:2013:715, paragraph 37.

474 Judgment of 7 November 2013, *IPI*, C-473/12, ECLI:EU:C:2013:715, paragraph 32.

475 Pursuant to Article 23(1) of Regulation 2016/679: "***Union or Member State law** to which the data controller or processor is subject may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 34, as well as Article 5 in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22 (…)*" (emphasis added).

476 Judgment of 11 December 2014, *Ryneš*, C-212/13, ECLI:EU:C:2014:2428, paragraph 34.

477 Judgment of 1st October 2015, *Bara and Others*, C-201/14, ECLI:EU:C:2015:638, paragraph 39 and paragraph 45.

478 Judgment of 1st October 2015, *Bara and Others*, C-201/14, ECLI:EU:C:2015:638, paragraph 41.

479 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, ECLI:EU:C:2003:294, paragraph 68; Judgment of 13 May 2014, *Google Spain and Google*, C-131/12, ECLI:EU:C:2014:317, paragraph 68; Judgment of 17 July 2014, *YS and Others*, C-141/12, ECLI:EU:C:2014:208, paragraph 54; Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 38 (with respect to the right to respect for private life).

480 Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, ECLI:EU:C:2003:294, paragraph 91.

481 Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraphs 207-212.

3.4 *Controller and processor*

3.4.1 *Joint controllers*

340. Article 26 of Regulation 2016/679 introduced a specific provision with regard to joint controllers which did not exist in Directive 95/46. The CJEU has not yet had to examine questions that specifically deal with this Article 26 of Regulation 2016/679. However, in the last few years, the CJEU has adopted three landmark rulings iregarding the concept of joint controllership which are analysed in Section 3.1.3(c) above.

3.4.2 *Data processor agreement*

341. In *Probst*, the CJEU held that Articles 16 and 17 of Directive 95/46[482] clarified that a processor may only act on the controller's instructions and "*that the controller must ensure compliance with the measures agreed in order to protect personal data against any form of unlawful processing*".[483]

3.4.3 *Records of processing activities*

342. Article 30 of Regulation 2016/679 introduced the obligation for controllers and processors to maintain a record of processing activities. This obligation essentially replaced the obligation to notify the supervisory authorities set out in Article 18 of Directive 95/46.

343. However, Article 18(2) of Directive 95/46 allowed Member States to provide the simplification or exemption from notification if a personal data protection official had been appointed who was notably responsible for "*keeping the register of processing operations carried out by the controller*".

344. In *Volker und Markus Schecke and Eifert*, the CJEU concluded that Article 18(2) of Directive 95/46 does not require the personal data protection official to keep the register before the processing activity is carried out.[484] It is unclear whether the CJEU's reasoning also applies to the obligation to keep a record for processing activities under Article 30 of Regulation 2016/679. In the absence of a specific obligation to draw up a record before a processing activity starts, one might argue that the CJEU's finding in *Volker und Markus Schecke and Eifert* still applies.

3.4.4 *Security of processing*

345. In *Rijkeboer* and in *Worten*, the CJEU recalled the principle laid down in Article 17 of Directive 95/46 without, however, clarifying as to what constitutes 'appropriate technical and organizational measures'.[485]

346. In *Worten,* the CJEU underlined that "*Article 17(1) of Directive 95/46 does not require Member States, except where they act as controllers, to adopt those technical and organisational measures, as the obligation to adopt such measures concerns solely the controller; namely, in the present case, the employer. Article 17(1) of Directive 95/46 does, however, require the Member States to adopt a provision in their national law providing for that obligation*".[486]

347. In the same decision, the CJEU also held that if access to personal data is authorised by national law, there is no accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, or any other unlawful form of processing.[487]

3.4.5 *Prior consultation*

348. Under Directive 95/46, the publication of personal data of beneficiaries of EU agricultural funds by national public authorities is not subject to the prior check requirement laid down in Article 20 of Directive 95/46 to the extent that this publication does not seem likely to present specific risks to the rights and freedoms of the data subjects. In this context, the CJEU notably based its decision on Recital 52 which favours an '*ex post facto*' verification by the supervisory authorities and Recital 54, which outlines that the number of processing activities that would require prior checking should be very limited.[488]

3.4.6 *Data protection officer*

349. Under Directive 95/46, the position of data protection officers (or 'data protection official', as it was referred to under the Directive) was not widespread. Only in *Volker und Markus Schecke and Eifert*, the CJEU briefly addressed this role by simply repeating that according to Article 18(2) of Directive 95/46, the personal data protection official's mission is to ensure that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.[489]

482 These two Articles are now covered by Article 28 of Regulation 2016/679, which has however become much more prescriptive.

483 Judgment of 22 November 2021, *Probst*, C-119/12; ECLI:EU:C:2012:748, paragraph 25.

484 Judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, joined cases C-92/09 and C-93/09, ECLI:EU:C:2010:662, paragraph 99.

485 Judgment of 7 May 2009, *Rijkeboer*, C-553/07, ECLI:EU:C:2009:293, paragraph 62 and Judgment of 30 May 2013, *Worten,* C-342/12, ECLI:EU:C:2013:355, paragraph 24.

486 Judgment of 30 May 2013, *Worten,* C-342/12, ECLI:EU:C:2013:355, paragraph 25.

487 Judgment of 30 May 2013, *Worten,* C-342/12, ECLI:EU:C:2013:355, paragraphs 26.

488 Judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, joined cases C-92/09 and C-93/09, ECLI:EU:C:2010:662, paragraphs 102-108.

489 Judgment of 9 November 2010, *Volker und Markus Schecke and Eifert*, joined cases C-92/09 and C-93/09, ECLI:EU:C:2010:662, paragraph 98.

3.5 *International data transfers*

3.5.1 *General*

350. Neither Directive 95/46 nor Regulation 2016/679 precisely defines international transfers of personal.

351. In *Lindqvist*[490], the referring court enquired whether the uploading of personal data onto an internet page, thereby making the data accessible to anyone who connects to the internet including people in a third country, constituted a 'transfer of personal data to a third country' within the meaning of Article 25 of Directive 95/46.

352. Analysing the objective of Chapter IV of Directive 95/46 and considering the state of the internet at the time Directive 95/46 was drawn up, the CJEU argued that "*one cannot presume that the Community legislature intended the expression 'transfer* [of data] *to a third country' to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them*".[491] According to the CJEU, a different interpretation would mean that "*every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all third countries where there are the technical means needed to access the internet*".[492] This would imply implies that either the European Commission has to adopt adequacy decisions for all countries in which the internet can be accessed or, in the absence hereof, that no personal data may be uploaded on the internet. The CJEU therefore concluded that the uploading of personal data onto a webpage does not qualify as a transfer of data to a third country.

3.5.2 *Adequacy decisions*

(a) *General*

353. The landmark decisions concerning international data transfers, and perhaps data protection in general, are obviously *Schrems*[493] and *Facebook Ireland and Schrems*[494].

354. Both decisions dealt with the mechanism of 'adequacy decisions' laid down in Articles 25(6) of Directive 95/46 and 45 of Regulation 2016/679.

(b) *The notion of 'adequate protection'*

355. Article 25(1) of Directive 95/46 prohibited transfers of personal data to a third country that did not ensure an adequate level of protection. In *Schrems,* the CJEU underlined that the word 'adequate' does not require the level of protection in a third country to be identical to that guaranteed in the EU.[495] Following the observation of Advocate General Bot, the CJEU stated that it should be understood as "*requiring the third country (…) to ensure (…) a level of protection of fundamental rights and freedoms that is essentially equivalent to that guaranteed within the European Union by virtue of Directive 95/46 read in the light of the Charter*".[496] Recital 104 of Regulation 2016/679 now expressly refers to the requirement of 'essential equivalence' in the context of adequacy decisions.

356. The CJEU also noted that the European Commission is required to periodically check whether the adequacy of the level of protection is still factually and legally justified.[497] Unlike Directive 95/46, Article 45(3) and (4) of Regulation 2016/679 now expressly obliges the European Commission to conduct such periodic reviews.

(c) *Adequacy and self-certification mechanisms*

357. In *Schrems*, the CJEU ruled that recourse by a third country to a system of self-certification, such as the Safe Harbour or Privacy Shield, is not in itself contrary to the requirement laid down in Article 25(6) of Directive 95/46. However, the CJEU also added that "*the reliability of such a system (…) is founded essentially on the establishment of effective detection and supervision mechanisms enabling any infringements of the rules ensuring the protection of fundamental rights (…) to be identified and punished in practice*".[498]

358. In this context, the CJEU noted that the Safe Harbour adequacy decision "*laid down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations (…) are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them.*"[499] That is, the adequacy decision established an interference with fundamental rights. Furthermore, in *Facebook Ireland and Schrems,* the

490 Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596.
491 Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraphs 64-68.
492 Judgment of 6 November 2003, *Lindqvist*, C-101/01, ECLI:EU:C:2003:596, paragraphs 69.
493 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650.
494 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/118, ECLI:EU:C:2020:559.
495 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 73.
496 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 73. Opinion of 23 September 2015, *Schrems,* C-362/14, ECLI:EU:C:2015:627, paragraph 141. See also, Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/118, ECLI:EU:C:2020:559, paragraph 94. See also See also Recommendations 02/2020 of the EDPB on the European Essential Guarantees for surveillance measures, 10 November 2020 and Recommendations 01/2020 of the EDPB on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 November 2020, version for public consultation.
497 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 76.
498 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 81.
499 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 86.

CJEU came to the same finding regarding the Privacy Shield adequacy decision.[500]

359. In *Schrems,* the CJEU indicated that the adequacy decision did not specify the rules that were to be adopted by the United States to limit that interference nor did it refer to the existence of effective legal protection against such interference. Moreover, the CJEU noted that the European Commission itself, in the meantime, had ascertained that the access rights of United States authorities "*went beyond what was strictly necessary and proportionate to the protection of national security*".[501] For these reasons, the CJEU concluded that the adequacy decision failed to comply with the requirements of Article 25(6) of Directive 95/46. Therefore, the adequacy decision was invalidated.

360. In *Facebook Ireland and Schrems,* the adequacy decision contained a detailed analysis of US surveillance laws pursuant to which the European Commission had concluded that the interference was limited to what was strictly necessary to achieve the legitimate objective of national security.[502] However, based on a detailed analysis of the relevant United States' legal provisions, the CJEU concluded that US surveillance laws did not provide a level of protection that was essentially equivalent. Therefore, the adequacy decision could not be reconciled with Article 45(1) of Regulation 2016/679 read in the light of considering Articles 7, 8 and 47 of the Charter, as a result of which the CJEU invalidated it as well.

3.5.3 *Standard Contractual Clauses*

(a) *The notion of 'appropriate safeguards'*

361. Recital 108 of Regulation 2016/679 states that the 'appropriate safeguards' aim at compensating for the lack of data protection in a third country. Both Advocate General Saugmandsgaard Øe and the Grand Chamber deducted therefrom that *"such appropriate guarantees must be capable of ensuring that data subjects whose personal data are transferred to a third country (…) are afforded (…) a level of protection essentially equivalent to that which is guaranteed within the European Union.*"[503]

362. Furthermore, the CJEU recalled that the adequacy of the level of protection must be assessed in light of Article 46(2)(c) of Regulation 2016/679, which states that data subjects must be afforded appropriate safeguards, enforceable rights and effective legal remedies. Additionally, both the contractual clauses agreed between the data exporter and the data importer must be considered along with the legal system of the third country with regard to access by its public authorities to the personal data transferred.[504]

(b) *Supplementary measures*

363. Having conducted a detailed assessment of the standard contractual clauses, the CJEU concluded that generally, in light of Articles 7, 8 and 47 of the Charter, the validity of the European Commission's decision regarding the standard contractual clauses was not affected.

364. However, referring to Recital 109 of Regulation 2016/679, the CJEU ruled that the data exporter is required "*to verify, on a case-by-case basis and where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred*".[505] This implies that the data exporter and the data importer are *"required to verify, prior to any transfer, whether the level of protection required by EU law is respected in the third country concerned*".[506]

365. Where such adequate protection cannot be guaranteed, the data exporter might be required to adopt "*supplementary measures*" to ensure compliance with the level of protection required under EU law.[507] Unfortunately, the CJEU has provided no indication of what could constitute acceptable supplementary measures. In its FAQ on this judgment, the EDPB stated that "*the supplementary measures you could envisage where necessary would have to be provided on a case-by-case basis, taking into account all the circumstances of the transfer and following the assessment of the law of the third country, in order to check if it ensures an adequate level of protection. (…) The EDPB is currently analysing the Court's judgment to determine the kind of supplementary measures that could be provided in addition to SCCs or BCRs, whether legal, technical or organizational measures*".[508] Based on this analysis, it has published two draft Recommendations that, once adopted, should assist with the assessment of what constitutes supplementary measures.[509]

500 See also Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/118, ECLI:EU:C:2020:559, paragraph 164.

501 Judgment of 6 October 2015, *Schrems*, C-362/14, ECLI:EU:C:2015:650, paragraph 90.

502 The CJEU analysed the Foreign Intelligence Surveillance Act (FISA), and more specifically its Article 702, Executive Order 12333 (E.O 12333) and Presidential Policy 28 (PPD-28).

503 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/118, ECLI:EU:C:2020:559, paragraph 96, Opinion of 19 December 2019, *Facebook Ireland and Schrems*, C-311/118, ECLI:EU:C:2019:1145, paragraph 115.

504 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/118, ECLI:EU:C:2020:559, paragraph 102-105.

505 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/118, ECLI:EU:C:2020:559, paragraphs 133-134.

506 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/118, ECLI:EU:C:2020:559, paragraph 142.

507 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/118, ECLI:EU:C:2020:559, paragraph 133.

508 Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, EDPB, 23 July 2020, page 5.

509 Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, EDPB, 10 November 2020, version for public consultation; Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, EDPB, 10 November 2020.

3.6 *Independent supervisory authorities*

3.6.1 *The principle of complete independence*

366. The right to independent supervision by a data protection authority derives from the primary law of the European Union, *inter alia* Article 8(3) of the Charter and Article 16(2) TFEU.[510] As such, it is an essential element of the protection accorded to data subjects under EU data protection law.

367. The guarantee of independence of national supervisory authorities was established in Article 28(1) second subparagraph of Directive 95/46, which states that the supervisory authorities "*shall act with complete independence in exercising the functions entrusted to them*".[511] The CJEU has interpreted this requirement in several decisions. In doing so, it has issued judgments on state (or 'Länder') law[512], national law[513] and national constitutional law[514].

368. The CJEU proposes an autonomous interpretation of this guarantee of independence.[515] In *Commission v Germany*, it interpreted Article 28(1) second subparagraph of Directive 95/46 considering its purpose, the actual wording of the provision, as well as the aim and scheme of Directive 95/46.[516]

369. The aim of the guarantee of independence of supervisory authorities is, as the CJEU clarifies, "*to ensure the effectiveness and reliability of the supervision of compliance with the provisions on personal data protection*".[517] It is an essential component of the protection of individuals regarding to the processing of their personal data. To guarantee this protection, national supervisory authorities are entrusted with the specific task of ensuring a fair balance between observance of the fundamental right to privacy on the one hand and the interests requiring free movement of personal data on the other.[518] Most importantly, the independence of supervisory authorities is not a goal in and of itself. Rather, it serves the purpose of strengthening the protection of individuals and bodies that are affected by their decisions.

370. The autonomous interpretation of 'independence' under Article 28(1) second subparagraph of Directive 95/46 also means that it must be viewed separately from the concept of 'independence' as is required for a judicial body to qualify as a court or tribunal of a Member State under Article 267 TFEU. In *Commission v Austria*, the CJEU held that satisfying the standard of independence for judicial courts under Article 267 TFEU does not imply that the condition of 'with complete independence' as per Article 28(1) second subparagraph of Directive 95/46 is satisfied.[519] Interestingly, in his opinion on *Commission v Germany*, Advocate General Mazák had already argued that independence must not be interpreted with respect to the case law of the CJEU concerning the independence of the courts. Supervisory authorities are administrative structures and on account of this, they belong to the sphere of the executive – and not the judiciary where another standard definition of 'independence' applies.[520] The CJEU followed this reasoning in *Commission v Austria*.

3.6.2 *Independence from any external influence*

371. In their role as guardians of the right to private life as the CJEU describes it, the supervisory authorities must act objectively and impartially.[521] To do so, they must remain free from any external influence, direct or indirect, which could call into question their performance of tasks under the Directive.[522]

372. Throughout its case law, the CJEU has provided guidance regarding whose influence the supervisory authorities must avoid to be regarded as 'completely independent'. They must remain free from the influence of the bodies that are subject to their supervision.[523] Furthermore, as became clear in *Commission v Germany*,[524] *Com-*

510 Article 8(3) of the Charter stipulates: "*Compliance with these rules shall be subject to control by an independent authority.*"; Article 16(2) TFEU stipulates: "*The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities.*" (emphasis added)

511 Today, this is set out in Article 52 of Regulation 2016/670. Most of the findings of the CJEU as explained in this section have been codified into Regulation 2016/679.

512 Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125.

513 Judgment of 16 October 2012, *Commission v Austria,* C-614/10, ECLI:EU:C:2012:631.

514 Judgment of 8 April 2014, *Commission v Hungary*, C-288/12, ECLI:EU:C:2014:237.

515 Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, paragraphs 17 and 29.

516 Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125.

517 Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, paragraph 25.

518 See Judgment of 9 March, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, paragraph 24; Judgment of 8 April 2014, C-288/12, *Commission v Hungary*, C-288/12, ECLI:EU:C:2014:237, paragraph 51.

519 Judgment of 16 October 2012, C-614/10, *Commission v Austria,* C-614/10, ECLI:EU:C:2012:631, paragraphs 39-40.

520 See in that regard Opinion of 22 October 2009, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, paragraph 14.

521 Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, paragraph 23.

522 Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, paragraphs 25 and 30. This reasoning is now expressly included in Article 52(2) of Regulation 2016/679, which reads as follows: "*The member or members of each supervisory authority shall, in the performance of their tasks and exercise of their powers in accordance with this Regulation, remain free from external influence, whether direct or indirect, and shall neither seek nor take instructions from anybody.*"

523 Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, paragraph 19.

524 Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, paragraph 36.

mission v Austria[525] and *Commission v Hungary*,[526] they must also remain free from any direct or indirect influence from the state.[527]

373. Finally, in *Wirtschaftsakademie Schleswig-Holstein*, the CJEU found that supervisory authorities of one Member State shall be able to perform their tasks independently of supervisory authorities of other Member States that might also be competent to deal with a given case in their Member State.[528] In this regard, the CJEU stated that "[a] *supervisory authority which is competent under its national law is (…) not obliged to adopt the conclusion reached by another supervisory authority in an analogous situation*".[529]

3.6.3 *Independence and adequacy decisions*

374. Even though supervisory authorities cannot adopt measures contrary to an adequacy decision until the CJEU invalidates the latter, such a decision cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) of the Charter and Article 28 of Directive 95/46 or Article 58 of Regulation 2016/679.[530]

3.6.4 *The standard of independence*

375. In *Commission v Germany,* the CJEU held that the mere risk that a scrutinising authority could exercise a political influence over the supervisory authority's decisions is incompatible with the requirement of complete independence from the supervisory authorities.[531] First, according to the CJEU, this could lead to "*'prior compliance' on the part of the supervisory authorities in the light of the scrutinising authority's decision-making practice*"[532] – i.e. the supervisory authority might adopt decisions, which it believes will be according to what the scrutinizing authority would expect. Second, in their roles of guardians of the right to private life, "*it is necessary that their decisions, and therefore the authorities themselves, remain above any suspicion of partiality*".[533] In that regard, the CJEU held that operational independence of the supervisory authorities, in the sense of not being bound by instructions of any kind in the performance of their duties, is not sufficient in itself to protect supervisory authorities from all external influence.[534] Indeed, as became clear in *Commission v Austria,* an organisational overlap between the supervisory authority and government authorities could also prevent the supervisory authority from being above all suspicion of partiality.[535]

376. In this context, Advocate General Mazák suggested that the fact that the duties of members are only a part-time activity which is concurrent with other professional activities might also result in an external influence over the members' work. Pursuant to Article 44(3) of Regulation 45/2001[536], members of the European Data Protection Supervisor are prohibited from engaging in any other occupation during their term. The CJEU did not go so far as to rule out the possibility of a part-time activity as members of a supervisory authority, as is the case for members of the European Data Protection Supervisor. Rather, it refrained from expressing its opinion on the matter. As per Article 52(3) of Regulation 2016/679, members of the supervisory authorities can engage in other (part-time) occupations, so long those are not incompatible with their duties.[537]

377. Interestingly, Advocate General Mazák initially adopted a more relaxed approach to state supervision. In *Commission v Germany,* he stated that whether supervisory authorities can perform their functions in complete independence when under state supervision depends on what that state supervision entails. According to the Advocate General, if the oversight is designed, and limited to what is necessary, "*to establish whether the monitoring carried out by the supervisory authority is rational, lawful*

525 Judgment of 16 October 2012, C-614/10, *Commission v Austria,* C-614/10, ECLI:EU:C:2012:631, paragraph 59.

526 Judgment of 8 April 2014, C-288/12, *Commission v Hungary*, C-288/121, ECLI:EU:C:2014:237, paragraph 53.

527 Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, paragraph 25. This includes influence from the 'government', as the government might itself be an interested party and neglect the data protection law 'in order to fulfil certain of its other functions, in particular for taxation or law enforcement purposes. See in this regard also Judgment of 9 March 2010, *Commission v Germany*, C-518-17, ECLI:EU:C:2010:125, paragraph 35.

528 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein,* C-210/16, ECLI:EU:C:2018:388, paragraphs 68-70. Regulation 2016/679 introduced a mechanism whereby supervisory authorities must cooperate with each other and, where relevant, with the Commission to ensure the consistent application of that regulation.

529 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein,* C-210/16, ECLI:EU:C:2018:388, paragraph 70. See also Section 3.7 below, which examines cooperation and consistency in more detail.

530 Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/118, ECLI:EU:C:2020:559, paragraphs 118-120 and 156-157.

531 Judgment of, 16 October 2012, *Commission v Austria,* C-614/10, ECLI:EU:C:2012:631, paragraphs 36 and 52.

532 Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, paragraph 36; Judgment of 16 October 2012, *Commission v Austria*, C-614/10, ECLI:EU:C:2012:631, paragraph 51; Judgment of 8 April 2014, *Commission v Hungary*, C-288/12, ECLI:EU:C:2014:237, paragraph 53.

533 Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, paragraph 36; Judgment of 16 October 2012, *Commission v Austria*, C-614/10, ECLI:EU:C:2012:631, paragraph 52; Judgment of 8 April 2014, *Commission v Hungary*, C-288/12, ECLI:EU:C:2014:237, paragraph 53.

534 Judgment of 8 April 2014, C-288/12, *Commission v Hungary*, ECLI:EU:C:2014:237, paragraph 52.

535 In *Commission v Austria*, some staff members of the supervisory authority were under direct supervision of the Federal Chancellor. Moreover, under Austrian law, the Federal Chancellor had the right to be informed at all times on all aspects of the work of the supervisory authority. The CJEU considered this incompatible with the criterion of independence as set forward in Article 28(1) of Directive 95/46.

536 Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data [2000] OJ L008.

537 Opinion of 3 July 2012, *Commission v Austria,* C-614/10, ECLI:EU:C:2012:406, paragraph 33.

and proportionate", such supervision does not hinder the supervisory authority in exercising their functions with complete independence.[538] The CJEU did not follow that line of reasoning. Instead it concluded that the "*mere risk*" of state scrutiny is sufficient to determine a lack of complete independence.[539]

3.6.5 *Independence and budgetary constraints*

378. In *Commission v Austria*, the CJEU clarified that 'complete independence' does not mean that Member States should give their national supervisory authorities a separate budget.[540] Member states can still provide that, from the point of view of budgetary law, the supervisory authorities are to come under a specified ministerial department. However, a case-by-case analysis remains necessary to determine whether the attribution of the necessary equipment and staff to such authorities does not prevent them from acting 'with complete independence'.[541] This reasoning has now expressly been included in Article 52(6) of Regulation 2016/679, which reads: "*Each Member State shall ensure that each supervisory authority is subject to financial control which does not affect its independence and that it has separate, public annual budgets, which may be part of the overall state or national budget.*"

3.6.6 *Independence versus the supervisory authority's term of office*

379. In *Commission v Hungary*, the CJEU ruled that the requirement of complete independence must necessarily be construed "*as covering the obligation to allow supervisory authorities to serve their full term of office*".[542] In this case, the supervisory authority's office was reformed during the term of the then appointed Supervisor. This reform caused the Supervisor to vacate the office before the expiry of the legally set term. The CJEU recognized that Member States have a measure of discretion with regard to choosing the institutional model of their supervisory authority, which includes the duration of the supervisory authority's term of office.[543] However, once that term has been set, it must be respected. The supervisory authority cannot be compelled to vacate the office before the expiry of that term, except for overriding and objectively verifiable reasons. The CJEU reasoned that "*if Member States were allowed to compel a supervisory authority to vacate office before serving its full term, in contravention of the rules and safeguards established in the applicable law, the threat of such premature termination could lead the supervisory authority to enter into a form of 'prior compliance' with the political authority*".[544] This, the CJEU ruled, is incompatible with the requirement of independence. This finding holds true, "*even where the premature termination of the term served comes about as a result of the restructuring or changing of the institutional model, which must be organised in such a way as to meet the requirement of independence laid down in the applicable legislation*".[545]

3.7 ***Cooperation and consistency***

3.7.1 *Cooperation*

380. In an interconnected world, cross-border processing of personal data is common. In such cases of cross-border processing, it is important that the right to privacy of individuals is still protected effectively and completely.

381. In that setting, Regulation 2016/679 sets out an elaborate scheme to ensure cooperation and consistency between the supervisory authorities.[546] Directive 95/46, however, only addressed the topic of cooperation, in brief terms under its Article 28(6).[547]

382. Article 28(6) of Directive 95/46 determined that each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with Article 28(3).[548]

383. This article further dictated that each authority may be requested by an authority of another Member State to exercise its powers, and that the supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

384. The CJEU has interpreted Article 28(6) of Directive 95/46 for the first time in *Weltimmo*.[549] Here, the CJEU clarified that this duty of cooperation serves to ensure the free flow of personal data, whilst ensuring the compliance with the rules protecting the privacy of individuals. The cooperation between supervisory authorities is all the

538 Opinion of 22 October 2009, *Commission v Germany*, C-518/07, ECLI:EU:C:2009:694, paragraph 30.

539 Judgment of 9 March 2010, *Commission v Germany*, C-518/07, ECLI:EU:C:2010:125, paragraph 36.

540 Judgment of 16 October 2012, *Commission v Austria*, C-614/10, ECLI:EU:C:2012:631, paragraph 58.

541 Judgment of 16 October 2012, C-614/10, *Commission v Austria,* C-614/10, ECLI:EU:C:2012:631, paragraph 58.

542 Judgment of 8 April 2014, Commission v Hungary, C-288/12, ECLI:EU:C:2014:237, paragraph 55.

543 In this regard, it is worth noting that under Article 54(1)(d) of Regulation 2016/679, Member States now have less discretion to decide on the supervisory authority's term of office. Article 54(1)(d) of Regulation 2016/679 states the following: "*the duration of the term of the member or members of each supervisory authority of no less than four years, except for the first appointment after 24 May 2016, part of which may take place for a shorter period where that is necessary to protect the independence of the supervisory authority by means of a staggered appointment procedure*".

544 Judgment of 8 April 2014, *Commission v Hungary*, C-288/12, ECLI:EU:C:2014:237, paragraph 53.

545 Judgment of 8 April 2014, *Commission v Hungary*, C-288/12, ECLI:EU:C:2014:237, paragraph 54.

546 See Chapter VII of Regulation 2016/679.

547 See Section I of Chapter VII of Regulation 2016/679.

548 Article 28(3) of Directive 95/46 requires that each authority has investigatory powers, effective powers of intervention and the power to engage in legal proceedings.

549 Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639.

more relevant in cross-border data protection cases where a controller that is established in one Member State infringes the right to personal data protection in another Member State without having an establishment in the latter Member State.[550] Without the cooperation mechanism, it would be difficult for the supervisory authority to which a complaint has been submitted to enforce the right to data protection if the controller is established in another Member State.

385. As we have seen under Section 3.1.2, the national law applicable to such a controller in respect of that processing were the laws of the country where the controller had its establishment. The CJEU found in *Weltimmo*, that a national supervisory authority to which a complaint had been submitted "*may examine that complaint, irrespective of the applicable national law*".[551] What is more, it was allowed to examine that complaint before even knowing which national law was applicable to the processing in question.[552]

386. However, the CJEU continued, if said authority reached the conclusion that the law of another Member State applied, "*it cannot impose penalties outside the territory of its own Member State*".[553] In such a situation, it had to comply with its duty of cooperation under Article 28(6) of Directive 95/46. This implied that the supervisory authority to which the complaint had been addressed had to request the supervisory authority of that other Member State to establish the infringement and to impose a sanction. Such sanction could be based on the information which the authority of the first Member State had.[554]

3.7.2 *Consistency*

387. In *Wirtschaftsakademie Schleswig-Holstein*,[555] the CJEU found that there is no duty of consistency imposed on supervisory authorities in relation to each other's findings. According to the CJEU, Directive 95/46 does not lay down any criterion of priority governing the intervention of one supervisory authority against another, nor does it lay down an obligation for a supervisory authority of one Member State to comply with a position which may have been expressed by the supervisory authority of another Member State. Therefore, "[a] *supervisory authority which is competent under its national law is (…) not obliged to adopt the conclusion reached by another supervisory authority in an analogous situation*".[556] Although the position of the CJEU made sense from a legal perspective, it obviously did not contribute to a consistent application of data protection law across the EU.

388. Under Regulation 2016/679, Articles 63 and following have introduced a new consistency mechanism that aims at avoiding an inconsistent application of Regulation 2016/679 by the supervisory authorities.[557] At the time of publishing, the new cooperation and consistency mechanism installed by Regulation 2016/679 is the subject of a pending request for a preliminary ruling before the CJEU.[558] In this case, *Facebook Ireland and Others*, the referring court essentially asked whether the one-stop-shop mechanism impedes a supervisory authority of a Member State from bringing judicial proceedings before a court of that state for an infringement with respect to cross-border data processing if that authority is not the lead supervisory authority. Advocate General Bobek contends that the lead supervisory authority has a general competence over cross-border processing. By implication, supervisory authorities concerned[559] enjoy a limited power to act in exceptional cases only.[560] The CJEU has not yet adjudicated on the matter. It remains to be seen whether it will follow the Advocate General's opinion.

3.8 ***Remedies, liability and penalties***

3.8.1 *Right to an effective judicial remedy*

389. In *Rijkeboer*, the CJEU underlined the importance of the right to access for the obtainment of an effective judicial remedy.[561]

550 Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, paragraph 53.
551 Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, paragraph 54.
552 Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, paragraphs 54 and 57.
553 Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, paragraph 57.
554 Judgment of 1 October 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639, paragraph 57
555 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein,* C-210/16, ECLI:EU:C:2018:388.
556 Judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein,* C-210/16, ECLI:EU:C:2018:388, paragraph 70. In this case, the CJEU ruled that the German supervisory authority was competent in respect of data processing where the controller was established in another Member State (Ireland) and the establishment in Germany was responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State (Facebook Germany).
557 See in this regard, Judgment of 16 July 2020, *Facebook Ireland and Schrems*, C-311/118, ECLI:EU:C:2020:559, paragraph 147.
558 Request for a preliminary ruling of 30 August 2019, *Facebook Ireland and Others*, C-645/19.
559 The 'supervisory authority concerned' is defined under Article 4(22) of Regulation 2016/679 as "*a supervisory authority which is concerned by the processing of personal data because: (a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority.*"
560 Opinion of 13 January 2021, *Facebook Ireland and Others*, C-645/19, ECLI:EU:C:2021:5, paragraph 43. The Advocate General identified five scenarios in which the supervisory authority concerned would be allowed to act: where a supervisory authority (i) actsoutside the material scope of the GDPR;(ii) acts in the context of cross-border data processing carried out by public authorities, in the public interest, in the exercise of official authority (iii) acts in the context of cross-border data processing carried out by controllers not established in the European Union; (iv) adopts urgent measures; or (v) intervenes where the lead data protection authority has decided not to handle a case.
561 Judgment of 7 May 2009, *College van burgemeesters en wethouders van Rotterdam v M.E.E. Rijkeboer*, C-533/07, ECLI:EU:C:2009:293, paragraphs 51-53.

3.8.2 *Representation of data subjects*

390. In *Fashion ID*[562], the CJEU was questioned on the validity of national legislation providing for the right for consumer protection associations to bring or defend legal proceedings against a person who allegedly infringed data protection law.

391. In its decision, the CJEU took into account Articles 22, 28(4) and 28(3), third indent of Directive 95/46. Pursuant to Article 22 of the Directive, every person should have a right to judicial remedy for any breach of the national provisions implementing Directive 95/46. Secondly, national supervisory authorities are authorised to hear claims from associations representing data subjects under Article 28(4) of the directive. Pursuant to Article 28(3) third indent of Directive 95/46, supervisory authorities also have the power to bring a violation of national data protection law – from which they may have heard through such a claim – to the attention of the legal authorities.[563]

392. On this basis, the CJEU concluded that there is no provision in Directive 95/46 that requires Member States to provide a right to associations to represent data subjects in legal proceedings or commence legal proceedings on their own initiative against a person who allegedly infringed data protection law. That being said, the CJEU ruled that such a recourse is a 'suitable measure', in the sense of its Article 24, to achieve the objectives pursued by Directive 95/46. It therefore concluded that national provisions allowing such actions are valid under the Directive.[564]

393. It is worth noting that, at the time of publication, a request for a preliminary ruling is pending before the CJEU on the interpretation of Articles 80(1) and (2), as well as Article 84(1) of Regulation 2016/679.[565] More specifically, the German Federal Court of Justice has asked the CJEU whether competitors and associations are entitled to bring proceedings for breaches of Regulation 2016/679, independently of the infringements of specific rights of individual data subjects and without being mandated to do so by a data subject, when national law provides for such rights.[566]

562 Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629.

563 Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraphs 44-48.

564 Judgment of 29 July 2019, *Fashion ID*, C-40/17, ECLI:EU:C:2019:629, paragraphs 51 and 59.

565 Request for preliminary ruling of 15 July 2020, *Facebook Ireland*, C-319/20.

566 The request for a preliminary ruling pertains to proceedings brought before civil courts on the basis of the prohibition of unfair commercial practices or breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions.

3.9 ***Provisions relating to specific processing situations***

3.9.1 *General*

394. Several specific processing situations are regulated differently under Regulation 2016/679. Member States can enact certain exemptions to general principles under the regulation to the extent necessary to reconcile the conflicting underlying interests.

395. Similarly, Article 9 of Directive 95/46 required that Member States provide for exemptions or derogations from some of the obligations under the Directive "*for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression*".[567] These exemptions or derogations were to apply "*only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression*".

3.9.2 *Processing solely for journalistic purposes*

(a) *Scope*

396. In two cases, the CJEU was requested to adjudicate on whether a specific processing operation could be considered as conducted *'solely for journalistic purposes'*.[568] The two cases called for the balancing of the right to personal data protection versus the right to freedom of expression. In both cases, the CJEU refrained from actually conducting the balancing test on the facts of the individual cases, as this is a prerogative reserved to the Member States. Nevertheless, the CJEU provided useful pointers for the referring courts to conduct the balancing test themselves.

397. The CJEU ruled that the system which is established by Article 9 of the Directive is one of reconciliation of two fundamental rights: the Member States must provide a number of derogations and exemptions to the fundamental right to privacy for some specific data processing operations that fall within the scope of the fundamental right to freedom of expression.[569]

398. The CJEU stated that, in order to take account of the importance of the right to freedom of expression in every democratic society, the notions relating to this freedom, such as 'journalism', must be interpreted broadly.[570]

567 Article 9 of Directive 95/46 reads as follows: "*Member States shall provide for exemptions or derogations from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression*".

568 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727; Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122.

569 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraphs 52-55.

570 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraph 56.

On the other hand, to achieve a balance between the two fundamental rights, any derogations and limitations to the right to data protection must only apply insofar as strictly necessary.[571] The reasoning of the CJEU was included, almost *ad verbatim*, in Recital 153 *in fine* of Regulation 2016/679.

399. When conducting the balancing test and assessing the necessity of the derogations and limitations to the protection of personal data, the CJEU indicated that the case law of the ECtHR contains a number of relevant criteria.[572] These criteria include the contribution to a debate of public interest, the degree of notoriety of the person affected, the subject of the news report, the prior conduct of the person concerned, the content, form and consequences of the publication, the manner and circumstances in which the information was obtained and its veracity.[573] Similarly, the CJEU mentioned that "*the possibility for the controller to adopt measures to mitigate the extent of the interference with the right to privacy must be taken into account*".[574]

(b) *Meaning of 'journalism'*

400. The CJEU further set out a list of criteria to be taken into account when interpreting 'journalism' under Article 9 of Directive 95/46. Firstly, 'journalism' under Article 9 of the Directive is not reserved to media undertakings. The notion extends to every person engaged in journalism.[575]

401. Secondly, the pursuit of profit with a publication does not impede such a publication from being considered as an activity undertaken 'for solely journalistic purposes'.[576]

402. Thirdly, "*the medium which is used to transmit the processed data, whether it be classic in nature, such as paper or radio waves, or electronic, such as the internet, is not determinative as to whether an activity is undertaken 'solely for journalistic purposes'*".[577] In *Buivids*, the CJEU confirmed its position on the methods of communication and dissemination of information, reiterating that this is not relevant for assessing whether an activity is undertaken 'solely for journalistic purposes'.[578] However, the CJEU added, not all information published on the internet involving personal data falls under the scope of 'journalistic activities' under Article 9 of Directive 95/46.[579]

403. In the end, what matters to the CJEU is whether the sole object of the activity is the disclosure to the public of information, opinions or ideas.[580]

(c) *Examples*

404. In *Satakunnan Markkinapörssi*[581], the CJEU examined a request for a preliminary ruling concerning the activities of two Finnish media undertakings who published tax data of approximately 1.2 million data subjects and made these available against payment via a mobile text-messaging service. The CJEU ruled that for these activities to fall under the exemptions and derogations of Article 9 of Directive 95/46, those activities had to becarried out *solely* for the purpose of the disclosure to the public of information, opinions or ideas. Whether that was the case, the CJEU left for the referring court to decide.

405. It is worth noting that, following the CJEU's ruling, the Finish Data Protection Board issued a prohibition on the media outlets to continue publishing the tax data. Both media outlets challenged this prohibition and the case was eventually brought before the ECtHR.[582] The two media outlets relied on the exception provided for journalistic activities by the Finnish data protection law to justify their data processing operations. The ECtHR found that the prohibition imposed by the Finnish supervisory authority from publishing personal tax data did not violate the right to freedom of expression and information. According to the ECtHR, the Finish Data Protection Board had struck the right balance between the right to privacy and the right to freedom of expression. Moreover, the ECtHR found that the mass collection and wholesale dissemination of taxation data had not contributed to a debate of

571 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraph 56; Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122, paragraph 64.

572 Article 7 and 11 of the Charter correspond to Articles 8(1) and 10 ECHR, respectively. In accordance with Article 52(3) of the Charter, these rights under the Charter have to be given the same meaning and scope as the rights under the ECHR, as interpreted by the case law of the European Court of Human Rights.

573 See judgment of the ECtHR of 27 June 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, CE:ECHR:2017:0627JUD000093113, paragraph 165.

574 Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122, paragraph 66.

575 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraph 58.

576 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraph 59.

577 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727, paragraph 60

578 Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122, paragraph 57.

579 Judgment of 14 February 2019, *Buivids*, C-345/17, ECLI:EU:C:2019:122, paragraph 58; Opinion of 27 September 2018, *Buivids*, C-345/17, ECLI:EU:C:2018:780, paragraph 55.

580 The Advocate General states that the dissemination of personal data pursues journalistic purposes if it aims to impart information and ideas on matters of public interest. See Opinion of 8 May 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:266, paragraph 68. The CJEU, however, did not include this additional criterion in its interpretation of 'journalistic purposes'. The reasons why it has not done so were already provided by the Advocate General, namely that one cannot determine in advance what information relates to the public interest. See in this regard Opinion of 8 May 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:266, paragraph 78.

581 Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C-73/07, ECLI:EU:C:2008:727.

582 Judgment of the ECtHR of 27 June 2017, *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland*, CE:ECHR:2017:0627JUD000093113.

public interest and had not been for a solely journalistic purpose.

406. In the second CJEU case on this topic, *Buivids*, the CJEU was requested to clarify whether the recording, in a police station, of police officers carrying out procedural measures, and the subsequent publishing of the video on *YouTube* constituted processing of personal data for journalistic purposes.

407. The CJEU ruled that these processing activities "*may constitute a processing of personal data solely for journalistic purposes, within the meaning of that provision, in so far as it is apparent from that video that the sole object of that recording and publication thereof is the disclosure of information, opinions or ideas to the public*".[583] When assessing whether this is the case, the national court may take into account the fact that the video in question appeared to have been published to draw the attention of society to alleged police malpractice. The establishment of such malpractice is, however, not a condition for the applicability of Article 9 of Directive 95/46.[584]

4. E-privacy

4.1 *Introduction*

408. Directive 2002/58 deals with the processing of personal data *"in connection with the provision of publicly available electronic communications services in public communications networks (…)*" (Art. 3 of Directive 2002/58).

409. In several cases, the CJEU has recalled the objective of Directive 2002/58, which is to protect users of electronic communications services with regard to the processing of their personal data.[585]

410. It is therefore not surprizing that most requests for a preliminary ruling deal with the confidentiality of communications and the related traffic data.[586] To be more precise, the questions intend to get an understanding of the situations in which electronic communication service providers are authorised to retain such data and/or grant access to such data, either at the request of law enforcement agencies[587] or in the context of civil proceedings.[588]

411. In recent years, the CJEU has also been requested to respond to other e-privacy related questions, notably regarding the use of cookies (Art. 5(3) of Directive 2002/58).

4.2 *Material scope*

4.2.1 *General rule*

412. Contrary to Directive 95/46 and Regulation 2016/679, Directive 2002/58 does not clearly set out its scope in a single article.

413. Article 1(1) of Directive 2002/58, which is entitled 'Scope and Aim', states that Directive 2002/58 "*provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms (…) with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community*".

414. The actual scope is however defined in Article 3 ('Services concerned'): "*This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices*".

415. With regard to the application of the material scope of Directive 2002/58, the CJEU has only clarified that it applies to providers of electronic communications services in the sense of Article 2(c) of Directive 2002/21.[589]

583 Judgment of 14 February 2019, *Buivids,* C-345/17, ECLI:EU:C:2019:122, paragraph 69.

584 Judgment of 14 February 2019, *Buivids,* C-345/17, ECLI:EU:C:2019:122, paragraphs 60-61. In this regard, Advocate General Sharpston emphasized that there may be particular circumstances where the only way investigative journalism can uncover serious wrongdoings is by having recourse to some kind of covert operation. Such circumstances, however, will nevertheless require careful scrutiny to see whether an appropriate balance between competing fundamental rights can be struck. See Opinion of 27 September 2018, *Buivids*, C-345/17, ECLI:EU:C:2018:780, paragraph 72.

585 Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 106. Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraphs 82-83; Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraph 34.

586 Traffic data is defined in Article 2 (b) of Directive 2002/58 as "*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*". See also Recital 15 of Directive 2002/58 for examples of what constitutes traffic data.

587 See Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970; Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788; Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790.

588 See Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54; Order of 19 February 2009, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, C-557/07, ECLI:EU:C:2009:107; Judgment of 24 November 2011, *Scarlet Extended*, C-70/10, ECLI:EU:C:2011:771; Judgment of 19 April 2012, *Bonnier Audio and Others*, C-461/10, ECLI:EU:C:2012:219.

589 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 70, Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraph 33. See also Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive) [2002] OJ L108; in the meantime replaced by Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code [2018] OJ L321.

4.2.2 *Exception – activities outside the scope of EU law*

416. The CJEU has had the opportunity to clarify the scope of the exception laid down in Article 1(3) of Directive 2002/58 in several cases.[590]

417. This Article contains an exception which is quite similar to the one laid down in Article 3(2) of Directive 95/46 and Article 2(2)(a) and (b) of Regulation 2016/679.[591] Are excluded from its scope, activities which fall outside the scope of EU law, and especially "*activities concerning public security, defence, State security (including the economic well-being of the State, when the activities relate to State security matters) and the activities of the State in areas of criminal law*".[592] According to the settled case law of the CJEU, these activities are "*in any event, activities of the State or of State authorities and are unrelated to fields in which individuals are active*".[593]

418. The CJEU has ruled that legislative measures requiring providers of electronic communications services to retain personal data or to grant competent national authorities access to those data, "*necessarily involve the processing of personal data by those providers*". As such, these measures relate to fields in which individuals – as opposed to public authorities – are active. It is the settled case law of the CJEU that "[s]*uch measures, to the extent that they regulate the activities of electronic communications service providers, cannot be regarded as activities characteristic of states, referred to in Article 1(3) of Directive 2002/58*".[594]

419. On the other hand, legislative measures that derogate from the principle of confidentiality of communications, "*without imposing processing obligations on providers of electronic communications services*", do not fall under the scope of Directive 2002/58.[595] In that case, only national law applies, subject to the application of Directive 2016/680.[596] In his Opinion in *La Quadrature du Net,* Advocate General Campos Sánchez-Bordona had taken the same view: "[t]*he provisions of* [Directive 2002/58] *will not apply to activities which are intended to safeguard national security and are undertaken by the public authorities themselves, without requiring the cooperation of private individuals and, therefore, without imposing on them obligations in the management of businesses*".[597]

420. In *La Quadrature du Net* and *Privacy International*, the CJEU furthermore clarified that in interpreting Article 1(3) of Directive 2002/58, one must make the distinction as to who carries out the data processing operation concerned.[598] The CJEU stated this to differentiate between the exceptions in Article 1(3) of Directive 2002/58 and in Article 3(2) of Directive 95/46. In *Parliament v Council and Commission,*[599] the CJEU had previously ruled that the processing of passenger data by airlines, consisting of the collection and subsequent transfer to public authorities of a third country, for the purpose of fighting terrorism and serious crime fell under the exception of Article 3(2) of Directive 95/46. That exception excluded 'processing activities relating to state security', which anyone can carry out (i.e. also commercial undertakings).[600] In *La Quadrature du Net* and *Privacy International,* the CJEU stressed however that this interpretation cannot be applied to Article 1(3) of Directive 2002/58, which is phrased in a way that only the 'activities related to state security' are excluded from the Directive's scope. The CJEU followed Advocate General Campos Sánchez-Bordona's view that these activities "*cannot be carried out by anyone, but only by the State itself*".[601] It is worth noting that Regulation 2016/679, which has in the meantime replaced and repealed Directive 95/46, does contain a distinction as to who carries out a

590 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970; Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788; Judgment of 6 October 2020 , *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791; Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790.

591 See Section 3.1.1(b) above.

592 Article 1(3) of Directive 2002/58. See also Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 69.

593 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 69, Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraph 32; Judgment of 6 October 2020 , *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 92; Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraph 48.

594 Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraph 37. See also Judgment of 21 December 2016, *Tele2 Sverige*, Joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraphs 75-76; Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 96; Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraph 39.

595 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 101 and Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraph 48.

596 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA [2016] OJ 2016 L 119.

597 Opinion of 15 January 2020, *La Quadrature du Net and Others*, joined cases C-511/18 and C-512/18, ECLI:EU:C:2020:6, paragraphs 78-79.

598 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 101; Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraph 46.

599 Judgment of 30 May 2006, *Parliament v Council and Commission*, C-317/04 and C-318/04, ECLI:EU:C:2006:346.

600 Opinion of 13 January 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:6, paragraph 70.

601 Opinion of 13 January 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:6, paragraph 72.

processing operation concerned for the determination of its scope.[602]

4.3 *Definitions*

4.3.1 *Definitions of general data protection law*

421. In *Promusicae* and *Bonnier Audio and Others,* the CJEU recalled that as per the first paragraph of Article 2 of Directive 2002/58, the definitions of Directive 95/46 also apply, unless they are expressly derogated from.[603] Consequently, the terms 'personal data' and 'processing' have the meaning as set out in Directive 95/46.

422. Similarly, when interpreting the phrase 'acting under the authority of providers of the public communications services', the CJEU indicated that account had to be given to Articles 16 and 17 of Directive 95/46, which clarify *"the level of control that the controller must exercise over the processor which it appoints"*. Accordingly, 'acting under the authority of providers of the public communications services' must be interpreted as *"acting only on the controller's instructions"* and where the controller *"ensures compliance with the measures agreed in order to protect personal data against any form of unlawful processing"*.[604]

4.3.2 *Traffic data*

423. Traffic data consists of '*any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof*' (Art. 2 (b) of Directive 2002/58).[605] They may also consist of the format in which the communication is conveyed by the network. In *Ministerio Fiscal*,the CJEU clarified that the notion of traffic data covers data relating to the identity of owners of SIM cards, such as surnames, forenames and addresses.[606]

4.4 *Confidentiality of the communications*

4.4.1 *General principle*

424. The principle of confidentiality of both communications and the related traffic data is enshrined in Article 5(1) of Directive 2002/58 and is complemented by its Articles 6 and 9(1). In *Tele2 Sverige,* the CJEU underlined that the scope of Articles 5, 6 and 9(1) of Directive 2002/58 "*must be assessed in the light of recital 30 of that directive, which states: 'Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum'*".[607]

425. As the CJEU recalled, pursuant to Article 5(1) of Directive 2002/58, "*any person other than the users is prohibited from storing, without the consent of the users concerned*,[the communications and] *the traffic data related to electronic communications*".[608] In *La Quadrature du Net*, the CJEU highlighted that this principle "*gave concrete expression to the rights enshrined in Articles 7 and 8 of the Charter, so that the users of electronic communications services are entitled to expect, in principle, that their communications and data relating thereto will remain anonymous and may not be recorded, unless they have agreed otherwise*".[609] This prohibition on the interception of communications and traffic data "*therefore encompasses any instance of providers of electronic communications services making traffic data and location data available to public authorities (…), as well as the retention of that data by those authorities (…)*".[610] Such activities are therefore only authorised if and to the extent, they meet the requirements of the restrictions laid down in Article 15(1) of Directive 2002/58.

426. In *Tele2 Sverige*, the CJEU clarified that "[t]*he only exceptions relate to persons lawfully authorised in accordance with Article 15(1) of that directive and to the technical storage necessary for conveyance of a communication*".[611] Furthermore,the CJEU indicated that Article 5(1) applies

602 See in that regard Articles 2(2)(d) and 23(1)(d) and (h) of Regulation 2016/679. See also Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 102 and judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraph 47.

603 Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, paragraph 45 and Judgment of 19 April 2012, *Bonnier Audio and Others*, C-461/10, ECLI:EU:C:2012:219, paragraph 52.

604 Judgment of 22 November 2012, *Probst*, C-119/12, ECLI:EU:C:2012:748, paragraphs 24-25.

605 Recital 15 of Directive 2002/58 specifies that traffic data may, *inter alia*, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection.

606 Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraph 42. The CJEU seems to have gone against the position that the EU legislature had taken in Directive 2006/24, where 'data necessary to identify the subscriber or user' was listed as data that relates to traffic without being traffic data as such. See Art. 2(2)(a) of Directive 2006/24.

607 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 87.

608 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 85; Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 107.

609 Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 109. Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraphs 53-57.

610 Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraphs 55-56.

611 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 85. See also Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, paragraph 47.

to the measures taken by all other persons than users, "*whether private persons or bodies or State bodies*".[612]

4.4.2 *Traffic data*

427. Article 6 of Directive 2002/58 lays down specific obligations in relation to traffic data that complement the general principle of its Article 5(1). Under Article 6(1) of Directive 2002/58, traffic data must, in principle, be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. However, the processing of traffic data is permitted for the billing and marketing of electronic communications services and the provision of value added services subject to the conditions laid down in Article 6(2)-(5) of Directive 2002/58.[613]

428. In *Promusicae*, the CJEU recalled that the exceptions covered by Article 6(2)-(5) of Directive 2002/58 "*do not concern the communication of that data to persons other than those acting under the authority of the provider (…)*". Put differently, these provisions do not authorise the communication of that data to interested third parties who wish to use it in civil proceedings against the subscriber or user, nor to public authorities.[614]

429. Specifically with regard to the processing of traffic data for billing purposes, the CJEU clarified in *Probst* that the authorisation not only extends to the actual billing of the services but also to the debt collection: "*By authorising traffic data processing 'up to the end of the period during which the bill may lawfully be challenged or payment pursued', that provision relates not only to data processing at the time of billing but also to the processing necessary for securing payment thereof*".[615] Bearing this in mind, a service provider is authorised to communicate traffic data to a factoring service provider to which it assigned his claim for the sole purpose of the recovery of the debts, provided that the factoring service provider acts under its authority.[616]

430. Finally, pursuant to Article 6(6) of Directive 2002/58, traffic data may be communicated to competent bodies 'with a view of settling disputes, in particular interconnection or billing disputes'. In *Promusicae*, the CJEU specified that these disputes only relate to those between suppliers and subscribers or users. This Article therefore does not authorise the communication of traffic data to a right holder who wishes to bring civil proceedings against a user for copyright infringements.[617]

4.4.3 *Location data other than traffic data*

431. Location data, other than traffic data, is protected under Article 9 of Directive 2002/58. Such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.[618]

4.5 ***Application of certain provisions of Directive 95/46/EC***

4.5.1 *General principle*

432. Member States are allowed to introduce exceptions to the obligation of principle that communications must be kept confidential.[619] More specifically, pursuant to Article 15(1) of Directive 2002/58, Member States may introduce legislative measures restricting the scope of the above principle when such restriction constitutes a necessary measure 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*'."

433. The objectives of these measures substantially overlap with the ones referred to in Article 1(3) of Directive 2002/58, which contains the exclusions from the material scope of that Directive.[620] However, according to the settled case law of the CJEU, this overlap does not "*permit the conclusion that the legislative measures referred to in Article 15(1) of directive 2002/58 are excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose*".[621] The CJEU added that Article

612 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 77. As confirmed in recital 21 of Directive 2002/58, the aim of the Directive is to prevent unauthorised access to communications, including 'any data related to such communications', in order to protect the confidentiality of electronic communications.

613 Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, paragraph 47; Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 86; Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 108.

614 Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, paragraph 48; judgment of 22 November 2012, *Probst*, C-119/12, C-119/12, ECLI:C:2912:748, paragraph 18.

615 Judgment of 22 November 2012, *Probst*, C-119/12, C-119/12, ECLI:C:2912:748, paragraph 17; Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 86.

616 Judgment of 22 November 2012, *Probst*, C-119/12, C-119/12, ECLI:C:2912:748, paragraph 18.

617 Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, paragraph 48.

618 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 86; Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 108.

619 See Articles 5(1), 6 and 9(1) of Directive 2002/58. Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, paragraph 49; Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 88.

620 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 72.

621 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 73; Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, paragraphs 97-98; Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraphs 42-43. See also Opinion of 13 January 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:6, paragraph 75; Opinion of 15 January 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:5, paragraph 24.

15(1) of Directive 2002/58 "*necessarily presupposes that the national measures referred to therein (…) fall within the scope of that directive, since it expressly authorises the Member States to adopt them only if the conditions laid down in the directive are met*".[622] In *Privacy International*, the CJEU concluded that "[t]*he concept of 'activities' referred to in Article 1(3) of Directive 2002/58 cannot therefore (…), be interpreted as covering the legislative measures referred to in Article 15(1) of that directive*".[623]
Furthermore, the CJEU observed that the legislative measures referred to in Article 15(1) of Directive 2002/58 govern the activities of providers of electronic communications services and not those of public authorities as such. Therefore, when read together with Article 3 of Directive 2002/58, the CJEU concluded that legislative measures requiring providers of electronic communications services to retain traffic data and location data fall within the material scope of Directive 2002/58. Similarly, legislative measures relating to the access by national authorities to the data retained by the providers of electronic communications services equally fall within the material scope of the directive.[624]

434. The restrictions mentioned above must also constitute '*a necessary, appropriate and proportionate measure within a democratic society*'to safeguard the interests listed under Article 15(1).

435. According to the settled case law of the CJEU, these restrictions must be interpreted strictly. Article 15(1) of Directive 2002/58 "*cannot (…) permit the exception to that obligation of principle* [that communications and traffic data are confidential] *and, in particular, to the prohibition on storage of data (…) to become the rule*".[625] The list of objectives in Article 15(1) of Directive 2002/58 for which Member States can lay down laws derogating from the principle of confidentiality of communications and traffic data relating thereto is exhaustive. Accordingly, Member States cannot lay down measures referred to in Article 15(1) for other purposes than those listed in that provision.[626] To support this interpretation, the CJEU pointed out the second sentence of Article 15(1) according to which the legislative measures must be justified on "*the grounds laid down*" in the first sentence of that provision.[627]

436. With regard to the requirement of proportionality, the CJEU highlighted that the domestic legislation laying down the measures that create the interference must contain clear and precise rules with regard to the scope and application of the measure. Furthermore, the domestic legislation must impose minimum safeguards to ensure that the data is effectively protected against the risk of abuse. According to the CJEU, "[t]*he need for such safeguards is all the greater where personal data is subjected to automated processing, particularly where there is a significant risk of unlawful access to that data*".[628]

437. The CJEU has been asked to clarify the scope of this exception in multiple cases. Approximately half of them related to the retention of traffic data for objectives of general interest, such as the fight against crime or terrorism.[629] These cases were heavily influenced by the *Digital Rights Ireland and Others* judgment, in which the CJEU invalidated Directive 2016/24.[630] The other half related to interested third parties requesting access to traffic data in the context of civil proceedings against a user, typically in relation to copyright infringements.[631]

4.5.2 *Objectives of general interest*

(a) *Introduction*

438. In view of safeguarding national security, public security and combating (serious) crime, many Member States have adopted national legislation that obliges providers of electronic communications services to retain traffic and location data of all subscribers and users for a certain period of time. Even after the CJEU invalidated Di-

622 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraphs 72-73.

623 Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraph 43; Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:791, paragraph 98; Opinion of 13 January 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, ECLI:EU:C:2020:6, paragraph 75; Opinion of 15 January 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:5, paragraph 24.

624 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraphs 74-81.

625 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 89; Judgment of 22 November 2012, *Probst*, C-119/12, ECLI:EU:C:2021:748, paragraph 23. Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 111; Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraph 59.

626 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 90; Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 111.

627 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 90.

628 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 132. See also Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 68.

629 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970; Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788; Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790.

630 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238.

631 Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54; Order of 19 February 2009, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, C-557/07, ECLI:EU:C:2009:107; Judgment of 24 November 2011, *Scarlet Extended*, C-70/10, ECLI:EU:C:2011:771; Judgment of 19 April 2012, *Bonnier Audio and Others*, C-461/10, ECLI:EU:C:2012:219.

rective 2016/24[632], several cases were referred in which the CJEU was asked to assess the compatibility of national data retention provisions with Article 15(1) of Directive 2002/58.

439. The CJEU conducted this assessment on the basis of the criteria laid down in Article 52(1) of the Charter. For a detailed analysis of these criteria, we refer to Sections 2.7 and 5.

440. It is settled case law of the CJEU that the obligation to retain traffic and location data constitutes in itself an interference with Articles 7 and 8 of the Charter.[633] In this context, it is irrelevant whether the retained data has been used subsequently.[634] Moreover, according to the CJEU, the data that is typically to be retained "*is liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them*".[635] The interference is therefore "*very far-reaching and must be considered to be particularly serious*" even if such legislation does not permit the retention of the communications as such, and only the traffic data and location data.[636]

(b) *Serious crime and serious threats to public security*

441. In *Tele2 Sverige*, when examining the notion of 'crime', the CJEU concluded that only the general interest objective of combating 'serious' crime, as opposed to 'non-serious' crime, is capable of justifying a general and indiscriminate retention of all traffic and location data of all subscribers and users; considering its serious interference with fundamental rights.[637] The same goes for the right of access by public authorities to such retained data.[638] Similarly, only the general interest objective of preventing 'serious' threats to public security is capable of justifying this kind of measure.[639]

442. Although the objectives of combating serious crime and safeguarding public security are lawful objectives of general interest, the CJEU ruled that Article 15(1) of Directive 2002/58 precludes national legislation that imposes a general and indiscriminate retention obligation for these objectives.[640]

443. However, according to the CJEU, Article 15(1) of Directive 2002/58 does not prevent targeted data retention *"as a preventive measure, (…), for the purpose of fighting serious crime* [and preventing serious threats to public security]*, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary"*.[641] Notwithstanding the foregoing, the CJEU added that "[i]*n order to satisfy the requirement of proportionality, the legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards*" to protect the data against the risk of abuse.[642]

444. In *La Quadrature du Net*, the CJEU specified that these measures must ensure that the targeted retention is based "*on objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion*". Moreover, they must be limited in time to what is strictly necessary, it being understood that they may be extended.[643]

445. In *Tele2 Sverige,* the CJEU had previously indicated that the access by public authorities to the data retained must be based on objective criteria and, as a general rule, be subject to prior review by a court or an independent administrative authority. In addition, the public authorities must notify the individuals affected *"as soon as that notification is no longer liable to jeopardise the investigations being undertaken*". The CJEU specifically un-

632 See Section 5 below.

633 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraphs 32-37; Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 115; Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 71.

634 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 116.

635 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraphs 98-99. See also Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraphs 26-27; Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 117.

636 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraphs 100-101. See also Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 37; Opinion of 12 December 2013, *Digital Rights Ireland and Others*, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2013:845, paragraphs 77-80.

637 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 102.

638 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 115.

639 Judgment of 6 October, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraphs 140.

640 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraph 112; Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraphs 140-141.

641 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraphs 108; Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 147.

642 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 132.

643 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraphs 148-151. See also Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraphs 110-111.

derlined that national law must require the data to be retained within the EU and to be irreversibly destructed at the end of the data retention period.[644]

(c) *Non-serious crime and non-serious threats to public security*

446. In *Ministerio Fiscal*, the CJEU was asked whether Article 15(1) of Directive 2002/58 allows the access by public authorities to traffic data for the purpose of identifying the owner of SIM cards activated with a stolen mobile phone, in light of the fact that such theft does not constitute 'serious crime'. Reiterating that the list of objectives set out in Article 15(1) of Directive 2002/58 is exhaustive, the CJEU noted that this Article refers to 'criminal offences' generally, without requiring these to be 'serious'.[645]

447. The CJEU then confirmed that only the purpose of combating 'serious crime' justifies access by public authorities to traffic and location data which, "*taken as a whole, allow precise conclusions to be drawn concerning the private lives of the persons whose data is concerned*", since this results in a serious interference with Articles 7 and 8 of the Charter. However, when the interference is not serious, such access may be justified when the purpose relates to 'criminal offences' generally.[646] On this basis, the CJEU ruled that Article 15(1) of Directive 2002/58 does not preclude access by public authorities to traffic data for the purpose of identifying the owner of SIM cards activated with a stolen mobile phone. This interference is not to be considered 'serious' since it does not provide any information on the communications and the private lives of such users.[647]

(d) *National security*

448. In *La Quadrature du Net* and in *Privacy International*, the CJEU also recognised that national security constitutes a lawful objective of general interest, adding that it is "*capable of justifying measures entailing more serious interferences with fundamental rights*" than those which might be justified by the other objectives set out in Article 15(1) of Directive 2002/58.[648]

449. Therefore, the CJEU concluded that Article 15(1) of Directive 2002/58 does not, in principle, preclude the retention of traffic and location data of all users of electronic communications systems, for a limited period of time, "*as long as there are sufficiently solid ground for considering that the Member State concerned is confronted with a serious threat (…) to national security which is shown to be genuine and present or foreseeable*".[649]

450. Similarly, the CJEU stated that the automated analysis of traffic and location data of all users of electronic communication systems may be justified in the context of a serious threat to national security, "*which is shown to be genuine and present or foreseeable, and provided that the retention is limited to what is strictly necessary*".[650] This implies notably that the criteria of the automated analysis may not be based on special categories of personal data in isolation (e.g. racial, ethnical, political, religious data, etc.).[651] Furthermore, the CJEU held that any positive outcome obtained on the basis of the automated analysis must be subject to human oversight before additional measures are adopted that may adversely affect the individual concerned.[652]

451. Also, the CJEU took the view that real-time collection of technical data concerning the location of terminal equipment and of traffic and location data may be justified for the purpose of preventing terrorism, but only with regard to individuals about whom there is a valid reason to suspect that they are involved in terrorist activities. People falling outside of that category may only be the subject of non-real-time access.[653]

452. Considering the seriousness of these interferences, the CJEU indicated that such measures must be subject to "*effective review, either by a court or by an independent administrative body whose decision is binding*". The task of such court or body is to verify the existence of a genuine, present or foreseeable threat to national security and the observance of the conditions and safeguards put in place.[654]

453. The CJEU added that the duration of each preventive retention measure cannot exceed a foreseeable period

644 Judgment of 21 December 2016, *Tele2 Sverige*, joined cases C-203/15 and C-698/15, ECLI:EU:C:2016:970, paragraphs 118-123.

645 Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraph 53. See also Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraphs 157-158.

646 Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraphs 53-57. See also Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 140.

647 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 157. National security

648 Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 136; Judgment of 6 October 2020, *Privacy International*, C-623/17, ECLI:EU:C:2020:790, paragraph 75.

649 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 137.

650 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 177.

651 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraphs 180-181.

652 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 182.

653 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 188.

654 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraphs 139, 179 and 189.

of time, it being understood that such measures can be renewed on the basis of the ongoing nature of a threat.[655]

454. Finally, the CJEU ruled that authorities that engage in real-time collection of traffic and location data must notify the individuals concerned "*as soon as that notification is no longer liable to jeopardise the tasks for which those authorities are responsible*". The purpose of this notification is to allow the individuals concerned to exercise their rights under Article 7 and 8 of the Charter and, where relevant, to avail themselves of an effective remedy before a competent court in accordance with Article 47 of the Charter.[656]

455. With regard to the automated analysis of traffic and location data, the CJEU took the view that the authorities are not obliged to notify the individuals concerned individually. It suffices to publish information of a general nature about the way in which the automated analysis is set up. However, if the data analysed matches the parameters defined by the authority, as a result of which the authority decides to identify the individual, then that individual must be notified individually.[657]

(e) *Expedited retention – Serious crime and national security*

456. In *La Quadrature du Net,* the CJEU decided that the retention of traffic and location data may also be justified to shed light on serious criminal offences or acts adversely affecting national security, "*where those offences or acts (…) have already been established and where, after an objective examination of all of the relevant circumstances, such offences or acts (…) may reasonably be suspected*".[658]

457. Such expedited retention must be limited in time and must be limited to that traffic and location data that may shed light on the serious crime offence or acts adversely affecting national security. The CJEU clarified however, that this does not necessarily imply the expedited retention to be limited to the suspect. The expedited retention may be extended to other persons, "*provided that that data can, on the basis of objective and non-discriminatory factors, shed light on such an offence or acts adversely affecting national security*". The measure might therefore also apply to the victim, his or her social or professional circle or even to specified geographical areas.[659]

458. To avoid function creep, the CJEU stressed that the data retained must not be used for the purpose of prosecuting and punishing an ordinary criminal offence. However, data retained for the objective of combating serious crime may subsequently be used for the objective of safeguarding national security, and vice versa, if the required substantive and procedural measures have been met.[660]

4.5.3 *Civil proceedings*

459. The CJEU has also developed a body of case law on the exceptions authorised by Article 15(1) of Directive 2002/58 in the context of civil proceedings.

460. It first had to determine whether Article 15(1) of Directive 2002/58 allowed Member States to restrict the scope of the confidentiality of communications in this context. This question was debated because the exhaustive list of exceptions in Article 15(1) of Directive 2002/58 does not expressly refer to the bringing of civil proceedings. It does however include a reference to Article 13(1) of Directive 95/46. That Article allows restrictions, which are necessary to safeguard 'the protection (…) of the rights and freedoms of others'.

461. According to Advocate General Kokott, the grounds mentioned in Article 13(1) of Directive 95/46 are applicable to the electronic communications sector only insofar as they are expressly included in Article 15(1) of Directive 2002/58. As the protection of the rights and freedoms of others under Article 13(1)(g) of Directive 95/46 is not in that list, the Advocate General took the view that traffic data cannot be communicated in the context of civil proceedings.[661]

462. Interestingly, the CJEU ruled differently. It pointed out that Article 15(1) 2002/58 ends the list of exceptions to the principle of confidentiality with an express reference to Article 13(1) of Directive 95/46. As the 'other' rights and freedoms covered by that exception are not specified, the CJEU concluded that "*Article 15(1) must be interpreted as expressing the Community legislature's intention not to exclude from their scope the protection of the right to property or situations in which authors seek to obtain that protection in civil proceedings*".[662] In *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, the CJEU confirmed that Article 15(1) of Directive 2002/58 allowed measures aimed at protecting "*the right to proper-*

655 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 138.
656 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 190.
657 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraph 191.
658 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraphs 160-161.
659 Judgment of 6 October 2020, *La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraphs 164-165.
660 Judgment of 6 October 2020, *La Quadrature du Net and Others*, Joined cases C-511/18, C-512/18 and 520/18, ECLI:EU:C:2020:791, paragraphs 166 and 176.
661 Opinion of 18 July 2007, *Promusicae*, C-275/06, EU:C:2007:454, paragraphs 86-88.
662 Judgment of 29 January 2008, *Promusicae*, C-275/06, ECLI:EU:C:2008:54, paragraph 53; Order of 19 February 2009, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, C-557/07, ECLI:EU:C:2009:107, paragraph 26.

ty or situations in which authors seek to obtain that protection through civil proceedings".[663]

463. The CJEU therefore concluded that Article 15(1) of Directive 2002/58 does not preclude Member States to lay down an obligation to communicate personal data in the context of civil proceedings. However, the CJEU also ruled that this provision does not compel Member States to lay down such an obligation either.[664]

464. Should Member States decide to lay down such an obligation, according to the CJEU, they should ensure to strike "*a fair balance (…) between the various fundamental rights involved*". Moreover, Member States would have to make sure that their implementation of EU directives into national laws would not "*conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality*".[665]

465. With regard hereto, in *Scarlet Extended*, the CJEU decided that a court order requiring an internet service provider to install a continuous and indiscriminate filtering system in view of preventing the sharing of copyright protected works via a peer-to-peer file sharing network, did not respect the requirement that a fair balance be struck between the right to intellectual property and the right to protection of personal data.[666]

466. *BonnierAudio and Others* dealt with a request by a copyright holder to receive from the internet service provider the identity of the individual allegedly engaged in illegal file exchanges. The CJEU ruled that national legislation allowing a court to order such disclosure is likely to ensure a fair balance between the rights involved if the court is required to weigh the conflicting interests involved on a case-by-case basis, taking due account of the requirements of the principle of proportionality.[667]

4.6 *Directories of subscribers*

467. Directories and directory enquiry services were considered as an essential access tool for publicly available telephone services under the Universal Service Directive.[668] As such, they formed part of its universal services obligation. These directories of subscribers, which can be on paper or electronic, are populated with the help of undertakings assigning telephone numbers of end-users. To that end, under the Universal Service Directive, the latter were – and still are today under the European Electronic Communications Code – required to make data of end-users available to providers of directory enquiry services and directories on terms that are "*fair, objective, cost oriented and non-discriminatory*".[669]

468. Article 12 of Directive 2002/58 ensures, inter alia, subscribers' right to privacy with regard to the inclusion of their personal information in a public directory. Under Article 12(1) of Directive 2002/58, subscribers have a right to be informed, before they are included in a directory, about the purpose(s) of public directories in which their personal data are to be included, "*and of any further usage possibilities based on search functions embedded in electronic versions of the directory*". Article 12(2) of Directive 2002/58, grants subscribers the opportunity "*to determine whether their personal data are published in a directory and if so, which*". In addition, Article 12(3) stipulates that Member States may require that, for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other identifiers, additional consent be asked of the subscribers.

469. In two cases, the CJEU has taken a closer look at the consent requirements under Article 12 of Directive 2002/58.

470. In *Deutsche Telekom*,[670] the first case on this topic, the CJEU was asked to clarify whether consent (or a lack of objection) must be obtained for passing on data to a provider of publicly available directory enquiry services and directories where that data relates not to the disclosing provider's own subscribers, but rather, to subscribers of a third-party undertaking. In essence, the CJEU decided that the consent given by a subscriber not only relates to the publication in the initial directory but also extends to any subsequent processing for the purpose of publishing the data in other directories. The CJEU did clarify, however, that subscribers must be informed before the first inclusion in a public directory, of the purpose of that directory and of the fact that the data may be communicated to other telephone service providers. Secondly, referring to Recital 39 of Directive 2002/58, it clarified that the data must not be used for other purposes than that of being in-

663 Order of 19 February 2009, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, C-557/07, ECLI:EU:C:2009:107, paragraph 26.

664 Judgment of 29 January 2008, *Promusicae*, C-275/06, EU:C:2008:54, paragraphs 54-55; Judgment of 19 April 2012, *Bonnier Audio and Others*, C-461/10, ECLI:EU:C:2012:219, paragraph 55.

665 Order of 19 February 2009, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, C-557/07, ECLI:EU:C:2009:107, paragraph 29. See also Judgment of 19 April 2012, *Bonnier Audio and Others*, C-461/10, ECLI:EU:C:2012:219, paragraph 56.

666 Judgment of 24 November 2011, *Scarlet Extended*, C-70/10, ECLI:EU:C:2011:771, paragraph 53.

667 Judgment of 19 April 2012, *Bonnier Audio and Others*, C-461/10, ECLI:EU:C:2012:219 paragraphs 57-60.

668 In the meantime, the Universal Service Directive has been repealed by Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code OJ 2018 L 321 ("EECC"). Under the new EECC, the universal service obligations for directory services have been abolished.

669 Article 25(2) Universal Service Directive; now Article 112 EECC.

670 Judgment of 5 May 2011, *Deutsche Telekom*, C-543/09, ECLI:EU:C:2011:279.

cluded in a directory.[671] For a more detailed analysis of this point and our comments on the CJEU's reasoning, see Section 3.2.2(a) on specific consent above.

471. The CJEU also clarified that this consent must be provided by the subscriber, and not by the telephone service provider (see our analysis under Section 3.2.2(a) above).

472. In *Tele2 (Netherlands) and Others*, the CJEU added that the consent obtained to include a subscriber in an initial public directory, may also be relied on when passing the personal data onto a telephone service provider based in another Member State in view of their inclusion in a public directory.[672]

4.7 ***Cookies***

4.7.1 *Consent*

473. Since Directive 2009/136[673], Article 5(3) of Directive 2002/58 stipulates that the storing of information, or the gaining of access to information in the terminal equipment of a subscriber or user, is subject to the consent of that user or subscriber. Before giving consent, the subscriber or user must have been provided with 'clear and comprehensive information, in accordance with [Regulation 2016/679], inter alia, about the purposes of the processing'.

474. In *Planet49*, the CJEU was asked to clarify the consent conditions for the placing or reading out of cookies, as well as the information that must be provided to users or subscribers in that context.[674]

475. In relation to the consent requirements, unsurprinsingly, the CJEU decided that a pre-checked checkbox for placing or reading out a cookie, which the user must deselect to refuse his or her consent, does not constitute a valid consent under Article 2(h) of Directive 95/46 and Article 4(11) and Article 6(1)(a) of Regulation (EU) 2016/679.[675]

476. Indeed, the CJEU noted that the wording of Article 5(3) of Directive 2002/58 implies that an action is required from the user to give consent.[676] The definition of consent under Article 2(h) of Directive 95/46, to which Article 2(f) of Directive 2002/58 refers, points to a similar conclusion: it defines consent as an 'indication' of the data subject's wishes, which, as Advocate General Szpunar pointed out, "*clearly points to active, rather than passive, behaviour*". In that regard, the CJEU noted that "*consent given in the form of a preselected tick in a checkbox does not imply active behaviour on the part of a website user*".[677]

477. This CJEU further indicated that Article 7(a) of Directive 95/46, which requires consent to be given 'unambiguously', supports this interpretation. According to the CJEU, "[o]*nly active behaviour on the part of the data subject with a view to giving his or her consent may fulfil that requirement*". When relying on a pre-ticked checkbox, "*it would appear impossible in practice to ascertain objectively whether a website user had actually given his or her consent to the processing of his or her personal data by not selecting a pre-ticked checkbox*".[678] The CJEU found additional support for this interpretation in the fact that the initial wording of Article 5(3) of Directive 2002/58 provided only for a right to refuse cookies. As a result, the CJEU indicated that the evolution of this legal provision seems to indicate that "*henceforth user consent may no longer be presumed but must be the result of active behaviour on the part of the user*".[679]

478. The CJEU further emphasized that consent must be 'specific', in that it must "*relate specifically to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes*".[680]

479. Although the findings of the CJEU were made in relation to the provisions regulating consent under Directive 95/46, the CJEU noted that these findings apply *a fortiori* in light of Regulation 2016/679, as that regulation imposes more stringent requirements for consent than Directive 95/46. Indeed, under Article 4(11) of Regulation 2016/679, consent must be 'freely given, specific, informed and unambiguous'. It must take the form of a statement or of 'clear affirmative action' signifying agreement by the data subject to the processing of the personal data relating

671 Judgment of 5 May 2011, *Deutsche Telekom*, C-543/09, ECLI:EU:C:2011:279, paragraphs 62-63. See also, Judgment of 15 March 2017, *Tele2 (Netherlands) and Others*, C-536/15, ECLI:EU:C:2017:214 paragraphs 34-35.

672 Judgment of 15 March 2017, *Tele2 (Netherlands) and Others*, C-536/15, ECLI:EU:C:2017:214, paragraphs 34-41.

673 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2009] OJ L 337.

674 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801.

675 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 57.

676 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 49.

677 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 51-52. See also Opinion of 21 March 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:246, paragraph 60.

678 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraphs 54-55.

679 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraphs 56.

680 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 58.

to him or her.[681] In that regard, the CJEU specifically drew attention to Recital 32 of Regulation 2016/79, which states that consent could include 'ticking a box when visiting an internet website', and that '[s]ilence, pre-ticked boxes or inactivity should not therefore constitute consent'.

480. Finally, the CJEU concluded that the notion of 'consent' under Articles 2(f) and 5(3) of Directive 2002/58 must fulfil the requirements of Article 2(h) of Directive 95/46 and Articles 4(11) and 6(1)(a) of Regulation (EU) 2016/679, regardless of whether the information stored or accessed on a user's terminal equipment is personal data. As Advocate General Szpunar had already asserted, that provision"*aims to protect the user from interference with his or her private sphere, regardless of whether that interference involves personal data*".[682]

4.7.2 *Information to be provided*

481. The CJEU also clarified which information service providers must provide in relation to the use of cookies. It first recalled that "*Article 5(3) of Directive 2002/58 requires that the user concerned has given his or her consent, having been provided with clear and comprehensive information, 'in accordance with Directive* [95/46]*', inter alia, about the purposes of the processing*".[683]

482. According to the CJEU, such clear and comprehensive information must be sufficiently detailed "*so as to enable the user to comprehend the functioning of the cookies employed*".[684]

483. The referring court had asked whether the operator of a website is required to inform website users on the duration of the operation of the cookies and on whether or not third parties may have access to those cookies.

484. With regard to the duration of the processing of personal data, the CJEU noted that Article 10 of Directive 95/46 did not specifically require such information to be provided to the data subject. However, the CJEU highlighted that this Article did not include an exhaustive enumeration and specified that the provision of further information might be required where it was necessary to guarantee fair processing in respect of the data subject. Looking at the factual elements of the case referred, the CJEU concluded that the provision of information on the duration of the processing of personal data was indeed required to meet the requirement of fair data processing. The situation is even clearer under the regime of Regulation 2016/679, as Article 13(2)(a) now specifically mentions that the controller must, 'in order to ensure fair and transparent processing, provide the data subject with information relating, inter alia, to the period for which the personal data will be stored, or if that is not possible, to the criteria used to determine that period'.

485. As to whether or not information must be provided on the third parties who may have access to the cookies, the CJEU noted that both Article 10 of Directive 95/46 and Article 13 of Regulation 2016/679 expressly require that data subjects be informed of the recipients or categories of recipients of the data.[685]

5. Data Retention Directive

5.1 *Introduction*

486. Directive 2006/24 aimed at harmonising Member States' law concerning the obligations of providers of publicly available electronic communications services or of public communications networks to retain traffic and location data for the purpose of the investigation, detection and prosecution of serious crime.

487. In *Bonnier Audio and Others*[686], the CJEU had the opportunity to clarify the scope of application of Directive 2006/24 vis-à-vis Directive 2002/58; and in particular Article 15 of the latter Directive.

488. The CJEU first highlighted the scope and purpose of Directive 2006/24, as set out in Article 1(1), namely "*the handling and retention of* [electronic communications data] *for the purpose of the investigation, detection and prosecution of serious crime and their communication to the competent national authorities*".[687] The CJEU then indicated that Article 11 of Directive 2006/24 expressly stated that "*if such* [electronic communications data] *were retained specifically for the purposes of Article 1(1) of the directive, Article 15(1) of Directive 2002/58 does not apply to those data*".

489. On this basis, the CJEU concluded that Directive 2006/24 constitutes "*a special and restricted set of rules, derogating from and replacing Directive 2002/58 general in scope and, in particular, Article 15(1) thereof*".[688]

5.2 *Invalidation*

490. In its landmark decision *Digital Rights Ireland,* the CJEU invalidated Directive 2006/24 on the grounds that it

681 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraphs 60-61. See also Opinion of 21 March 2019, *Planet49*, C-679/17, ECLI:EU:C:2019:246, paragraph 70.

682 Opinion of 21 March 2019, *Planet49*, C-679/17, ECLI:EU:C:2019:246, paragraph 107.

683 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 73.

684 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 74.

685 Judgment of 1 October 2019, *Planet49*, C-673/17, ECLI:EU:C:2019:801, paragraph 80.

686 Judgment of 19 April 2012, *Bonnier Audio and Others*, C-461/10, ECLI:EU:C:2012:219.

687 Judgment of 19 April 2012, *Bonnier Audio and Others*, C-461/10, ECLI:EU:C:2012:219 paragraph 40.

688 Judgment of 19 April 2012, *Bonnier Audio and Others*, C-461/10, ECLI:EU:C:2012:219 paragraphs 40-43.

was incompatible with Articles 7 and 8 of the Charter in light of its Article 52(1).

5.2.1 *Existence of an interference*

491. Having analysed the types of data that were to be retained, the CJEU found that, even though the retention of the content of the communication was not mandated, these data 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 frequented by them*".[689]

492. The CJEU then noted that the data retention requirement derogated from the protections offered by Directives 95/46 and 2002/58 and especially the confidentiality of communications and of traffic data laid down in the latter Directive. The CJEU also recalled its earlier case law that to establish the existence of an interference with fundamental rights, it does not matter whether the data is sensitive or whether the individuals have been inconvenienced in any way.[690]

493. On the basis of these elements, the CJEU not only concluded that Directive 2006/24 constituted an interference with Articles 7 and 8 of the Charter, but it also followed the view of the Advocate General that this interference was wide-ranging and particularly serious.[691]

5.2.2 *Justification of the interference*

494. The CJEU then assessed whether the interference met the criteria of Article 52(1) of the Charter: (i) Was it provided for by law? (ii) Did it respect the essence of the fundamental rights? (iii) Was the proportionality principle met? (iv) Was it necessary? and (v) Did it meet objectives of general interest?

495. The fact that the interference was provided for by law, *in casu* Directive 2006/24 was not disputed. As for the essence of the fundamental right criterion, the CJEU decided that "*even though the retention of data required by Directive 2006/24 constitutes a particularly serious interference*"with Articles 7 and 8 of the Charter, the Directive did not adversely affect the essence of these rights because it did "*not permit the acquisition of knowledge of the content of the electronic communications as such*". The CJEU also noted that in relation to Article 8 of the Charter, Directives 95/46 and 2002/58 require Member States to ensure that appropriate security measures are adopted to avoid data breaches.[692]

496. The CJEU also recalled that it has ruled on several occasions that the fight against international terrorism and against serious crime satisfies the 'general interest' criterion. Therefore, taking into account the material objective laid down in Article 1(1) of Directive 2006/24, the interference at stake genuinely satisfied an objective of general interest.[693]

497. Next, the CJEU examined whether the data retention measures were appropriate for attaining the legitimate interests pursued and whether they did not exceed the limits of what was appropriate and necessary in order to achieve those objectives. Although the discretion of the EU legislature was reduced, given the importance of the protection of personal data in the EU, the CJEU concluded that the data retention measures were appropriate, as "*they are a valuable tool for criminal investigation*".[694]

498. The CJEU did however conclude that the interference was not limited to what was strictly necessary to attain the objectives of general interest. Particularly problematic was the fact that the data retention measure covered "*in a generalised manner, all persons, and all means of electronic communications 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*".[695] This means that it affects every person using electronic communications services; even those "*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*".[696] The CJEU also mentioned the fact that the retention obligation did not provide for any exception, as a result of which the data of individuals whose communications are protected by the obligation of professional secrecy are also retained.

499. Other issues that the CJEU identified related to the fact that Directive 2006/24 did not clearly define the access criteria and limitations for public authorities, that the period of retention adopted by the Member States was not required to be based on objective criteria and that the

689 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraphs 26-27.

690 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 33: Judgment of 20 May 2003, *Österreichischer Rundfunk and Others*, C-465/00, C-138/01 and C-139/01, ECLI:EU:C:2003:294, paragraph 75. See also Judgment of 2 October 2018, *Ministerio Fiscal*, C-207/16, ECLI:EU:C:2018:788, paragraph 51.

691 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 37. Opinion of 12 December 2013, *Digital Rights Ireland and Others*, Joined cases C-293/12 and C-594/12, ECLI:EU:C:2013:845, paragraph 80.

692 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraphs 39-40.

693 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraphs 41-44 and the case law referred therein.

694 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph, paragraph 49.

695 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph, paragraph 57.

696 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph, paragraph 58.

retention period did not distinguish between the categories of data being retained.[697]

500. The CJEU therefore concluded that Directive 2006/24 "*entails a wide-ranging and particularly serious interference*" with Articles 7 and 8 of the Charter, "*without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary*".[698] On this basis, it decided to invalidate Directive 2006/24.

6. Conclusion

501. In the past 25 years, the CJEU has developed a rich body of data protection case law. It has clarified a broad range of data protection topics, many of which were previously the subject of diverging interpretations by courts, regulators and practitioners.

502. However, despite the wealth of case law already available, many concepts of data protection law remain unclear. It is therefore not surprising that the number of referrals is increasing year after year.

503. There are currently twelve requests for a preliminary ruling pending before the CJEU.[699] They touch upon a wide array of topics, ranging from the application of the one-stop-shop[700], to the publication of personal data in the UBO register[701], and to the circumstances in which a DPO may be dismissed[702]. Some of these cases are rather anecdotic. Others have the potential of becoming landmark cases.

504. Therefore, the CJEU will clearly continue to play a crucial role in shaping EU data protection law in the coming years. Therefore, data protection practitioners are well advised to follow this up very closely.

697 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph, paragraphs 60-64.

698 Judgment of 8 April 2014, *Digital Rights Ireland and Others*, joined cases C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph, paragraphs 65.

699 Request for a preliminary ruling of 20 January 2021, Hauptpersonalrat der Lehrerinnen und Lehrer, C-34/21; Request for a preliminary ruling of 22 December 2020, *Avis Autovermietung,* C701/20; Request for a preliminary ruling of 13 November 2020, *SOVIM,* C-601/20; Request for a preliminary ruling of 21 October 2020, *Leistritz,* C-534/20; Request for a preliminary ruling of 24 September 2020, *Google,* C-460/20; Request for a preliminary ruling of 15 July 2020, *Facebook Ireland*,C-319/20; Request for a preliminary ruling of 29 May 2020, *Autoriteit Persoonsgegevens*, C-245/20, Request for a preliminary ruling of 28 April 2020, *Vyriausioji tarnybinės etikos komisija*, C-184/20; Request for a preliminary ruling of 14 April 2020, *Valsts ieņēmumu dienests,* C-175/20; Request for a preliminary ruling of 31 October 2019, *Ligue des droits humains*, C-817/19; Request for a preliminary ruling of 30 August 2019, *Facebook Ireland and Others*, C-645/19; Request for a preliminary ruling of 11 June 2019, *Latvijas Republikas Saeima*, C-439/19. Last checked on 5 February 2021.

700 Request for a preliminary ruling of 30 August 2019, *Facebook Ireland and Others*, C-645/19.

701 Request for a preliminary ruling of 13 November 2020, *SOVIM,* C-601/20.

702 Request for a preliminary ruling of 21 October 2020, *Leistritz,* C-534/20.