COURT OF JUSTICE
OF THE EUROPEAN UNION
RESEARCH AND DOCUMENTATION
DIRECTORATE

Fact sheet

PROTECTION OF PERSONAL DATA

The right to the protection of personal data is a fundamental right compliance with which is an important objective for the European Union.

It is enshrined in the Charter of Fundamental Rights of the European Union ('the Charter') which provides, in Article 8, that:

'1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.'

That fundamental right is, moreover, closely connected with the right to respect for private and family life enshrined in Article 7 of the Charter.

The right to the protection of personal data is also laid down in Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), which succeeded Article 286 EC in that respect.

As regards secondary legislation, the European Community has, since the mid-1990s, developed a range of instruments to ensure the protection of personal data. 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, [1] adopted on the basis of Article 100a EC, is the Union's principal legal instrument in this area. It lays down the general rules on the lawfulness of the processing of such data and the rights of data subjects and provides in particular for the establishment of independent supervisory authorities in Member States.

[1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995, L 281, p. 31); consolidated version of 20 November 2003, repealed as of 25 May 2018 (see footnote 5):

Directive 2002/58/EC [2] subsequently supplemented Directive 95/46 by harmonising the provisions of Member States' legislation on the protection of the right to privacy, notably with respect to the processing of personal data in the electronic communications sector [3]. It should be noted that the Union legislature is considering a review of that directive. In that regard, on 10 January 2017, the Commission put forward a proposition to replace that directive by a regulation relating to privacy and electronic communications. [4]

In addition, in the area of freedom, security and justice (ex Articles 30 and 31 TEU), Framework Decision 2008/977/JHA [5] regulates (until May 2018) the protection of personal data in the areas of judicial cooperation in criminal matters and police cooperation.

In 2016, the European Union reformed the overall legal framework in this area. To that end, it adopted Regulation (EU) 2016/679 [6] on data protection ('the GDPR'), which repeals Directive 95/46 and has been applicable from 25 May 2018, and Directive (EU) 2016/680 [7] on the protection of such data in criminal matters, which repeals Framework Decision 2008/977/JHA and was required to be transposed by Member States by 6 May 2018.

Last, in the context of the processing of personal data by the EU institutions and bodies, Regulation (EC) Nº 45/2001 ensured, first of all, the protection of such data. [8] In particular, the regulation enabled the European Data Protection Supervisor to be established in 2004. In 2018, the European Union adopted a new legal framework in this area, in particular through the adoption of Regulation (EU) 2018/1725, [9] which repeals Regulation (EC) Nº 45/2001 and Decision Nº 1247/2002/EC [10] and is applicable from 11 December 2018. In the interest of a coherent approach to personal data protection throughout the Union, that new regulation aims to align as far as possible the rules in this area with the regime established by the GDPR.

---

2 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 ('Privacy and electronic communications' Directive) (OJ 2002, L 201, p. 37); consolidated version : 19 December 2009.

3 Directive 2002/58 was amended by 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 (OJ 2006, L 105, p. 54). That directive was declared invalid by the Court in the judgment of 8 April 2014, *Digital Rights Ireland and Seitlinger and Others* (C-293/12 and C-594/12, EU:C:2014:238), on the ground that it adversely affected the right to respect for private life and the right to the protection of personal data (see Section I.1. 'Compatibility of secondary EU law with the right to the protection of personal data' in this fact sheet).

4 Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM/2017/010 final — 2017/03 (COD).

5 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ 2008, L 350, p. 60), repealed as of 6 May 2018 (see footnote 6).

6 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 (OJ 2016, L 119, p. 1).

7 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 (OJ 2016, L 119, p. 89).

8 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 (OJ 2001, L 8, p. 1).

9 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.

10 Decision Nº 1247/2002/EC of the European Parliament, of the Council and of the Commission of 1 July 2002 on the regulations and general conditions governing the performance of the European Data-protection Supervisor's duties (OJ 2002, L 183, p. 1).

TABLE OF CONTENTS

I. The right to the protection of personal data recognised by the Charter of Fundamental Rights of the European Union

1. Compatibility of secondary EU law with the right to the protection of personal data

Judgment of 9 November 2010 (Grand Chamber), Volker und Markus Schecke and Eifert (C-92/09 and C-93/09, EU:C:2010:662) [11]

In this case, the main proceedings were brought by agricultural operators against the *Land* of Hesse, and concerned the publication on the website of the Bundesanstalt für Landwirtschaft und Ernährung (German Federal Office for Agriculture and Food) of personal data relating to them as beneficiaries of funds from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD). The agricultural operators objected to such publication, claiming, in particular, that it was not justified by an overriding public interest. The *Land* of Hesse contended that the publication of the data arose from Regulations (EC) N° 1290/2005 [12] and N° 259/2008 [13], which governed the financing of the common agricultural policy and required the publication of information on natural persons in receipt of aid from the EAGF and EAFRD.

In that context, the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany) referred a number of questions to the Court concerning the validity of certain provisions of Regulation N° 1290/2005 and that of Regulation N° 259/2008, which required such information to be made available to the public, in particular through websites operated by the national offices.

The Court stated, with regard to the relationship between the right to the protection of personal data recognised by the Charter and the obligation of transparency in relation to European funds, that publication on a website of data naming the beneficiaries of the funds and indicating the amounts received by them constitutes, because the site is freely accessible to third parties, an interference with the right of the beneficiaries concerned to respect for their private life in general and to the protection of their personal data in particular (paragraphs 56 to 64).

In order to be justified, such interference must be provided for by law, respect the essence of those rights and, pursuant to the principle of proportionality, be necessary and genuinely meet objectives of general interest recognised by the European Union, whilst derogations from and

[11] This judgment was included in the 2010 Annual Report, p. 11.

[12] Council Regulation (EC) N° 1290/2005 of 21 June 2005 on the financing of the common agricultural policy (OJ 2005, L 209, p. 1), repealed by Regulation (EU) N° 1306/2013 of the European Parliament and of the Council of 17 December 2013 on the financing, management and monitoring of the common agricultural policy (OJ 2013, L 347, p. 549).

[13] Commission Regulation (EC) N° 259/2008 of 18 March 2008 laying down detailed rules for the application of Council Regulation (EC) N° 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the EAGF and the EAFRD (OJ 2008, L 76, p. 28), repealed by Commission Implementing Regulation (EU) N° 908/2014 of 6 August 2014 laying down rules for the application of Regulation (EU) N° 1306/2013 of the European Parliament and of the Council with regard to paying agencies and other bodies, financial management, clearance of accounts, rules on checks, securities and transparency (OJ 2014, L 255, p. 59).

limitations on those rights must apply only in so far as is strictly necessary (paragraph 65). In this context, the Court held that, whilst in a democratic society taxpayers have a right to be kept informed of the use of public funds, the Council and the Commission were nevertheless required to strike a proper balance between the various interests involved, and it was therefore necessary, before adopting the contested provisions, to ascertain whether publication of the data via a single website in a Member State went beyond what was necessary for achieving the legitimate aims pursued (paragraphs 77, 79, 85 and 86).

Thus, the Court declared certain provisions of Regulation Nº 1290/2005, and Regulation Nº 259/2008 in its entirety, to be invalid to the extent to which, with regard to natural persons who are beneficiaries of EAGF and EAFRD aid, those provisions impose an obligation to publish personal data relating to each beneficiary without drawing a distinction based on relevant criteria such as the periods during which those persons received such aid, the frequency of such aid or the nature and amount thereof (paragraph 92 and operative part 1). However, the Court did not call in question the effects of the publication of the lists of beneficiaries of such aid by the national authorities during the period prior to the date on which judgment was delivered (paragraph 94 and operative part 2).

Judgment of 17 October 2013, Schwarz (C-291/12, EU:C:2013:670)

Mr Schwarz had applied to the City of Bochum (Germany) for a passport, but had refused at that time to have his fingerprints taken. After Bochum had rejected his application, Mr Schwarz brought an action before the Verwaltungsgericht Gelsenkirchen (Administrative Court, Gelsenkirchen, Germany) in which he requested that the municipality be ordered to issue him with a passport without taking his fingerprints. In the proceedings before that court, Mr Schwarz disputed the validity of Regulation (EC) Nº 2252/2004 [14] which created the obligation to take the fingerprints of persons applying for passports, claiming, inter alia, that the regulation infringed the right to the protection of personal data and the right to respect for private life.

In that context, the Verwaltungsgericht Gelsenkirchen made a reference to the Court for a preliminary ruling in order to establish whether that regulation is valid, particularly in the light of the Charter, in so far as it obliges any person applying for a passport to provide fingerprints and provides for those fingerprints to be stored in that passport.

The Court replied in the affirmative, ruling that, although the taking and storing of fingerprints by the national authorities which is governed by Article 1(2) of Regulation Nº 2252/2004 constitutes an infringement of the rights to respect for private life and the protection of personal data, that infringement is justified by the aim of protecting against any fraudulent use of passports.

First of all, such a limitation, provided for by law, pursues an objective of general interest recognised by the Union, in so far as it is designed to prevent, inter alia, illegal entry into the European Union (paragraphs 35 to 38). Next, the taking and storing of fingerprints is

[14] 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).

appropriate for attaining that objective. Although the use of fingerprints as a means of ascertaining identity is not wholly reliable, it significantly reduces the likelihood of unauthorised persons being accepted. Moreover, a mismatch between the fingerprints of the holder of a passport and the data in that document does not mean that the person concerned will automatically be refused entry to the European Union but will simply result in a more detailed check in order definitively to establish that person's identity (paragraphs 42 to 45).

Last, as regards whether such processing is necessary, the Court was not made aware of any measures that are sufficiently effective but less of a threat to the rights recognised by Articles 7 and 8 of the Charter than the measures deriving from the method based on the use of fingerprints (paragraph 53). Article 1(2) of Regulation N° 2252/2004 does not require the processing of any fingerprints taken to go beyond what is necessary to achieve the aim pursued. The regulation explicitly states that fingerprints may be used only for verifying the authenticity of a passport and the identity of its holder. Furthermore, Article 1(2) of the regulation ensures protection against the risk of data including fingerprints being read by unauthorised persons and does not provide for the storage of fingerprints except within the passport itself, which belongs to the holder alone (paragraphs 54 to 57, 60 and 63).

Judgment of 8 April 2014 (Grand Chamber), Digital Rights Ireland and Seitlinger and Others (Joined Cases C-293/12 and C-594/12, EU:C:2014:238) [15]

This judgment has its origin in requests, made in national proceedings before the courts of Ireland and Austria, for a determination of the validity of Directive 2006/24/EC on the retention of data by reference to the fundamental rights to respect for private life and the protection of personal data. In Case C–293/12, proceedings were brought before the High Court (Ireland) by Digital Rights, a company, against the Irish authorities regarding the legality of national measures concerning the retention of data relating to electronic communications. In Case C–594/12, a number of constitutional cases came before the Verfassungsgerichtshof (Constitutional Court, Austria), in which annulment was sought of national legislation transposing Directive 2006/24 into Austrian law.

By their requests for a preliminary ruling, the Irish and Austrian courts referred questions to the Court concerning the validity of Directive 2006/24 in the light of Articles 7, 8 and 11 of the Charter. More specifically, the referring courts asked the Court whether the obligation which that directive places on providers of publicly available electronic communications or public communications networks to retain, for a certain period, data relating to a person's private life and to his communications and to allow the competent national authorities to access those data entailed an unjustified interference with those fundamental rights. The types of data concerned include data necessary to trace and identify the source of a communication and its destination, to identify the date, time, duration and type of a communication, to identify users' communication equipment, and to identify the location of mobile communication equipment, data which consist, inter alia, of the name and address of the subscriber or registered user, the calling telephone number, the number called and an IP address for internet services. Those data

[15] This judgment was included in the 2014 Annual Report, p. 60.

make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

The Court, first of all, held that, by imposing such obligations on those providers, Directive 2006/24 constituted a particularly serious interference with the fundamental rights to respect for private life and the protection of personal data, guaranteed by Articles 7 and 8 of the Charter. In that context, the Court found that that interference may be justified where it pursues an objective of general interest, such as the fight against organised crime. The Court stated in that regard, in the first place, that the retention of data required by the directive was not such as to adversely affect the essence of the fundamental rights to respect for privacy and the protection of personal data, in so far as it did not permit the acquisition of knowledge of the content of the electronic communications as such and provided that providers of services or of networks must respect certain principles of data protection and data security. In the second place, the Court observed that the retention of data for possible transmission to the competent national authorities genuinely satisfied an objective of general interest, namely the fight against serious crime and, ultimately, public security (paragraphs 38 to 44).

However, the Court found that, by adopting the directive on data retention, the EU legislature had exceeded the limits imposed by compliance with the principle of proportionality. Accordingly, it declared the directive invalid, on the ground that the wide-ranging and particularly serious interference with fundamental rights that it entailed was not sufficiently circumscribed to ensure that that interference was limited to what was strictly necessary (paragraph 65). Directive 2006/24 covered, in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting serious crime (paragraphs 57 to 59). The directive also failed to lay down any objective criterion by which to ensure that the competent national authorities would have access to the data and be able to use them for the sole purpose of preventing, investigating and prosecuting offences capable of being considered to be sufficiently serious to justify such an interference, or the substantive and procedural conditions relating to such access or such use (paragraphs 60 to 62). Finally, so far as the data retention period was concerned, the directive required that data be retained for a period of at least six months, without any distinction being made between the categories of data according to the persons concerned or on the basis of the possible usefulness of the data for the purposes of the objective pursued (paragraphs 63 and 64).

Furthermore, as regards the requirements arising under Article 8(3) of the Charter, the Court held that Directive 2006/24 did not provide for sufficient safeguards to ensure effective protection of the data against the risk of abuse and against any unlawful access to and use of the data, nor did it require that the data be retained within the European Union.

Consequently, the directive did not fully ensure control by an independent authority of compliance with the requirements of protection and security, as explicitly required by the Charter (paragraphs 66 to 68).

2. Respect for the right to the protection of personal data in the implementation of EU law

Judgment of 21 December 2016 (Grand Chamber), Tele2 Sverige (Joined Cases C-203/15 and C-698/15, EU:C:2016:970) [16]

Following the judgment in *Digital Rights Ireland and Seitlinger and Others* in which Directive 2006/24 was declared invalid (see above), two cases were brought before the Court concerning the general obligation imposed, in Sweden and in the United Kingdom, on providers of electronic communications services to retain the data relating to such communications, retention of which was required by the invalid directive.

On the day following delivery of the judgment in *Digital Rights Ireland and Seitlinger and Others*, the telecommunications company Tele2 Sverige informed the Swedish Post and Telecom Authority that it had decided that it would no longer retain data and that it intended to erase data previously recorded (Case C–203/15). Swedish law required the providers of electronic communications services to retain, systematically and continuously, and with no exceptions, all the traffic and location data of all their subscribers and registered users, with respect to all means of electronic communication. In Case C–698/15, three individuals brought actions challenging the United Kingdom rules on the retention of data which enabled the Secretary of State for the Home Department to require public telecommunications operators to retain all the data relating to communications for a maximum period of 12 months, although retention of the content of those communications was excluded.

In requests for a preliminary ruling from the Kammarrätten i Stockholm (Administrative Court of Appeal, Stockholm, Sweden) and the Court of Appeal (England and Wales) (Civil Division) (United Kingdom), the Court was asked to rule on the interpretation of Article 15(1) of Directive 2002/58 (the 'Privacy and Electronic Communications' directive), which enables the Member States to introduce certain exceptions to the obligation laid down in that directive to ensure the confidentiality of electronic communications and related traffic data.

In its judgment, the Court first of all held that Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, precludes national legislation such as the Swedish legislation which, for the purpose of fighting crime, provides for the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication. According to the Court, such legislation exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a

[16] This judgment was included in the 2016 Annual Report, p. 62.

democratic society, as required by Article 15(1), read in the light of the aforementioned provisions of the Charter (paragraphs 99 to 105, 107, 112 and operative part 1).

The same article, read in the light of the same provisions of the Charter, also precludes national legislation governing the protection and security of traffic and location data and, in particular, access of the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the European Union (paragraphs 118 to 122, 125 and operative part 2).

The Court, however, considered that Article 15(1) of Directive 2002/58 does not preclude legislation which permits the targeted retention of such data, as a preventive measure, for the purpose of fighting serious crime, provided that that retention is limited to what is strictly necessary with respect to the categories of data affected, the means of communication affected, the persons concerned and the retention period adopted. In order to satisfy those requirements, that national legislation must, first, lay down clear and precise rules ensuring the effective protection of data against the risk of misuse. It must, in particular, indicate the circumstances and conditions under which a data retention measure may be adopted as a preventive measure, thereby ensuring that such a measure is limited to what is strictly necessary. Second, as regards the substantive conditions which must be satisfied by national legislation, if it is to be ensured that data retention is limited to what is strictly necessary, the retention of data must continue to meet objective criteria that establish a connection between the data to be retained and the objective pursued. In particular, such conditions must be shown to be such as actually to circumscribe, in practice, the extent of that measure and thus the public affected. As regards the setting of limits on such a measure, the national legislation must be based on objective evidence which makes it possible to identify a public whose data are likely to reveal a link, at least an indirect one, with serious criminal offences, to contribute in one way or another to fighting serious crime or to prevent a serious risk to public security (paragraphs 108 to 111).

II. The processing of personal data within the meaning of the general legislation in this area

1. Personal data-processing operations excluded from the scope of Directive 95/46

Judgment of 30 May 2006 (Grand Chamber), Parliament v Council (C-317/04 and C-318/04, EU:C:2006:346)

Following the terrorist attacks of 11 September 2001, the United States had passed legislation providing that air carriers operating flights to or from the United States or across United States

territory had to provide the United States authorities with electronic access to the data contained in their reservation and departure control systems, known as Passenger Name Records (PNR).

The Commission considered that those provisions could come into conflict with European legislation and with that of the Member States on data protection and entered into negotiations with the United States authorities. Following those negotiations the Commission adopted, on 14 May 2004, Decision 2004/535/EC [17] finding that the United States Bureau of Customs and Border Protection (CBP) ensured an adequate level of protection for PNR data transferred from the Community ('the decision on adequacy'). Next, on 17 May 2004, the Council adopted Decision 2004/496/EC [18] approving the conclusion of an agreement between the European Community and the United States on the processing and transfer of PNR data to the CBP by air carriers located within the territory of the Member States of the European Community.

The European Parliament applied to the Court for annulment of those two decisions, contending, in particular, that adoption of the decision on adequacy had been *ultra vires*, that Article 95 EC (now Article 114 TFEU) did not constitute an appropriate legal basis for the decision approving the conclusion of the agreement and, in both cases, that fundamental rights had been infringed.

As regards the decision on adequacy, the Court examined, first of all, whether the Commission could validly adopt its decision on the basis of Directive 95/46. In that context, it noted that it was apparent from the decision on adequacy that the transfer of PNR data to the CBP constituted processing operations concerning public security and the activities of the State in areas of criminal law. According to the Court, although PNR data were initially collected by airlines in the course of an activity which came within the scope of EU law, namely sale of an aeroplane ticket which provided entitlement to a supply of services, the data processing which was taken into account in the decision on adequacy was quite different in nature. That decision concerned not data processing necessary for a supply of services, but data processing regarded as necessary for safeguarding public security and for law-enforcement purposes (paragraphs 56 and 57).

In that respect, the Court noted that the fact that the PNR data had been collected by private operators for commercial purposes, and that it was they who arranged for transfer of the data to a third country, did not prevent that transfer from being regarded as data processing that was excluded from the scope of the directive. The transfer fell within a framework established by the public authorities that related to public security. Consequently, the Court concluded that the decision on adequacy did not fall within the scope of the directive because it concerned processing of personal data that was excluded from it. The Court therefore annulled the decision on adequacy (paragraphs 58 and 59).

---

17 Commission Decision 2004/535/EC of 14 May 2004 on the adequate protection of personal data contained in the Passenger Name Record of air passengers transferred to the United States' Bureau of Customs and Border Protection (OJ 2004, L 235, p. 11).

18 Council Decision 2004/496/EC of 17 May 2004 on the conclusion of an Agreement between the European Community and the United States of America on the processing and transfer of PNR data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection (OJ 2004, L 183, p. 83, and corrigendum OJ 2005, L 255, p. 168).

As regards the Council decision, the Court found that Article 95 EC, read in conjunction with Article 25 of Directive 95/46, could not justify Community competence to conclude the agreement with the United States that was at issue. That agreement related to the same transfer of data as the decision on adequacy and therefore to data-processing operations which were excluded from the scope of the directive. Consequently, the Court annulled the Council decision approving the conclusion of the agreement (paragraphs 67 to 69).

Judgment of 11 December 2014, Ryneš (C-212/13, EU:C:2014:2428)

In response to repeated attacks, Mr Ryneš had installed a surveillance camera on his house. Following a further attack on his house, the recordings made by that camera had made it possible to identify two suspects, who had subsequently been prosecuted before the criminal courts. One of the suspects disputed, before the Czech Office for Personal Data Protection, the legality of the processing of the data recorded by the surveillance camera. The Office found that Mr Ryneš had infringed the personal data-protection rules and fined him.

The Nejvyšší správní soud (Supreme Administrative Court, Czech Republic), hearing an appeal by Mr Ryneš against a decision of the Městský soud v Praze (Prague City Court) which had confirmed the decision of the Office, asked the Court whether the recording made by Mr Ryneš for the purposes of protecting his life, health and property constituted a category of data processing that was not covered by Directive 95/46, on the ground that that recording had been made by a natural person in the course of a purely personal or household activity within the meaning of the second indent of Article 3(2) of that directive.

The Court ruled that the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity (paragraph 35 and operative part).

It noted in that regard that the protection of the fundamental right to private life guaranteed under Article 7 of the Charter requires that derogations and limitations in relation to the protection of personal data apply only in so far as is strictly necessary. 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 (paragraphs 27 to 29). Furthermore, the actual wording of that provision is such that Directive 95/46 does not cover the processing of data where the activity in the course of which that processing is carried out is a 'purely' personal or household activity. To the extent that video surveillance covers, even partially, a public space and is accordingly directed outwards from the private setting of the person processing the data in that manner, it cannot be regarded as an activity which is a purely 'personal or household' activity for the purposes of that provision (paragraphs 30, 31 and 33).

2. Concept of 'personal data'

Judgment of 19 October 2016, Breyer (C-582/14, EU:C:2016:779) [19]

Mr Breyer had brought an action before the German civil courts for an order prohibiting the Federal Republic of Germany from storing, or arranging for third parties to store, computerised data transmitted at the end of each consultation of websites of the German federal institutions. With a view to preventing attacks and making it possible to prosecute 'pirates', the provider of online media services of the German federal institutions was registering data consisting in a 'dynamic' IP address — an IP address which changes each time there is a new connection to the internet — and the date and time when the website was accessed. Unlike static IP addresses, dynamic IP addresses do not immediately enable a link to be established, through files accessible to the public, between a given computer and the physical connection to the network used by the internet service provider. The registered data would not, in themselves, enable the online media services provider to identify the user. However, the internet service provider did have additional information which, if combined with the IP address, would make it possible for the user to be identified.

In that context, the Bundesgerichtshof (Federal Court of Justice, Germany), before which an appeal on a point of law had been brought, asked the Court whether an IP address which is stored by an online media service provider when his website is accessed constitutes personal data for that service provider.

The Court noted, first of all, that, for information to be treated as 'personal data' within the meaning of Article 2(a) of Directive 95/46, there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person. The fact that the additional information necessary to identify the user of a website is held not by the online media services provider but by that user's internet service provider does not, therefore, appear to preclude dynamic IP addresses registered by the online media services provider from constituting personal data within the meaning of Article 2(a) of Directive 95/46 (paragraphs 43 and 44).

Consequently, the Court found that a dynamic IP address registered by an online media services provider when a person accesses a website that the provider makes accessible to the public constitutes personal data within the meaning of Article 2(a) of Directive 95/46, in relation to that provider, where the latter has the legal means which enable it to identify the data subject with additional data which the internet service provider has about that person (paragraph 49 and operative part 1).

[19] This judgment was included in the 2016 Annual Report, p. 61.

Judgment of 20 December 2017, Nowak (C-434/16, EU:C:2017:994)

Mr Nowak, a trainee accountant, had failed the examination set by the Institute of Chartered Accountants of Ireland. He submitted a data access request, under section 4 of Ireland's Data Protection Act, seeking all the personal data relating to him held by the Institute of Chartered Accountants. That institute sent certain documents to Mr Nowak, but refused to send to him his examination script, on the ground that it did not contain personal data relating to him, within the meaning of the data protection legislation.

Since the Data Protection Commissioner had also declined to grant his access request on the same grounds, Mr Nowak turned to the national courts. The Supreme Court (Ireland), hearing the appeal brought by Mr Nowak, asked the Court whether Article 2(a) of Directive 95/46 must be interpreted as meaning that, in circumstances such as those at issue in the main proceedings, the written answers submitted by a candidate at a professional examination and any examiner's comments with respect to those answers constitute personal data relating to that candidate, within the meaning of that provision.

In the first place, the Court noted that, for information to be treated as 'personal data' within the meaning of Article 2(a) of Directive 95/46, there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person. Furthermore, in the event that the examiner does not know the identity of the candidate when marking the answers submitted by that candidate in an examination, the body that set the examination, in this case the Institute of Chartered Accountants, does, nevertheless, have available to it the information needed to enable it easily and infallibly to identify that candidate through his identification number, placed on the examination script or its cover sheet, and thereby to ascribe the answers to that candidate.

In the second place, the Court found that the written answers submitted by a candidate at a professional examination constitute information that is linked to him as a person. The content of those answers reflects the extent of the candidate's knowledge and competence in a given field and, in some cases, his intellect, thought processes, and judgment. In addition, the purpose of collecting those answers is to evaluate the candidate's professional abilities and his suitability to practise the profession concerned. Moreover, the use of that information — one consequence of that use being the candidate's success or failure at the examination concerned — is liable to have an effect on his rights and interests, in that it may determine or influence, for example, the chance of entering the profession aspired to or of obtaining the post sought. It is equally true that the written answers submitted by a candidate at a professional examination constitute information that relates to that candidate by reason of its content, purpose or effect, where the examination is an open-book examination (paragraphs 31and 36 to 40).

In the third place, as regards the comments of an examiner with respect to the candidate's answers, the Court considered that they, no less than the answers submitted by the candidate at the examination, constitute information relating to that candidate, since they reflect the opinion or the assessment of the examiner of the individual performance of the candidate in the examination, particularly of his knowledge and competences in the field concerned. The

purpose of those comments is, moreover, precisely to record the examiner's evaluation of the candidate's performance, and those comments are liable to have effects for the candidate (paragraphs 42 and 43).

In the fourth place, the Court ruled that the written answers submitted by a candidate at a professional examination and any comments made by an examiner with respect to those answers are liable to be checked for, in particular, their accuracy and the need for their retention, within the meaning of Article 6(1)(d) and (e) of Directive 95/46, and may be subject to rectification or erasure, under Article 12(b) of the directive. To give a candidate a right of access to those answers and to those comments, under Article 12(a) of that directive, serves the purpose of that directive of guaranteeing the protection of that candidate's right to privacy with regard to the processing of data relating to him, irrespective of whether that candidate does or does not also have such a right of access under the national legislation applicable to the examination procedure. However, the Court pointed out that the rights of access and rectification, under Article 12(a) and (b) of Directive 95/46, do not extend to the examination questions, which do not as such constitute the candidate's personal data (paragraphs 56 and 58).

In the light of these points, the Court concluded that, in circumstances such as those at issue in the main proceedings, the written answers submitted by a candidate at a professional examination and any examiner's comments with respect to those answers constitute personal data, within the meaning of Article 2(a) of Directive 95/46 (paragraph 62 and operative part).

3. Concept of 'processing of personal data'

Judgment of 6 November 2003 (Grand Chamber), Lindqvist (C-101/01, EU:C:2003:596)

Mrs Lindqvist, a voluntary worker in a parish of the Protestant Church in Sweden, had set up, on her personal computer, internet pages on which she published personal data relating to a number of people working with her on a voluntary basis in the parish. Mrs Lindqvist was fined, on the ground that she had used the personal data by automatic means without giving prior written notice to the Swedish Datainspektion (supervisory authority for the protection of electronically transmitted data), that she had transferred the data to a third country without authorisation and that she had processed sensitive personal data.

In the appeal brought before the Göta hovrätt (Court of Appeal, Sweden) by Mrs Lindqvist against that decision, the national court referred questions to the Court for a preliminary ruling in order, in particular, to ascertain whether Mrs Lindqvist had carried out 'the processing of personal data wholly or partly by automatic means' within the meaning of Directive 95/46.

The Court held that the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by stating their telephone number or information regarding their working conditions and hobbies, constitutes 'the processing of personal data wholly or partly by automatic means' within the meaning of that directive (paragraph 27 and

operative part 1). Such processing of personal data in the course of charitable or religious activities is not covered by any of the exceptions to the scope of the directive, in so far as it does not fall within the category of activities concerning public security, or the category of a purely personal or household activity, which are outside the scope of the directive (paragraphs 38, 43 to 48 and operative part 2).

Judgment of 13 May 2014 (Grand Chamber), Google Spain and Google (C-131/12, EU:C:2014:317)

In 2010, a Spanish national had lodged with the Agencia Española de Protección de Datos (Spanish Data Protection Agency, 'the AEPD') a complaint against La Vanguardia Ediciones SL, the publisher of a daily newspaper with a large circulation in Spain, and against Google Spain and Google. The complainant contended that, when an internet user entered his name in the search engine of the Google group, the list of results would display links to two pages of La Vanguardia's newspaper, from 1998, which contained an announcement of an auction organised following attachment proceedings for the recovery of his debts. By his complaint, the complainant requested, first, that La Vanguardia be required either to remove or alter the pages in question, or to use certain tools made available by search engines in order to protect the data. Second, he requested that Google Spain or Google be required to remove or conceal the personal data relating to him so that they would disappear from the search results and links to La Vanguardia.

The AEPD had rejected the complaint against La Vanguardia, taking the view that the information in question had been lawfully published by it. However, it had upheld the complaint as regards Google Spain and Google and requested those two companies to take the necessary measures to withdraw the data from their index and to render access to the data impossible in the future. The companies brought two actions before the Audiencia Nacional (National High Court, Spain) for annulment of the AEPD's decision, and the Spanish court referred a series of questions to the Court.

Thus, the Court had occasion to clarify the concept of 'processing of personal data' on the internet in the light of Directive 95/46.

The Court held that the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as processing of personal data when that information contains personal data (operative part 1 of the judgment). The Court also noted that the operations referred to by the directive must be classified as processing where they exclusively concern material that has already been published in that form in the media. A general derogation from the application of the directive in such a case would largely deprive the directive of its effect (paragraphs 29 and 30).

Judgment of 10 July 2018 (Grand Chamber), Jehovan todistajat (C-25/17, EU:C:2018:551) [20]

The Finnish Data Protection Board adopted a decision prohibiting the Jehovah's Witnesses Community from collecting or processing personal data in the course of door-to-door preaching by its members unless the requirements of Finnish legislation relating to the processing of personal data were observed. The members of the Jehovah's Witnesses Community take notes in the course of their door-to-door preaching concerning visits to persons who are unknown to themselves or to that community. Those data are collected as a memory aid and in order to be retrieved for any subsequent visit without the knowledge or consent of the persons concerned. In that respect, the Jehovah's Witnesses Community has given its members guidelines on the taking of such notes which appear in at least one of its magazines which is dedicated to the activity of preaching.

The Court held that the collection of personal data by members of a religious community in the course of door-to-door preaching and the subsequent processing of those data does not come within the exceptions to the scope of Directive 95/46 since it does not constitute either the processing of personal data for the purpose of activities referred to in Article 3(2), first indent, of that directive or the processing of personal data carried out by a natural person in the course of a purely personal or household activity, within the meaning of Article 3(2), second indent, thereof (paragraph 51 and operative part 1).

Judgment of 14 February 2019, Buivids (C-345/17, EU:C:2019:122)

In this case, the Court examined the interpretation of, first, the scope of Directive 95/46 and, second, the concept of 'processing of personal data solely for journalistic purposes' in Article 9 of that directive.

This judgment was delivered in the context of a request for a preliminary ruling made by the Supreme Court of Latvia, adopted in proceedings between Mr Buivids ('the applicant') and the National Data Protection Agency concerning an action seeking a declaration as to the illegality of a decision of that authority, according to which the applicant infringed national law as regards protection of personal data by publishing a video, filmed by him, on an internet site of the statement which he made in the context of administrative proceedings involving the imposition of a penalty in a station of the Latvian national police. Following the dismissal of his action by two lower courts, the applicant brought an appeal in cassation before the Supreme Court. He invoked, before that court, his right to freedom of expression, claiming that the video in question shows public officials of the Latvian national police — namely public persons in a place accessible to the public — who, on that ground, fall outside the scope of the Personal Data Protection Law.

First of all, as regards the scope of Directive 95/46, the Court stated, first, that the recorded images of the police officers constitute personal data and second, that the video recording

[20] This judgment was included in the 2018 Annual Report, p. 87 and 88.

which was stored in the memory of the camera used by the applicant constitutes a processing of personal data. The Court thus added that the act of publishing a video recording, which contains personal data, on a video website on which users can watch and share videos, constitutes processing of those data wholly or partly by automatic means. Furthermore, the Court notes that that recording and publication of the video in question do not come within the scope of the exceptions to the scope of Directive 95/46, which concern, in particular, the processing of data for the exercise of an activity which falls outside the scope of that directive and processing in the course of a purely personal or household activity. Therefore, the Court concluded that the recording of a video of police officers in a police station, while a statement is being made, and the publication of that video on a website, on which users can send, watch and share videos, are matters which come within the scope of Directive 95/46 (paragraphs 31, 32, 35, 39, 42, 43 and operative part 1).

Second, as regards the concept of 'processing personal data solely for journalistic purposes', the Court noted, first, that, by interpreting the notion of 'journalism' broadly, the exemptions in Article 9 of Directive 95/46 apply to every person engaged in journalism. Thus, the Court held that the fact that the applicant is not a professional journalist does not appear to be capable of excluding the possibility that the recording of the video in question and its transmission may constitute 'processing of personal data solely for journalistic purposes'. Moreover, the Court stated that the exemptions and derogations in Article 9 of Directive 95/46 must be applied only where they are necessary in order to reconcile two fundamental rights, namely the right to privacy and the right to freedom of expression. In that respect, the Court noted that it cannot be ruled out that the recording and publication of the video in question, which took place without the police officers in that video being informed of the recording and its purposes, constitutes and interference with the fundamental right to privacy of those persons. Therefore, the Court held that the recording and publication of the video in question on a video website may constitute a processing of personal data solely for journalistic purposes 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, this being a matter which it is for the referring court to determine (paragraphs 51, 52, 55, 63, 67 and operative part 2).

Judgment of 22 June 2021 (Grand Chamber), Latvijas Republikas Saeima (Penalty points) (C-439/19, EU:C:2021:504)

B is a natural person upon whom penalty points were imposed on account of one or more road traffic offences. The Ceļu satiksmes drošības direkcija (Road Safety Directorate, Latvia) ('the CSDD') entered those penalty points in the national register of vehicles and their drivers.

Under the Latvian Law on road traffic, [21] information relating to the penalty points imposed on drivers of vehicles entered in that register is accessible to the public and disclosed by the CSDD to any person who so requests, without that person having to establish a specific interest in obtaining that information, including to economic operators for re-use. Uncertain as to the lawfulness of that legislation, B brought a constitutional appeal before the Latvijas Republikas

[21] Article 141(2) of the Ceļu satiksmes likums (Law on road traffic) of 1 October 1997 (Latvijas Vēstnesis 1997, Nº 274/276).

Satversmes tiesa (Constitutional Court, Latvia), requesting the court to examine whether the legislation complied with the right to respect for private life.

The Constitutional Court held, in its assessment of that constitutional right, that it must take into account the GDPR. Thus, it asked the Court to clarify the scope of several provisions of the GDPR with the aim of determining whether the Latvian aw on road traffic is compatible with that regulation.

By its judgment, delivered in the Grand Chamber, the Court holds that the processing of personal data relating to penalty points constitutes 'processing of personal data relating to criminal convictions and offences' [22] in respect of which the GDPR provides for enhanced protection because of the particular sensitivity of the data at issue (paragraphs 10, 46, 74, 94 and operative part 1).

In that context, it notes, as a preliminary point, that the information relating to penalty points is personal data and that its disclosure by the CSDD to third parties constitutes processing which falls within the material scope of the GDPR. That scope is very broad, and that processing is not covered by the exceptions to the applicability of that regulation (paragraphs 60, 61 and 72).

Thus, first, that processing is not covered by the exception relating to the non-applicability of the GDPR to processing carried out in the course of an activity which falls outside the scope of EU law [23]. That exception must be regarded as being designed solely to exclude from the scope of that regulation the processing of personal data carried out by State authorities in the course of an activity which is intended to safeguard national security or of an activity which can be classified in the same category. These activities encompass, in particular, those that are intended to protect essential State functions and the fundamental interests of society. Activities relating to road safety do not pursue that objective and consequently cannot be classified in the category of activities having the aim of safeguarding national security (paragraphs 62 and 66 to 68).

Second, the disclosure of personal data relating to penalty points is not processing covered by the exception providing for the non-applicability of the GDPR to processing of personal data carried out by the competent authorities in criminal matters either. [24] The Court finds, in fact, that in carrying out that disclosure, the CSDD cannot be regarded as such a 'competent authority' [25] (paragraphs 69 to 71).

In order to determine whether access to personal data relating to road traffic offences, such as penalty points, amounts to processing of personal data relating to 'offences' [26] which enjoys enhanced protection, the Court finds, relying in particular on the origins of the GDPR, that that concept refers only to criminal offences. However, the fact that, in the Latvian legal system, road

22 Article 10 of the GDPR.

23 Article 2(2)(a) of the GDPR

24 Article 2(2)(d) of the GDPR.

25 Article 3(7) of 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 (OJ 2016 L 119, p. 89).

26 Article 10 of the GDPR.

traffic offences are classified as administrative offences is not decisive when determining whether those offences fall within the concept of 'criminal offence', since it is an autonomous concept of EU law which requires an autonomous and uniform interpretation throughout the European Union. Thus, after recalling the three criteria relevant for assessing whether an offence is criminal in nature, namely the legal classification of the offence under national law, the nature of the offence and the degree of severity of the penalty incurred, the Court finds that the road traffic offences at issue are covered by the term 'offence' within the meaning of the GDPR. As regards the first two criteria, the Court finds that, even if offences are not classified as 'criminal' by national law, the nature of the offence, and in particular the punitive purpose pursued by the penalty that the offence may give rise to, may result in its being criminal in nature. In the present case, the giving of penalty points for road traffic offences, like other penalties to which the commission of those offences may give rise, are intended, inter alia, to have such a punitive purpose. As regards the third criterion, the Court observes that only road traffic offences of a certain seriousness entail the giving of penalty points and that they are therefore liable to give rise to penalties of a certain severity. Moreover, the imposition of such points is generally additional to the penalty imposed, and the accumulation of those points has legal consequences, which may even extend to a driving ban (paragraphs 77, 80, 85, 87 to 90 and 93).

4. Concept of a 'personal data filing system'

Judgment of 10 July 2018 (Grand Chamber), Jehovan todistajat (C-25/17, EU:C:2018:551)

In this judgment (see also Section II.3. 'Concept of "processing of personal data"'), the Court clarified the concept of a 'filing system' in Article 2(c) of Directive 95/46.

Thus, after pointing out that that directive applies to the manual processing of personal data only where the data processed form part of a filing system or are intended to form part of a filing system, the Court held that that concept covers a set of personal data collected in the course of door-to-door preaching, consisting of the names and addresses and other information concerning the persons contacted, if those data are structured according to specific criteria which, in practice, enable them to be easily retrieved for subsequent use. In order for such a set of data to come within that concept, it is not necessary that they include data sheets, specific lists or other search methods (paragraph 62 and operative part 2).

5. Concept of a 'controller of the processing of personal data'

Judgment of 10 July 2018 (Grand Chamber), Jehovan todistajat (C-25/17, EU:C:2018:551)

In this judgment (see also Sections II.3. and II.4. 'Concept of "processing of personal data"' and 'Concept of a "personal data filing system"'), the Court adjudicated on the responsibility of a religious community with regard to the processing of personal data carried out in the context of door-to-door preaching organised, coordinated and encouraged by that community.

Thus, the Court found that the obligation for every person to comply with the rules of EU law on the protection of personal data cannot be regarded as amounting to an interference in the organisational autonomy of religious communities. In that regard, the Court held that Article 2(d) of Directive 95/46, read in the light of Article 10(1) of the Charter, must be interpreted as supporting the finding that a religious community is a controller, jointly with its members who engage in preaching, of the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community, without it being necessary that the community has access to those data and without it being necessary to establish that that community has given its members written guidelines or instructions concerning that data processing (paragraphs 74, 75 and operative part 3).

Judgment of 5 June 2018 (Grand Chamber), Wirtschaftsakademie Schleswig Holstein (C-210/16, EU:C:2018:388) [27]

The German data protection authority, in its capacity as supervisory authority within the meaning of Article 28 of Directive 95/46, had ordered a German company, operating in the field of education and offering educational services by means of a fan page hosted on the social networking site Facebook, to deactivate its page. According to that authority, neither the company nor Facebook informed visitors to the fan page that Facebook, by means of cookies, collected personal data concerning them and that the company and Facebook then processed those data.

In that context, the Court clarified the concept of a 'controller of the processing' of personal data. In that respect, it took the view that the administrator of a fan page hosted on Facebook, such as the company at issue in the main proceedings, takes part, by its definition of parameters (depending in particular on its target audience and the objectives of managing and promoting its activities), in the determination of the purposes and means of processing the personal data of the visitors to that fan page. According to the Court, that administrator must therefore be categorised as a controller responsible for such processing within the European Union, jointly with Facebook Ireland (the subsidiary in the European Union of the US company Facebook), within the meaning of Article 2(d) of Directive 95/46 (paragraph 39).

Judgment of 29 July 2019, Fashion ID (C-40/17, EU:C:2019:629)

In this judgment, the Court had occasion to clarify the concept of a 'controller of the processing of personal data' as regards the embedding of a social plugin on a website.

In this case, Fashion ID, a German online clothing retailer, had embedded on its website the 'Like' social plugin from the social network Facebook. The act of embedding that plugin appears to have made it possible for Facebook Ireland to obtain the personal data of visitors to the Fashion ID website. That transmission of data appears to occur regardless of whether or not the

[27] This judgment was included in the 2018 Annual Report, p. 86 and 87.

visitor is aware of such an operation, is a member of the social network Facebook or has clicked on the Facebook 'Like' button.

The Verbraucherzentrale NRW, a German public-service association tasked with safeguarding the interests of consumers, criticises Fashion ID for transmitting to Facebook Ireland personal data belonging to visitors to its website, first, without their consent and, second, in breach of the duties to inform set out in the provisions relating to the protection of personal data. In the context of that dispute, the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany) requested the Court to provide an interpretation of a number of provisions of Directive 95/46.

The Court held, first, that the operator of a website, such as Fashion ID, can be considered to be a controller within the meaning of Article 2(d) of Directive 95/46. That status is, however, limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means, that is to say, the collection and disclosure by transmission of the data at issue. By contrast, the Court states that it seems, at the outset, impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland following their transmission to the latter, with the result that Fashion ID cannot be considered to be a controller in respect of those operations within the meaning of Article 2(d) (paragraphs 76, 85 and operative part 2).

Furthermore, the Court noted that it is necessary that that operator and that provider each pursue a legitimate interest, within the meaning of Article 7(f) of Directive 95/46, through those processing operations in order for those operations to be justified in respect of each of them (paragraph 97 and operative part 3).

Lastly, the Court stated that the consent of the data subject, referred to in Article 2(h) and Article 7(a) of Directive 95/46, must be obtained by the operator of a website only with regard to the operations involving the processing of personal data in respect of which that operator determines the purposes and means. In such a situation, the duty to inform laid down in Article 10 of that directive is incumbent also on that operator, but the information that the latter must provide to the data subject need relate only to the operation or set of operations involving the processing of personal data in respect of which that operator actually determines the purposes and means (paragraph 106 and operative part 4).

Judgment of 9 July 2020, Land Hessen (C-272/19, EU:C:2020:535)

A citizen who presented a petition to the Petitions Committee of the Parliament of Land Hessen (Germany) asked the latter for access to personal data concerning him kept by it in the context of the processing of his petition. The citizen based his request on the GDPR, which provides for the right of a data subject to obtain, from the controller, access to personal data concerning him.

The President of the Parliament Land Hessen rejected this request on the basis that the petition procedure is a parliamentary task and that the parliament is not subject to the GDPR.

The Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany), hearing the appeal brought by the citizen, considers that German law does not grant any right of access to personal data in the context of a petition such as the one in question. Believing, however, that such a right of access could result from the GDPR, the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden) made a reference to the Court of Justice on this point. In addition, having doubts as to its own independence and therefore its capacity as a court authorized to submit preliminary questions to the Court, the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden) included this question in its reference to the Court of Justice.

By its judgment, the Court replies that, insofar as a Petitions Committee of the parliament of a federated state of a member state determines, alone or together with others, the purposes and means of the processing of personal data, this committee must be qualified as a "controller" within the meaning of the GDPR [28]. The processing of personal data carried out by such a committee is therefore subject to this regulation, in particular to the provision conferring on data subjects a right of access to personal data concerning them [29].

The Court noted in particular that the activities of the Petitions Committee of the Parliament of Land Hessen do not fall under an exception provided for by the GDPR. It admits that such activities are public and specific to this Land, as this committee contributes indirectly to parliamentary activity, but notes that these activities are also of a political as well as an administrative nature. In addition, it does not appear from the information available to the Court that these activities correspond, in this case, to one of the exceptions provided for by the GDPR (paragraph 71 to 74 and operative part).

6. Conditions for lawful processing of personal data

Judgment of 16 December 2008 (Grand Chamber), Huber (C-524/06, EU:C:2008:724) [30]

The Federal Office for Migration and Refugees (Bundesamt für Migration und Flüchtlinge, Germany) was responsible for maintaining a central register of foreign nationals which contained certain personal data relating to foreign nationals who were resident in Germany for a period of more than three months. The register was used for statistical purposes and in the exercise by the security and police services and by the judicial authorities of their powers in relation to the prosecution and investigation of activities which were criminal or which threatened public security.

Mr Huber, an Austrian national, moved to Germany in 1996 in order to carry on business there as a self-employed insurance agent. He took the view that he had been discriminated against by

[28] Article 4(7) of the GDPR.
[29] Article 15 of the GDPR.
[30] This judgment was included in the 2008 Annual Report, p. 45.

reason of the processing of the data concerning him contained in the register in question, there being no such database in respect of German nationals, and requested that the data be deleted.

In that context, the Oberverwaltungsgericht für das Land Nordrhein-Westfalen (Higher Administrative Court for the Land North Rhine-Westphalia, Germany), before which proceedings were brought, asked the Court whether the processing of personal data of the kind undertaken in the register in question was compatible with EU law.

The Court noted, first of all, that the right of residence of an EU citizen in a Member State of which he is not a national is not unconditional but may be subject to limitations. Thus, the use of such a register for the purpose of providing support to the authorities responsible for the application of the legislation relating to the right of residence is, in principle, legitimate and, having regard to its nature, compatible with the prohibition of discrimination on grounds of nationality laid down by Article 12(1) EC (now first paragraph of Article 18 TFEU). However, such a register must not contain any information other than what is necessary for that purpose, as provided for by the directive on the protection of personal data (paragraphs 54, 58 and 59).

As regards the concept of 'the necessity' of the processing under Article 7(e) of Directive 95/46, the Court noted first of all that what was at issue was a concept which had its own independent meaning in EU law and which had to be interpreted in a manner that fully reflected the objective of Directive 95/46 as defined in Article 1(1) thereof. The Court went on to find that a system for processing personal data complies with EU law if it contains only the data which are necessary for the application by those authorities of that legislation and if its centralised nature enables that legislation to be more effectively applied as regards the right of residence of Union citizens who are not nationals of that Member State.

The storage and processing of personal data containing individualised personal information in such a register for statistical purposes cannot, on any basis, be considered to be necessary within the meaning of Article 7(e) of Directive 95/46 (paragraphs 52, 66 and 68).

Furthermore, with regard to the question of the use of the data contained in the register for the purposes of the fight against crime, the Court stated, in particular, that that objective involves the prosecution of crimes and offences committed, irrespective of the nationality of their perpetrators. It follows that, as regards a Member State, the situation of its nationals cannot, as regards the objective of fighting crime, be different from that of Union citizens who are not nationals of that Member State and who are resident in its territory. Consequently, a difference in treatment between those nationals and those Union citizens which arises by virtue of the systematic processing of personal data relating only to Union citizens who are not nationals of the Member State concerned for the purposes of fighting crime constitutes discrimination which is prohibited by Article 12(1) EC (paragraphs 78 to 80).

Judgment of 24 November 2011, ASNEF and FECEMD (C-468/10 and C-469/10, EU:C:2011:777)

The Asociación Nacional de Establecimientos Financieros de Crédito (National Association of Credit Institutions) (ASNEF) and the Federación de Comercio Electrónico y Marketing Directo

(Federation of Electronic Commerce and Direct Marketing) (FECEMD) brought administrative proceedings before the Tribunal Supremo (Supreme Court, Spain) challenging several articles of Royal Decree 1720/2007 which had implemented Organic Law 15/1999 transposing Directive 95/46.

In particular, ASNEF and FECEMD submitted that, in order to enable personal data to be processed in the absence of the data subject's consent, Spanish law had added a condition not contained in Directive 95/46, requiring that the data appear in 'public sources', as set out in Article 3(j) of Organic Law 15/1999. They contended that that law and Royal Decree 1720/2007 restricted the scope of Article 7(f) of Directive 95/46, which makes the processing of personal data without the data subject's consent conditional only upon the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed.

In that regard, the Court noted, first of all, that Article 7 of Directive 95/46 sets out an exhaustive, restrictive list of cases in which the processing of personal data may be regarded as being lawful in the absence of the data subject's consent. Under Article 5 of the directive, Member States may not, therefore, introduce principles relating to the lawfulness of the processing of personal data other than those listed in Article 7, or alter, by additional requirements, the scope of the principles provided for in Article 7. Article 5 merely authorises Member States to specify, within the limits of Chapter II of that directive and, accordingly, Article 7 thereof, the conditions under which the processing of personal data is lawful (paragraphs 30, 32 and 33).

In particular, in order to carry out the necessary balancing of the opposing rights and interests, provided for in Article 7(f) of the directive, Member States may establish guidelines. They may take into consideration, too, the fact that the seriousness of the infringement of the data subject's fundamental rights resulting from that processing can vary depending on whether or not the data in question already appear in public sources (paragraphs 44 and 46).

However, the Court considered that, if national rules exclude the possibility of processing certain categories of personal data by definitively prescribing, for those categories, the result of the balancing of the opposing rights and interests, without allowing a different result by virtue of an individual's particular circumstances, that is no longer a case of precision within the meaning of Article 5 of Directive 95/46. In consequence, the Court concluded that Article 7(f) of Directive 95/46 precludes Member States from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case (paragraphs 47 and 48).

Judgment of 19 October 2016, Breyer (C-582/14, EU:C:2016:779)

In this judgment (see also Section II.2. 'Concept of "personal data"'), the Court also ruled on the question whether Article 7(f) of Directive 95/46 precludes a provision in national law under which an online media services provider may collect and use a user's personal data without his consent only to the extent necessary in order to facilitate, and charge for, the specific use of the telemedium by the user concerned, and under which the purpose of ensuring the general

operability of the telemedium cannot justify use of the data beyond the end of the particular use of the telemedium.

The Court held that Article 7(f) of Directive 95/46 precluded the legislation in question. Under that provision, personal data may be processed as provided for by that provision if processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. In that instance, the German legislation had excluded, categorically and in general, the possibility of processing certain categories of personal data, without allowing the opposing rights and interests at issue to be balanced against each other in a particular case. In so doing, it had unlawfully reduced the scope of the principle laid down in Article 7(f) of Directive 95/46 by excluding the possibility of balancing the objective of ensuring the general operability of the online media against the interests or fundamental rights and freedoms of those users (paragraphs 62 to 64 and operative part 2).

Judgment of 4 May 2017, Rīgas satiksme (C-13/16, EU:C:2017:336)

This case arose in proceedings between the Latvian national police and Rīgas satiksme, a trolleybus company in the city of Riga, concerning a request for disclosure of data identifying the perpetrator of an accident. In this case, in a traffic accident, a taxi driver had stopped his vehicle at the side of the road. While a trolleybus of Rīgas satiksme was passing alongside the taxi, a passenger sitting in the back seat of the taxi had opened the door, which had scraped against and damaged the trolleybus. In order to issue civil proceedings, Rīgas satiksme had, inter alia, asked the national police to disclose data identifying the perpetrator of the accident. The police had refused to disclose the passenger's identity document number and address and the documents relating to the explanations given by those involved in the accident on the ground that documents relating to administrative proceedings leading to penalties could be disclosed only to the parties to that case, and, as regards the identity document number and address, that the law on the protection of personal data prohibited the disclosure of such information concerning private individuals.

In those circumstances, the Augstākās tiesas Administratīvo lietu departaments (Supreme Court, Administrative Division, Latvia) decided to ask the Court whether Article 7(f) of Directive 95/46 imposes an obligation to disclose personal data to a third party in order to enable him to bring an action for damages before a civil court for harm caused by the person concerned by the protection of those data, and whether the fact that that person is a minor has a bearing on the interpretation of that provision.

The Court held that Article 7(f) of Directive 95/46 must be interpreted as not imposing an obligation to disclose personal data to a third party in order to enable him to bring an action for damages before a civil court for harm caused by the person concerned by the protection of those data. However, that provision would not preclude such disclosure if it were made on the

basis of national law, in accordance with the conditions laid down in that provision (paragraphs 27, 34 and operative part).

In that context, the Court noted that, subject to the determination to be carried out in that respect by the national court, it did not appear to be justified, in circumstances such as those at issue in the main proceedings, to refuse to disclose to an injured party the personal data necessary for bringing an action for damages against the person who caused the harm, or, where appropriate, the persons exercising parental authority, on the ground that the person who caused the damage was a minor (paragraph 33).

Judgment of 27 September 2017, Puškár (C-73/16, EU:C:2017:725)

In the dispute in the main proceedings, Mr Puškár had brought an action before the Najvyšší súd Slovenskej republiky (Supreme Court of the Slovak Republic) for an order requiring the Finančné riaditel'stvo (Finance Directorate), all tax offices under its control and the Kriminálny úrad finančnej správy (Financial Administration Criminal Office) not to include his name on the list of persons considered by the Finance Directorate to be 'front men', drawn up by the latter in the context of tax collection and the updating of which was carried out by the Finance Directorate and the Financial Administration Criminal Office ('the list at issue'). He also sought to have any reference to him removed from those lists and from the finance authority's IT system.

In those circumstances, the Najvyšší súd Slovenskej republiky (Supreme Court of the Slovak Republic) referred, inter alia, a question to the Court as to whether the right to respect for private and family life, home and communications, in Article 7, and the right to the protection of personal data, in Article 8 of the Charter, could be interpreted in such a way as not to allow a Member State to create, without the consent of the person concerned, a list of personal data for the purposes of tax administration, so that the fact that personal data were made available to a public authority for the purpose of combating tax fraud in itself constituted a risk.

The Court concluded that Article 7(e) of Directive 95/46 does not preclude the processing of personal data by the authorities of a Member State for the purpose of collecting tax and combating tax fraud such as that effected by the drawing-up of a list of persons such as that at issue in the main proceedings, without the consent of the data subjects, provided that, first, those authorities were invested by the national legislation with tasks carried out in the public interest within the meaning of that article, that the drawing-up of that list and the inclusion on it of the names of the data subjects is in fact adequate and necessary for the attainment of the objectives pursued and that there are sufficient indications to assume that the data subjects are rightly included in that list, and, second, that all of the conditions for the lawfulness of that processing of personal data imposed by Directive 95/46 are satisfied (paragraph 117 and operative part 3).

In that regard, the Court noted that it is for the national court to determine whether the establishment of the list at issue is necessary for the performance of the tasks carried out in the public interest at issue in the main proceedings, taking account, in particular, of the precise purpose of the establishment of the list at issue, the legal effects to which the persons

appearing on it are subject and whether or not that list is of a public nature. In the light of the principle of proportionality, it is, moreover, for the national court to ascertain whether the establishment of the list at issue and the inclusion of the names of the data subjects on it are suitable for achieving the objectives pursued by them and whether there is no other less restrictive means of achieving those objectives (paragraphs 111, 112 and 113).

The Court further held that the fact that a person is placed on the list at issue is likely to infringe some of his rights. Indeed, inclusion in that list could harm his reputation and affect his relations with the tax authorities. Likewise, such inclusion could affect the presumption of that person's innocence, set out in Article 48(1) of the Charter, as well as the freedom of legal persons associated with the natural persons included in the list at issue to conduct a business, enshrined in Article 16 of the Charter. Consequently, an infringement of this kind can be proportionate only if there are sufficient grounds to suspect the person concerned of purportedly acting as a company director of the legal persons associated with him and of thus undermining the collection of taxes and the combating of tax fraud (paragraph 114).

Furthermore, the Court found that if there were grounds for limiting, under Article 13 of Directive 95/46, certain of the rights provided for in Articles 6 and 10 to 12 thereof, such as the data subject's right to information, such a limitation 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 (paragraph 116).

Judgment of 11 November 2020, Orange Romania (C-61/19, EU:C:2020:901)

Orange România SA is a provider of mobile telecommunications services on the Romanian market. By decision of 28 March 2018, the l'Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) (the National Authority for the Supervision of Personal Data Processing, Romania) imposed a fine on Orange România for collecting and storing copies of customers' identity documents without their express consent.

According to the ANSPDCP, between 1 and 26 March 2018, Orange România had concluded contracts for the provision of mobile telecommunications services containing a clause which stated that customers had been informed and had consented to the collection and retention of a copy of their identity document for identification purposes. The box relating to this clause had been checked by the data controller before signing the contract.

It is in this context that the Tribunalul București (Regional Court, Bucharest, Romania) asked the Court to specify the conditions under which the consent of clients to the processing of personal data can be considered as being valid.

First of all, the Court points out that EU law [31] provides for a list of cases in which the processing of personal data may be considered to be lawful. In particular, the consent of the data subject

[31] Article 7 of Directive 95/16 and article 6 of the GDPR.

must be freely given, specific, informed and unambiguous [32]. In this regard, consent is not validly given in the event of silence, boxes ticked by default or inactivity (paragraphs 34, 36, 37 and 39).

In addition, when the consent of the data subject is given in the context of a written declaration, which also concerns other matters, this declaration must be presented in an understandable and easily accessible form and be formulated in clear and simple terms. 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 (paragraphs 34, 36, 37, 39 and 41).

The Court specifies that Orange România, being the controller of the processing of personal data, must be able to demonstrate the lawfulness of the processing of such data and, therefore, in this case, the existence of a valid consent of its clients. In this regard, given that the customers concerned do not appear to have themselves checked the box relating to the collection and retention of copies of their identity document, the mere fact that this box has been checked is not such as to establish a positive indication of their consent. It is for the national court to carry out the checks necessary for this purpose (paragraphs 42 and 46).

It is also for the national court to assess whether or not the contractual provisions in question were liable to mislead the customers concerned as to the possibility of concluding the contract notwithstanding a refusal to consent to the processing of their data, in the absence of details on this possibility. In addition, in the event of a client's refusal to consent to the processing of his or her data, the Court observes that Orange România required that the latter declare in writing that he or she did not consent to the collection or retention of the copy of his or her identity document. According to the Court, such an additional requirement is liable to unduly affect the freedom to choose to object to such collection and storage. In any event, as the company is required to establish that its customers have, by active behavior, given their consent to the processing of their personal data, this company cannot require them to actively express their refusal (paragraphs 49 to 51).

The Court therefore concludes that a contract relating to the supply of telecommunications services which contains a clause according to which the data subject has been informed and has consented to the collection and storage of a copy of his or her identity document for identification purposes is not such as to demonstrate that this person has validly given their consent to this collection and storage, in circumstances where the box referring to this clause has been checked by the data controller before the signing of the contract, the contractual provisions of this contract are likely to mislead the data subject into error as to the possibility of concluding the contract in question even if he or she refuses to consent to the processing of his or her data, or where the free choice as to whether to oppose this collection and storage is unduly affected by that controller by requiring the data subject to complete, in order to express his or her refusal to give their consent to such processing, an additional form setting out such refusal (paragraph 52 and operative part).

[32] Article 2(h) of Directive 95/46 and article 4(11) of the GDPR

Judgment of 12 May 2021 (Grand Chamber), Bundesrepublik Deutschland (Interpol red notice) (C-505/19, EU:C2021:376)

In 2012, the International Criminal Police Organisation ('Interpol') published, at the request of the United States and on the basis of an arrest warrant issued by the authorities of that country, a red notice in respect of WS, a German national, with a view to his potential extradition. Where a person who is the subject of such a notice is located in a State affiliated to Interpol, that State must, in principle, provisionally arrest that person or monitor or restrict his or her movements.

However, even before that red notice was published, a procedure investigating WS, which related, according to the referring court, to the same acts as those which formed the basis for that notice, had been carried out in Germany. That procedure was definitively discontinued in 2010 after a sum of money had been paid by WS as part of a specific settlement procedure provided for under German criminal law. The Bundeskriminalamt (Federal Criminal Police Office, Germany) subsequently informed Interpol that, in its view, as a result of that earlier procedure, the *ne bis in idem* principle was applicable in the present case. That principle, which is enshrined in both Article 54 of the Convention implementing the Schengen Agreement [33] and Article 50 of the Charter, prohibits, inter alia, a person whose trial has been finally disposed of from being prosecuted again for the same offence.

In 2017, WS brought an action against the Federal Republic of Germany before the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany) seeking an order requiring that Member State to take the measures necessary to arrange for that red notice to be withdrawn. In that regard, WS relies not only on an infringement of the *ne bis in idem* principle, but also on an infringement of his right to freedom of movement, as guaranteed under Article 21 TFEU, since he cannot travel to any State that is a party to the Schengen Agreement or to any Member State without risking arrest. He also argues that, due to those infringements, the processing of his personal data appearing in the red notice is contrary to Directive 2016/680, which concerns the protection of personal data in criminal matters. [34]

That is the context in which the Administrative Court, Wiesbaden decided to ask the Court about how the *ne bis in idem* principle is to be applied and, specifically, whether it is possible provisionally to arrest a person who is the subject of a red notice in a situation such as the one at issue. Furthermore, in the event that that principle does apply, the referring court wishes to know what the consequences are for the processing, by Member States, of the personal data contained in such a notice.

In its Grand Chamber judgment, the Court finds, *inter alia*, that the provisions of Directive 2016/680, read in the light of Article 54 of the CISA and Article 50 of the Charter, must be interpreted as not precluding the processing of personal data appearing in a red notice issued

[33] Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders (OJ 2000 L 239, p. 19; 'the CISA').

[34] 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 (OJ 2016 L 119, p. 89).

by Interpol in the case where it has not been established, by means of such a judicial decision, that the *ne bis in idem* principle applies in respect of the acts on which that notice is based, provided that such processing satisfies the conditions laid down by that directive (paragraph 121 and operative part 2).

As regards the matter of personal data appearing in an Interpol red notice, the Court notes that any operation performed on that data, such as registering them in a Member State's list of wanted persons, constitutes 'processing' which falls under Directive 2016/680. [35] Additionally, the Court finds, first, that that processing pursues a legitimate objective and, second, that it cannot be regarded as unlawful solely on the ground that the *ne bis in idem* principle may apply to the acts on which that red notice is based. [36] That processing, by the authorities of the Member States, may indeed be indispensable precisely in order to determine whether that principle applies (paragraphs 111, 114, 116, 117 and 119).

In those circumstances, the Court also finds that Directive 2016/680, read in the light of Article 54 of the CISA and Article 50 of the Charter, does not preclude the processing of personal data appearing in a red notice where no final judicial decision has established that the *ne bis in idem* principle applies in the relevant case. However, such processing must be carried out in compliance with the conditions laid down by that directive. In that respect, it must, inter alia, be necessary for the performance of a task carried out by a competent national authority for purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties [37] (paragraph 121 and operative part 2).

By contrast, where the *ne bis in idem* principle does apply, the recording, in the Member States' lists of wanted persons, of the personal data contained in an Interpol red notice is no longer necessary, because the person concerned can no longer be the subject of criminal proceedings in respect of the acts covered by that notice and, consequently, cannot be arrested for those same acts. It follows that the data subject must be able to request that his or her data be erased. If, nevertheless, those data remain recorded, they must be accompanied by a note to the effect that the person in question can no longer be prosecuted in a Member State or in a State that is a party to the Schengen Agreement for the same acts by reason of the *ne bis in idem* principle (paragraph 120).

Judgment of 22 June 2021 (Grand Chamber), Latvijas Republikas Saeima (Penalty points) (C-439/19, EU:C:2021:504)

By its judgment (see also Section II.3., entitled "Concept of 'processing of personal data'"), the Court holds that the GDPR precludes Latvian legislation which obliges the Ceļu satiksmes drošības direkcija (Road Safety Directorate, Latvia) ('the CSDD') to make the data relating to the penalty points imposed on drivers of vehicles for road traffic offences accessible to the public, without the person requesting access having to establish a specific interest in obtaining the data. It notes that it has not been established that disclosure of personal data relating to the

35 See Article 2(1) and Article 3(2) of Directive 2016/680.
36 See Article 4(1)(b) and Article 8(1) of Directive 2016/680.
37 See Article 1(1) and Article 8(1) of Directive 2016/680.

penalty points imposed for road traffic offences is necessary, particularly with regard to the objective of improving road safety invoked by the Latvian Government. Furthermore, according to the Court, neither the right of public access to official documents nor the right to freedom of information justify such legislation (paragraphs 113, 120 to 122 and operative part 2).

In that regard, the Court points out that the improvement of road safety, referred to in the Latvian legislation, is an objective of general interest recognised by the European Union and that Member States are therefore justified in classifying road safety as a 'task carried out in the public interest'. [38] However, it is not established that the Latvian scheme of disclosing personal data relating to penalty points is necessary to achieve the objective pursued. First, the Latvian legislature has a large number of methods which would have enabled it to achieve that objective by other means less restrictive of the fundamental rights of the persons concerned. Second, account must be taken of the sensitivity of the data relating to penalty points and of the fact that their public disclosure is liable to constitute a serious interference with the rights to respect for private life and to the protection of personal data, since it may give rise to social disapproval and result in stigmatisation of the data subject (paragraphs 109 to 113).

Furthermore, the Court takes the view that, in the light of the sensitivity of those data and of the seriousness of that interference with those two fundamental rights, those rights prevail over both the public's interest in having access to official documents, such as the national register of vehicles and their drivers, and the right to freedom of information (paragraphs 120 and 121).

In addition, for the same reasons, the Court holds that the GDPR also precludes Latvian legislation in so far as it authorises the CSDD to disclose the data on penalty points imposed on drivers of vehicles for road traffic offences to economic operators in order for the data to be re-used and disclosed to the public by them (paragraph 126 and operative part 3).

Lastly, the Court states that the principle of the primacy of EU law precludes the referring court, before which the action has been brought challenging the Latvian legislation, classified by the Court as incompatible with EU law, from deciding that the legal effects of that legislation be maintained until the date of delivery of its final judgment (paragraph 137 and operative part 4).

III. The processing of personal data within the meaning of Directive 2002/58

Judgment of 2 October 2018 (Grand Chamber), Ministerio Fiscal (C-207/16, EU:C:2018:788) [39]

At issue in the main proceedings was the refusal by a Spanish investigating magistrate to grant a request made in the context of an investigation into the robbery of a wallet and mobile

[38] Under Article 6(1)(e) of the GDPR, the processing of personal data is lawful where it is 'necessary for the performance of a task carried out in the public interest […]'.

[39] This judgment was included in the 2018 Annual Report, p. 88 and 89.

telephone. In particular, the police had asked the investigating magistrate to grant access, over a period of 12 days from the date of the robbery, to data identifying the users of telephone numbers activated with the stolen telephone. The refusal had been based on the reasoning that that the acts giving rise to the criminal investigation did not constitute a 'serious' offence — that is to say, an offence punishable under Spanish law by a term of imprisonment of more than five years — access to identification data being possible only in respect of that category of offences.

After pointing out that the access of public authorities to personal data retained by providers of electronic communications services in connection with a criminal investigation comes within the scope of Directive 2002/58, the Court held that the access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners of the SIM cards, constitutes an interference with the fundamental right to respect for private life and the fundamental right to the protection of personal data enshrined in the Charter, even in the absence of circumstances which would allow that interference to be defined as 'serious', without it being relevant that the information in question relating to private life is sensitive or whether the persons concerned have been inconvenienced in any way as a result of that interference. However, the Court made clear that such interference is not sufficiently serious to require that access to be limited, in the area of prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime. Although Directive 2002/58 contains an exhaustive list of the objectives capable of justifying national legislation governing the access of public authorities to the data concerned and thereby derogating from the principle of confidentiality of electronic communications, it being necessary for such access to correspond, genuinely and strictly, to one of those objectives, the Court observed that as regards the objective of preventing, investigating, detecting and prosecuting criminal offences, the wording of Directive 2002/58 does not limit that objective to the fight against serious crime alone, but refers to 'criminal offences' generally (paragraphs 38, 42, 59 to 63, and operative part).

Against that background, the Court stated that although, in its judgment in *Tele2 Sverige and Watson and Others* [40], it had held that only the objective of fighting serious crime is capable of justifying the access of public authorities to personal data retained by providers of communications services which, taken as a whole, allow precise conclusions to be drawn concerning the private lives of the persons whose data are concerned, that interpretation was based on the fact that the objective pursued by legislation governing that access must be proportionate to the seriousness of the interference with the fundamental rights in question which that access entails. Thus, having regard to the principle of proportionality, a serious interference can be justified, in this field, only by the objective of fighting crime which must also be defined as 'serious'. By contrast, when the interference is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally (paragraphs 54 to 57).

As regards the case in hand, the Court took the view that access to only the data referred to in the request at issue could not be defined as a 'serious' interference with the fundamental rights of the persons whose data are concerned, as those data do not allow precise conclusions to be

[40] Judgment of the Court of 21 December 2016, Tele2 Sverige and Watson and Others (C–203/15 and C–698/15, EU:C:2016:970).

drawn in respect of their private lives. The Court concluded that the interference that access to such data entails is therefore capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally, without it being necessary that those offences be defined as 'serious' (paragraphs 61 and 62).

Judgments of 6 October 2020 (Grand Chamber), Privacy International (C-623/17, EU:C:2020:790) and La Quadrature du Net and Others (C-511/18, C-512/18 et C-520/18, EU:C:2020:791) [41]

The case-law relating to the retention of and access to personal data in the field of electronic communications, in particular the judgment in *Tele2 Sverige* and *Watson and Others*, in which the Court held, inter alia, that Member States could not impose an obligation on providers of electronic communications services to retain traffic data and location data in a general and indiscriminate way, has caused concerns on the part of certain States that they may have been deprived of an instrument which they consider necessary to safeguard national security and to combat crime.

It is against that background that proceedings were brought before the Investigatory Powers Tribunal (United Kingdom) (*Privacy International*, C-623/17), the Conseil d'État (Council of State, France) (*La Quadrature du Net and Others*, Joined Cases C-511/18 and C-512/18) and the Cour constitutionnelle (Constitutional Court, Belgium) (*Ordre des barreaux francophones et germanophone and Others*, C-520/18) concerning the lawfulness of legislation adopted by certain Member States in those fields, laying down in particular an obligation for providers of electronic communications services to forward users' traffic data and location data to a public authority or to retain such data in a general or indiscriminate way.

By two Grand Chamber judgments delivered on 6 October 2020, the Court rules, first of all, that national legislation requiring providers of electronic communications services to retain traffic data and location data or to forward that data to the national security and intelligence authorities for that purpose falls within the scope of Directive 2002/58 (paragraph 49, operative part 1 of the judgment *Privacy International* and paragraph 104 of the judgment *La Quadrature du Net and Others*).

Next, the Court recalls that Directive 2002/58 [42] does not permit the exception to the obligation in principle to ensure the confidentiality of electronic communications, data relating thereto and the prohibition on storage of such data becoming the rule. This means that the directive does not authorise the Member States to adopt, inter alia for the purposes of national security, legislative measures intended to restrict the scope of rights and obligations provided for in that directive, in particular the obligation to ensure the confidentiality of communications and traffic data, [43] unless such measures comply with the general principles of EU law, including the principle of proportionality, and the fundamental rights guaranteed by the Charter [44]

41 These judgments were included in the 2020 Annual Report, p. 29 to 32
42 Article 15(1) and (3) of Directive 2002/58.
43 Article 5(1) of Directive 2002/58.
44 In particular, Articles 7, 8 and 11 and Article 52(1) of the Charter.

(paragraphs 59 and 60 of the judgment *Privacy International* and paragraphs 111 and 113 of the judgment *La Quadrature du Net and Others*).

In that context, the Court holds, first, in the *Privacy International* case, that Directive 2002/58, read in the light of the Charter, precludes national legislation requiring providers of electronic communications services to carry out the general and indiscriminate transmission of traffic data and location data to the security and intelligence agencies for the purpose of safeguarding national security. Secondly, in Joined Cases *La Quadrature du Net and Others* and in *Ordre des barreaux francophones et germanophone and Others*, the Court finds that the same directive precludes legislative measures requiring providers of electronic communications services to carry out the general and indiscriminate retention of traffic data and location data as a preventive measure.

Indeed, those obligations to forward and to retain such data in a general and indiscriminate way constitute particularly serious interferences with the fundamental rights guaranteed by the Charter, where there is no link between the conduct of the persons whose data is affected and the objective pursued by the legislation at issue. Similarly, the Court interprets Article 23(1) of the GDPR read in the light of the Charter, as precluding national legislation requiring providers of access to online public communication services and hosting service providers to retain, generally and indiscriminately, inter alia, personal data relating to those services (paragraphs 71, 82 and operative part 2 of the judgment *Privacy International* and paragraphs 146, 168, 174, 177, 212, operative part 1 and 3 of the judgment *La Quadrature du Net and Others*).

By contrast, the Court holds that, in situations where the Member State concerned is facing a serious threat to national security that proves to be genuine and present or foreseeable, Directive 2002/58, read in the light of the Charter, does not preclude recourse to an order requiring providers of electronic communications services to retain, generally and indiscriminately, traffic data and location data. In that context, the Court specifies that the decision imposing such an order, for a period that is limited in time to what is strictly necessary, must be subject to effective review either by a court or by an independent administrative body whose decision is binding, in order to verify that one of those situations exists and that the conditions and safeguards laid down are observed. In those circumstances, that directive also does not preclude the automated analysis of the data, inter alia traffic and location data, of all users of means of electronic communication (paragraphs 137 to 139, 177 to 179, operative part 1 and 2 of the judgment *La Quadrature du Net and Others*).

The Court adds that Directive 2002/58, read in the light of the Charter, does not preclude legislative measures that allow recourse to the targeted retention, limited in time to what is strictly necessary, of traffic and location data, which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion. Likewise, that directive does not preclude legislative measures that provide for the general and indiscriminate retention of IP addresses assigned to the source of a communication, provided that the retention period is limited to what is strictly necessary, or measures that provide for such retention of data relating to the civil identity of users of electronic communication systems, the Member States not being required in the latter case to

limit the retention period. Moreover, that directive does not preclude a legislative measure that allows recourse to the expedited retention of data available to service providers, where situations arise in which it becomes necessary to retain that data beyond statutory data retention periods in order to shed light on serious criminal offences or attacks on national security, where such offences or attacks have already been established or where their existence may reasonably be suspected (paragraphs 161, 163, 168 and operative part 1 of the judgment *La Quadrature du Net and Others*).

In addition, the Court rules that Directive 2002/58, read in the light of the Charter, does not preclude national legislation which requires providers of electronic communications services to have recourse to real-time collection, inter alia, of traffic data and location data, where that collection is limited to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities and is subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding, to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In urgent cases, the review must take place promptly (paragraph 192 and operative part 2 of the judgment *La Quadrature du Net and Others*).

Lastly, the Court addresses the issue of maintaining the temporal effects of national legislation held to be incompatible with EU law. In that regard, it rules that a national court may not apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality which it is bound to make in respect of national legislation imposing on providers of electronic communications services an obligation requiring the general and indiscriminate retention of traffic and location data that is incompatible with Directive 2002/58, read in the light of the Charter.

That being said, in order to give a useful answer to the referring court, the Court of Justice recalls that, as EU law currently stands, it is for national law alone to determine the rules relating to the admissibility and assessment, in criminal proceedings against persons suspected of having committed serious criminal offences, of information and evidence obtained by the retention of data in breach of EU law. However, the Court specifies that Directive 2002/58, interpreted in the light of the principle of effectiveness, requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of such criminal proceedings, where those persons suspected of having committed criminal offences are not in a position to comment effectively on that information and evidence (paragraphs 222, 228 and operative part 4 of the judgment *La Quadrature du Net and Others*).

Judgment of 2 March 2021 (Grand Chamber), Prokuratuur (Conditions of access to data relating to electronic communications) (C-746/18, EU:C:2021:152)

Criminal proceedings were brought in Estonia against H. K. on counts of theft, use of another person's bank card and violence against persons party to court proceedings. A court of first

instance convicted H. K. of those offences and imposed a custodial sentence of two years. That judgment was then upheld on appeal.

The reports relied upon in order to find H. K. guilty of those offences were drawn up, inter alia, on the basis of personal data generated in the context of the provision of electronic communications services. The Riigikohus (Supreme Court, Estonia), before which H. K. lodged an appeal on a point of law, expressed doubts as to whether the conditions under which the investigating authority had access to those data were compatible with EU law [45].

Those doubts concerned, first, whether the length of the period in respect of which the investigating authority has had access to the data is a criterion for assessing the seriousness of the interference, constituted by that access, with the fundamental rights of the persons concerned. Thus, the referring court raised the question whether, where that period is very short or the quantity of data gathered is very limited, the objective of combating crime in general, and not only combating serious crime, is capable of justifying such an interference. Second, the referring court had doubts as to whether it is possible to regard the Estonian public prosecutor's office, in the light of the various duties which are assigned to it by national legislation, as an 'independent' administrative authority, within the meaning of the judgment in *Tele2 Sverige and Watson and Others*, [46] that is capable of authorising access of the investigating authority to the data concerned.

By its judgment, delivered by the Grand Chamber, the Court holds that Directive 2002/58, read in the light of the Charter, precludes national legislation that permits public authorities to have access to traffic or location data, that are liable to provide information regarding the communications made by a user of a means of electronic communication or regarding the location of the terminal equipment which he or she uses and to allow precise conclusions to be drawn concerning his or her private life, for the purposes of the prevention, investigation, detection and prosecution of criminal offences, without such access being confined to procedures and proceedings to combat serious crime or prevent serious threats to public security. According to the Court, the length of the period in respect of which access to those data is sought and the quantity or nature of the data available in respect of such a period are irrelevant in that regard. The Court further holds that that directive, read in the light of the Charter, precludes national legislation that confers upon the public prosecutor's office the power to authorise access of a public authority to traffic and location data for the purpose of conducting a criminal investigation (paragraphs 45, 59 and operative part 1 and 2).

So far as concerns the objective of preventing, investigating, detecting and prosecuting criminal offences, which is pursued by the legislation at issue, in accordance with the principle of proportionality the Court holds that only the objectives of combating serious crime or preventing serious threats to public security are capable of justifying public authorities having access to a set of traffic or location data, that are liable to allow precise conclusions to be drawn concerning the private lives of the persons concerned. Other factors relating to the proportionality of a request for access, such as the length of the period in respect of which

[45] To be more precise, with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter

[46] Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraph 120).

access to such data is sought, cannot have the effect that the objective of preventing, investigating, detecting and prosecuting criminal offences in general is capable of justifying such access (paragraphs 33 and 35).

As regards the power conferred upon the public prosecutor's office to authorise access of a public authority to traffic and location data for the purpose of conducting a criminal investigation, the Court points out that it is for national law to determine the conditions under which providers of electronic communications services must grant the competent national authorities access to the data in their possession. However, in order to satisfy the requirement of proportionality, such legislation must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards, so that the persons whose personal data are affected have sufficient guarantees that data will be effectively protected against the risk of abuse. That legislation must be legally binding under domestic law and must indicate in what circumstances and under which substantive and procedural conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary (paragraph 48).

According to the Court, in order to ensure, in practice, that those conditions are fully observed, it is essential that access of the competent national authorities to retained data be subject to a prior review carried out either by a court or by an independent administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime. In cases of duly justified urgency, the review must take place within a short time (paragraph 51).

In that regard, the Court states that one of the requirements for the prior review is that the court or body entrusted with carrying it out must have all the powers and provide all the guarantees necessary in order to reconcile the various interests and rights at issue. As regards a criminal investigation in particular, it is a requirement of such a review that that court or body must be able to strike a fair balance between, on the one hand, the interests relating to the needs of the investigation in the context of combating crime and, on the other, the fundamental rights to privacy and protection of personal data of the persons whose data are concerned by the access. Where that review is carried out not by a court but by an independent administrative body, that body must have a status enabling it to act objectively and impartially when carrying out its duties and must, for that purpose, be free from any external influence (paragraphs 52 and 53).

According to the Court, it follows that the requirement of independence that has to be satisfied by the authority entrusted with carrying out the prior review means that that authority must be a third party in relation to the authority which requests access to the data, in order that the former is able to carry out the review objectively and impartially and free from any external influence. In particular, in the criminal field the requirement of independence entails that the authority entrusted with the prior review, first, must not be involved in the conduct of the criminal investigation in question and, second, has a neutral stance vis-à-vis the parties to the criminal proceedings. That is not so in the case of a public prosecutor's office which, like the

Estonian public prosecutor's office, directs the investigation procedure and, where appropriate, brings the public prosecution. It follows that the public prosecutor's office is not in a position to carry out the prior review (paragraphs 54, 55 and 57).

IV. Transfer of personal data to third countries

Judgment of 6 November 2003 (Grand Chamber), Lindqvist (C-101/01, EU:C:2003:596) [47]

In this case (see also Section II.3. 'Concept of "processing of personal data"'), the referring court sought, in particular, to establish whether Mrs Lindqvist had carried out a transfer of data to a third country within the meaning of that directive.

The Court held that there is no 'transfer [of data] to a third country' within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored on an internet site on which the page can be consulted and which is hosted by a natural or legal person who is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country (paragraph 71 and operative part 4).

Given, first, the state of development of the internet at the time when Directive 95/46 was drawn up and, second, the absence of criteria applicable to use of the internet in Chapter IV in which Article 25 appears and which is intended to allow the Member States to monitor transfers of personal data to third countries and to prohibit such transfers where those countries do not offer an adequate level of protection, it cannot be presumed that the Community legislature intended the expression 'transfer [of data] to a third country' to cover such loading 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 (paragraphs 63, 64 and 68).

Judgment of 6 October 2015 (Grand Chamber), Schrems (C-362/14, EU:C:2015:650) [48]

Mr Schrems, an Austrian citizen and user of the Facebook social network, had made a complaint to Ireland's Data Protection Commissioner on the ground that Facebook Ireland was transferring the personal data of its users to the United States and retaining those data on servers in the United States, where the data were processed. According to Mr Schrems, United States law and practice did not provide adequate protection against surveillance by the public authorities of data transferred to that country. The Data Protection Commissioner had refused to investigate the complaint on the ground, in particular, that the Commission had, in Decision

[47] This judgment was included in the 2003 Annual Report, p. 67.
[48] This judgment was included in the 2015 Annual Report, p. 53.

2000/520/EC [49], found that, in the context of the 'safe harbour' regime [50], the United States ensured an adequate level of protection for the personal data transferred.

It is against that background that a request was made to the Court by the High Court (Ireland) for interpretation of Article 25(6) of Directive 95/46, under which the Commission may find that a third country ensures a level of protection that is adequate for the data transferred, together with, in essence, a request for determination of the validity of Decision 2000/520, which was adopted by the Commission on the basis of Article 25(6) of Directive 95/46.

The Court declared the Commission's decision invalid in its entirety, stating, first of all, that its adoption required a duly reasoned finding by the Commission that the third country concerned does in fact ensure a level of protection of fundamental rights essentially equivalent to that guaranteed in the EU legal order. Since the Commission did not so find in Decision 2000/520, Article 1 of that decision fails to comply with the requirements laid down in Article 25(6) of Directive 95/46, read in the light of the Charter, and is accordingly invalid. Indeed, the 'safe harbour' principles are applicable solely to self-certified United States organisations receiving personal data from the European Union, and United States public authorities are not required to comply with them. Moreover, Decision 2000/520 enables interference with the fundamental rights of the persons whose personal data are or could be transferred from the European Union to the United States, without containing any finding regarding the existence, in the United States, of rules adopted by the State intended to limit any interference with those rights and without referring to the existence of effective legal protection against interference of that kind (paragraphs 82, 87 to 89, 96 to 98 and operative part 2).

In addition, the Court declared Article 3 of Decision 2000/520 to be invalid in so far as it denied the national supervisory authorities the powers which they derive from Article 28 of Directive 95/46, where a person puts forward matters that may call into question whether a Commission decision that has found that a third country ensures an adequate level of protection is compatible with the protection of the privacy and of the fundamental rights and freedoms of individuals (paragraphs 102 to 104). The Court concluded that the invalidity of Articles 1 and 3 of Decision 2000/520 affected the validity of that decision in its entirety (paragraphs 105 and 106).

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

---

[49] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000, L 215, p. 7).

[50] The safe harbour regime consists of a set of principles on the protection of personal data to which United States undertakings can subscribe voluntarily.

Furthermore and above all, protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary (paragraph 92). Thus, legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data have been transferred from the European Union without any differentiation, limitation or exception being made in the light of the objective pursued, and without any objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of the subsequent use of those data, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to those data and their use entail (paragraph 93). In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications compromises the essence of the fundamental right to respect for private life. Likewise, 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 (paragraphs 94 and 95).

Opinion 1/15 (EU-Canada PNR Agreement) of 26 July 2017 (Grand Chamber) (EU:C:2017:592)

On 26 July 2017, the Court delivered its first ruling on the compatibility of a draft international agreement with the Charter of Fundamental Rights of the European Union, and, in particular, with provisions relating to respect for private life and the protection of personal data.

The European Union and Canada negotiated an agreement on the transfer and processing of Passenger Name Record data (PNR Agreement) which was signed in 2014. The Council of the European Union having requested the European Parliament's approval of the agreement, the European Parliament decided to refer the matter to the Court in order to ascertain whether the envisaged agreement was compatible with EU law.

The envisaged agreement permits the systematic and continuous transfer of PNR data of all air passengers to a Canadian authority with a view to those data being used and retained, and possibly transferred subsequently to other authorities and to other third countries, for the purpose of combating terrorism and serious transnational crime. To that end, the envisaged agreement, amongst other things, provides for a data storage period of five years and lays down particular requirements in relation to PNR data security and integrity, such as immediate masking of sensitive data, whilst also providing for rights of access to and correction and erasure of data, and for the possibility of administrative and judicial redress.

The PNR data covered by the envisaged agreement include, inter alia, besides the name(s) of the air passenger(s) and contact information: information necessary to the reservation, such as the dates of intended travel and the travel itinerary, information relating to tickets, groups of persons checked-in under the same reservation numbers, information relating to the means of payment or billing, information concerning baggage and general remarks regarding the passengers.

The ruling given by the Court in the Opinion was that the PNR Agreement could not be concluded in its current form because several of its provisions were incompatible with the fundamental rights recognised by the European Union.

The Court found, in the first place, that both the transfer of PNR data from the European Union to the Canadian competent authority and the framework negotiated by the European Union with Canada of the conditions concerning the retention of those data, their use and their subsequent transfer to other Canadian authorities, Europol, Eurojust, judicial or police authorities of the Member States or indeed to authorities of other third countries constitute interferences with the right guaranteed in Article 7 of the Charter. Those operations also constitute an interference with the fundamental right to the protection of personal data guaranteed in Article 8 of the Charter since they constitute the processing of personal data (paragraphs 125 and 126).

Furthermore, the Court emphasised that even if some of the PNR data, taken in isolation, do not appear to be liable to reveal important information about the private life of the persons concerned, the fact remains that, taken as a whole, the data may, inter alia, reveal a complete travel itinerary, travel habits, relationships existing between air passengers and the financial situation of air passengers, their dietary habits or state of health, and may even provide sensitive information about those passengers, as defined in Article 2(e) of the envisaged agreement (information that reveals racial or ethnic origin, political opinions, religious beliefs, etc.) (paragraph 128).

In this connection, the Court considered that, although the interferences in question could be justified by the pursuit of an objective of general interest (to ensure public security in the context of the fight against terrorist offences and serious transnational crime), several provisions of the agreement were not limited to what is strictly necessary and did not lay down clear and precise rules.

In particular, the Court pointed out that, having regard to the risk of processing contrary to the principle of non-discrimination, a transfer of sensitive data to Canada requires a precise and particularly solid justification, based on grounds other than the protection of public security against terrorism and serious transnational crime. In this instance, however, there was no such justification. The Court concluded from this that the provisions of the agreement on the transfer of sensitive data to Canada and on the processing and retention of those data were incompatible with fundamental rights (paragraphs 165 and 232).

In the second place, the Court found that the continued storage of the PNR data of all air passengers after their departure from Canada, which the envisaged agreement permits, was not limited to what is strictly necessary. As regards air passengers in respect of whom no risk has been identified as regards terrorism or serious transnational crime on their arrival in Canada and up to their departure from that country, there would not appear to be, once they have left, any connection — even a merely indirect connection — between their PNR data and the objective pursued by the envisaged agreement which would justify those data being retained. By contrast, in the case of air passengers in respect of whom there is objective evidence from

which it may be inferred that they may present a risk in terms of the fight against terrorism and serious transnational crime even after their departure from Canada, the storage of their PNR data is permissible beyond their stay in Canada, even for a period of five years (paragraphs 205 to 207 and 209).

In the third place, the Court held that the fundamental right to respect for private life, enshrined in Article 7 of the Charter, means that the person concerned may be certain that his personal data are processed in a correct and lawful manner. In order to carry out the necessary checks, that person must have a right of access to the data relating to him which are being processed.

The Court pointed out in that regard that, in the envisaged agreement, air passengers must be notified of the transfer of their PNR data to the third country concerned and of the use of those data as soon as that information is no longer liable to jeopardise the investigations being carried out by the government authorities referred to in the envisaged agreement. That information is, in fact, necessary to enable the air passengers to exercise their rights to request access to data concerning them and, if appropriate, rectification of those data, and, in accordance with the first paragraph of Article 47 of the Charter, to an effective remedy before a tribunal.

Consequently, in the situations in which there is objective evidence justifying the use of the PNR data in order to combat terrorism and serious transnational crime and necessitating the prior authorisation of a judicial authority or an independent administrative body, it is necessary to notify air passengers individually. The same is true in the cases in which air passengers' PNR data are disclosed to other government authorities or to individuals. However, that information must be provided only once it is no longer liable to jeopardise the investigations being carried out by the government authorities referred to in the envisaged agreement (paragraphs 219, 220, 223 and 224).

Judgment of 16 July 2020 (Grand Chamber), Facebook Ireland and Schrems (C-311/18, ECLI:EU:C:2020:559) [51]

The GDPR provides that the transfer of such data to a third country may, in principle, take place only if the third country in question ensures an adequate level of data protection. According to the GDPR, the Commission may find that a third country ensures, by reason of its domestic law or its international commitments, an adequate level of protection. [52] In the absence of an adequacy decision, such a transfer may take place only if the personal data exporter established in the European Union has provided appropriate safeguards, which may arise, in particular, from standard data protection clauses adopted by the Commission, and if data subjects have enforceable rights and effective legal remedies. [53] Furthermore, the GDPR details the conditions under which such a transfer may take place in the absence of an adequacy decision or appropriate safeguards. [54]

51 This judgment was included in the 2020 Annual Report, p. 26 to 29.
52 Article 45 of the GDPR.
53 Article 46(1) and (2)(c) of the GDPR.
54 Article 49 of the GDPR.

Maximillian Schrems, an Austrian national residing in Austria, has been a Facebook user since 2008. As in the case of other users residing in the European Union, some or all of Mr Schrems's personal data are transferred by Facebook Ireland to servers belonging to Facebook Inc. that are located in the United States, where they undergo processing. Mr Schrems lodged a complaint with the Irish supervisory authority seeking, in essence, to prohibit those transfers. He claimed that the law and practices in the United States do not offer sufficient protection against access by the public authorities to the data transferred to that country. That complaint was rejected on the ground, inter alia, that, in Decision 2000/520 [55], the Commission had found that the United States ensured an adequate level of protection. In a judgment delivered on 6 October 2015, the Court, before which the High Court (Ireland) had referred questions for a preliminary ruling, declared that decision invalid ('the Schrems I judgment') [56] (paragraphs 52 and 53).

Following the Schrems I judgment and the subsequent annulment by the referring court of the decision rejecting Mr Schrems's complaint, the Irish supervisory authority asked Mr Schrems to reformulate his complaint in the light of the declaration by the Court that Decision 2000/520 was invalid. In his reformulated complaint, Mr Schrems claims that the United States does not offer sufficient protection of data transferred to that country. He seeks the suspension or prohibition of future transfers of his personal data from the European Union to the United States, which Facebook Ireland now carries out pursuant to the standard data protection clauses set out in the Annex to Decision 2010/87/EU. [57] Taking the view that the outcome of Mr Schrems's complaint depends, in particular, on the validity of Decision 2010/87, the Irish supervisory authority brought proceedings before the High Court in order for it to refer questions to the Court for a preliminary ruling. After the initiation of those proceedings, the Commission adopted Decision 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield [58] (paragraphs 54, 55 and 57).

By its request for a preliminary ruling, the referring court asked the Court whether the GDPR applies to transfers of personal data pursuant to the standard data protection clauses in Decision 2010/87, what level of protection is required by the GDPR in connection with such a transfer and what obligations are incumbent on supervisory authorities in those circumstances. The High Court also raised the question of the validity both of Decision 2010/87 and of Decision 2016/1250.

The Court found that examination of Decision 2010/87 in the light of the Charter of Fundamental Rights of the European Union ('the Charter') disclosed nothing to affect the validity of that decision. However, the Court declared Decision 2016/1250 invalid (operative part 4 and 5).

---

55 Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).

56 Judgment of the Court of 6 October 2015, *Schrems*, C-362/14 (see, also, CP Nº 117/15).

57 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ 2010 L 39, p. 5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100).

58 Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (OJ 2016 L 207, p. 1).

The Court considered, first of all, that EU law, and in particular the GDPR, applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, even if, at the time of that transfer or thereafter, that data may be processed by the authorities of the third country in question for the purposes of public security, defence and State security. The Court added that this type of data processing by the authorities of a third country cannot preclude such a transfer from the scope of the GDPR (paragraphs 86, 88, 89 and operative part 1).

Regarding the level of protection required in respect of such a transfer, the Court held that the requirements laid down for such purposes by the GDPR concerning appropriate safeguards, enforceable rights and effective legal remedies must be interpreted as meaning that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses must be afforded a level of protection essentially equivalent to that guaranteed within the European Union by the GDPR, read in the light of the Charter. In those circumstances, the Court specified that the assessment of that level of protection must take into consideration both the contractual clauses agreed between the data exporter established in the European Union and the recipient of the transfer established in the third country concerned and, as regards any access by the public authorities of that third country to the data transferred, the relevant aspects of the legal system of that third country (paragraph 105 and operative part 2).

Regarding the supervisory authorities' obligations in connection with such a transfer, the Court held that, unless there is a valid Commission adequacy decision, those competent supervisory authorities are required to suspend or prohibit a transfer of personal data to a third country where they take the view, in the light of all the circumstances of that transfer, that the standard data protection clauses are not or cannot be complied with in that country and that the protection of the data transferred that is required by EU law cannot be ensured by other means, where the data exporter established in the European Union has not itself suspended or put an end to such a transfer (paragraph 121 and operative part 3).

Next, the Court examined the validity of Decision 2010/87. The Court considered that the validity of that decision was not called into question by the mere fact that the standard data protection clauses in that decision do not, given that they are contractual in nature, bind the authorities of the third country to which data may be transferred. However, that validity, the Court added, depends on whether the decision includes effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them. The Court found that Decision 2010/87 establishes such mechanisms. In that regard, the Court pointed out, in particular, that that decision imposes an obligation on a data exporter and the recipient of the data to verify, prior to any transfer, whether that level of protection is respected in the third country concerned and that the decision requires the recipient to inform the data exporter of any inability to comply with the standard data protection clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the former (paragraphs 132, 136, 137, 142, 148 and operative part 4).

Lastly, the Court examined the validity of Decision 2016/1250 in the light of the requirements arising from the GDPR, read in the light of the provisions of the Charter guaranteeing respect for private and family life, personal data protection and the right to effective judicial protection. In that regard, the Court noted that that decision enshrines the position, as did Decision 2000/520, that the requirements of US national security, public interest and law enforcement have primacy, thus condoning interference with the fundamental rights of persons whose data are transferred to that third country. In the view of the Court, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to that third country, which the Commission assessed in Decision 2016/1250, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law, by the principle of proportionality, in so far as the surveillance programmes based on those provisions are not limited to what is strictly necessary. On the basis of the findings made in that decision, the Court pointed out that, in respect of certain surveillance programmes, those provisions do not indicate any limitations on the power they confer to implement those programmes, or the existence of guarantees for potentially targeted non-US persons. The Court added that, although those provisions lay down requirements with which the US authorities must comply when implementing the surveillance programmes in question, the provisions do not grant data subjects actionable rights before the courts against the US authorities (paragraphs 164, 165, 180 to 182, 184 and 185).

As regards the requirement of judicial protection, the Court held that, contrary to the view taken by the Commission in Decision 2016/1250, the Ombudsperson mechanism referred to in that decision does not provide data subjects with any cause of action before a body which offers guarantees substantially equivalent to those required by EU law, such as to ensure both the independence of the Ombudsperson provided for by that mechanism and the existence of rules empowering the Ombudsperson to adopt decisions that are binding on the US intelligence services. On all those grounds, the Court declared Decision 2016/1250 invalid (paragraphs 195 to 197, 201 and operative part 5).

V. Protection of personal data on the internet

1. Right to object to the processing of personal data ('right to be forgotten')

Judgment of 13 May 2014 (Grand Chamber), Google Spain and Google (C-131/12, EU:C:2014:317)

In this judgment (see also Section II.3. 'Concept of "processing of personal data"'), the Court clarified the scope of the right of access and the right to object to the processing of personal data on the internet, provided for by Directive 95/46.

Thus, when ruling on the question of the extent of the responsibility of the operator of a search engine on the internet, the Court held, in essence, that, in order to comply with the right of access and the right to object guaranteed by Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, and in so far as the conditions laid down by those provisions are satisfied, that operator is, in certain circumstances, 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. The Court stated that such an obligation may also exist where that name or the 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 (paragraph 88 and operative part 3).

Furthermore, questioned as to whether the directive enables the data subject to ask for links to web pages to be removed from such a list of results because he wishes the information displayed there and relating to him personally to be 'forgotten' after a certain time, the Court noted, first of all, that 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, in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes or in the light of the time that has elapsed (paragraph 93). Therefore, if it is found, following a request by the data subject, that the inclusion of those links in the list is, at this point in time, incompatible with the directive, the information and links in that list must be erased (paragraph 94). In this context, it is not necessary, in order to find a right of the data subject that the information relating to him personally should no longer be linked to his name by a list of results, that the inclusion of the information in question in the list of results causes prejudice to him (paragraph 96 and operative part 4).

Last, the Court made clear that, as the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question (paragraph 97 and operative part 4).

2. Processing of personal data and intellectual property rights

Judgment of 29 January 2008 (Grand Chamber), Promusicae (C-275/06, EU:C:2008:54) [59]

Promusicae, a Spanish non-profit-making organisation of producers and publishers of musical and audiovisual recordings, had brought proceedings before the Spanish courts for an order that Telefónica de España SAU (a commercial company whose activities include the provision of internet access services) be required to disclose the identities and physical addresses of certain persons to whom that company provided internet access services and whose IP addresses and the date and time of connection were known. According to Promusicae, those persons were using the peer-to-peer or P2P program (a transparent method of file sharing which is independent, decentralised, and features advanced search and download functions) and providing access in shared files of personal computers to phonograms in which the members of Promusicae held the exploitation rights. It had therefore sought disclosure of that information in order to be able to bring civil proceedings against the persons concerned.

In those circumstances, the Juzgado de lo Mercantil nº 5 de Madrid (Commercial Court No 5, Madrid, Spain) referred a question to the Court as to whether EU legislation requires Member States to lay down, in order to ensure effective protection of copyright, an obligation to communicate personal data in the context of civil proceedings.

According to the Court, that request for a preliminary ruling raised the question of the need to reconcile the requirements of the protection of different fundamental rights, namely the right to respect for private life, on the one hand, and the rights to protection of property and to an effective remedy, on the other.

In that respect, the Court concluded that Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') [60], Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society [61], Directive 2004/48/EC on the enforcement of intellectual property rights [62], and Directive 2002/58 do not require the Member States to lay down, in a situation such as that in the main proceedings, an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings. However, EU law requires that, when transposing those directives, the Member States take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be

[59] This judgment was included in the 2008 Annual Report, p. 46.

[60] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') (OJ 2000, L 178, p. 1).

[61] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001, L 167, p. 10).

[62] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ 2004, L 157, p. 45, and corrigendum OJ 2004, L 195, p. 16).

in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality (paragraph 70 and operative part).

Judgment of 24 November 2011, Scarlet Extended (C-70/10, EU:C:2011:771) [63]

The Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) had established that internet users using the services of Scarlet Extended SA, an internet service provider ('Scarlet'), were downloading works in SABAM's catalogue from the internet, without authorisation and without paying royalties, by means of peer-to-peer networks. SABAM brought proceedings before the national court and obtained, at first instance, an order requiring Scarlet to bring those copyright infringements to an end by making it impossible for its customers to send or receive in any way electronic files containing a musical work in the SABAM catalogue using peer-to-peer software.

Following an appeal by Scarlet, the cour d'appel de Bruxelles (Court of Appeal, Brussels, Belgium) stayed proceedings in order to ask the Court for a preliminary ruling on whether such an injunction was compatible with EU law.

The Court held that Directives 95/46, 2000/31, 2001/29, 2002/58 and 2004/48, read together and construed in the light of the requirements stemming from the protection of the applicable fundamental rights, must be interpreted as precluding an injunction made against Scarlet which requires it to install a system for filtering all electronic communications passing via its services, in particular those involving peer-to-peer software, which applies indiscriminately to all its customers, as a preventive measure, exclusively at its own expense, and for an unlimited period, and which is capable of identifying on that provider's network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold intellectual property rights, with a view to blocking the transfer of files the sharing of which infringes copyright (paragraph 54 and operative part).

According to the Court, such an injunction both infringes the prohibition on imposing a general monitoring obligation on such a provider laid down by Article 15(1) of Directive 2000/31, and fails to comply with the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other (paragraphs 40 and 49).

In that context, the Court noted that, first, the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network is sent. Those addresses are protected personal data because they allow those users to be precisely identified (paragraph 51). Second, that injunction could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications.

[63] This judgment was included in the 2011 Annual Report, p. 37.

Indeed, it is not contested that the reply to the question whether a transmission is lawful also depends on the application of statutory exceptions to copyright which vary from one Member State to another. Moreover, in some Member States certain works fall within the public domain or can be posted online free of charge by the authors concerned (paragraph 52).

Consequently, the Court held that, in granting the injunction requiring Scarlet to install the contested filtering system, the national court concerned would not be respecting the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other (paragraph 53).

Judgment of 19 April 2012, Bonnier Audio and Others (C-461/10, EU:C:2012:219)

The Högsta domstolen (Supreme Court, Sweden) made a reference to the Court of Justice for a preliminary ruling on the interpretation of Directives 2002/58 and 2004/48 in proceedings between Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB and Storyside AB ('the applicants in the main proceedings') and Perfect Communication Sweden AB ('ePhone') concerning the latter's opposition to an injunction obtained by the applicants in the main proceedings ordering the disclosure of data.

In this case, the applicants in the main proceedings were publishing companies holding, inter alia, exclusive rights to the reproduction, publishing and distribution to the public of 27 works in the form of audio books. They claimed that their exclusive rights had been infringed by the public distribution of these 27 works, without their consent, by means of an FTP ('file transfer protocol') server which allowed file sharing and data transfer between computers connected to the internet. They therefore applied to the Swedish courts for an order for disclosure of data for the purpose of communicating the name and address of the person using the IP address from which it was assumed that the files in question had been sent.

In that context, the Högsta domstolen, hearing an appeal in cassation, asked the Court whether EU law precludes the application of a national provision which is based on Article 8 of Directive 2004/48 and which permits an internet service provider in civil proceedings, in order to identify a particular subscriber, to be ordered to give a copyright holder or its representative information on the subscriber to whom the internet service provider provided a specific IP address, which address, it was claimed, had been used in the infringement. The question was based on the assumption that the applicant had adduced clear evidence of the infringement of a particular copyright and that the measure was proportionate.

The Court noted first of all that Article 8(3) of Directive 2004/48, read in conjunction with Article 15(1) of Directive 2002/58, does not preclude Member States from imposing an obligation to disclose to private persons personal data in order to enable them to bring civil proceedings for copyright infringements, but nor does it require those Member States to lay down such an obligation. However, the authorities and courts of Member States must not only interpret their national law in a manner consistent with those directives, but must also make sure that they do not rely on an interpretation of them which would conflict with those

fundamental rights or with the other general principles of EU law, such as the principle of proportionality (paragraphs 55 and 56).

The Court found, in that regard, that the national legislation in question required, inter alia, that, for an order for disclosure of the data in question to be made, there be clear evidence of an infringement of an intellectual property right, that the information can be regarded as facilitating the investigation into an infringement of copyright or impairment of such a right and that the reasons for the measure outweigh the nuisance or other harm which the measure could entail for the person affected by it or for some other conflicting interest (paragraph 58).

Consequently, the Court concluded that Directives 2002/58 and 2004/48 do not preclude national legislation such as that at issue in the main proceedings in so far as that legislation enables the national court seized of an application for an order for disclosure of personal data, made by a person who is entitled to act, to weigh the conflicting interests involved, on the basis of the facts of each case and taking due account of the requirements of the principle of proportionality (paragraph 61 and operative part).

Judgment of 17 June 2021, M.I.C.M. (C-597/19, EU:C:2021:492)

The undertaking Mircom International Content Management Consulting (M.I.C.M.) Limited ('Mircom') submitted a request for information against Telenet BVBA, an internet service provider, to the Ondernemingsrechtbank Antwerpen (Companies Court, Antwerp, Belgium; 'the referring court'). That request seeks a decision requiring Telenet to produce the identification data of its customers on the basis of IP addresses collected, by a specialised company, on behalf of Mircom. The internet connections of Telenet's customers have been used to share films in the Mircom catalogue, on a peer-to-peer network, using the BitTorrent protocol. Telenet challenges that request.

It is in that context that the referring court, first of all, asked the Court whether the sharing of pieces of a media file containing a protected work on that network constitutes a communication to the public under EU law. Next, it sought to ascertain whether the holder of intellectual property rights, such as Mircom, which does not use them, but claims damages from alleged infringers, can benefit from the measures, procedures and remedies provided for by EU law in order to ensure that those rights are enforced, for example by requesting information. Finally, the referring court asked the Court of Justice to clarify the question of the lawfulness, first, of the way in which the customers' IP addresses were collected by Mircom and, second, of the communication of the data requested by Mircom from Telenet.

The Court holds that EU law [64]does not preclude, in principle, the systematic registration, by the holder of intellectual property rights or by a third party on his or her behalf, of IP addresses of users of peer-to-peer networks whose internet connections have allegedly been used in infringing activities (upstream processing of data), or the communication of the names and of postal addresses of users to that holder or to a third party for the purposes of an action for

[64] Article 6(1)(f) of the GDPR and article (15) of the Directive 2002/58.

damages (downstream processing of data). However, initiatives and requests in that regard must be justified, proportionate, not abusive and provided for by a national legislative measure which limits the scope of rights and obligations under EU law. The Court states that the latter does not impose an obligation on a company such as Telenet to communicate personal data to private individuals in order to be able to bring proceedings before the civil courts for copyright infringements. However, EU law allows Member States to impose such an obligation (paragraphs 97,125 to 127 and operative part 3).

3. De-referencing of personal data

Judgment of 24 September 2019 (Grand Chamber), GC and Others (De-referencing of sensitive data) (C-136/17, EU:C:2019:773) [65]

In this judgment, the Court, sitting as the Grand Chamber, clarified the obligations of operators of a search engine in the context of a request for de-referencing relating to sensitive data.

Google had refused to accede to the requests of four individuals for the de-referencing, in the list of results displayed by the search engine in response to searches against their names, of various links leading to web pages published by third parties, including press articles. Following complaints by those four individuals, the Commission nationale de l'informatique et des libertés (CNIL) (French Data Protection Authority, France) refused to serve formal notice on Google to carry out the de-referencing requested. The Conseil d'État (Council of State, France), before which the case was brought, asked the Court to clarify the obligations of an operator of a search engine when handling a request for de-referencing under Directive 95/46.

First, the Court recalled that the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life is prohibited [66], subject to certain exceptions and derogations. As regards the processing of data relating to offences, criminal convictions or security measures, this may in principle be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law [67] (paragraphs 39 and 40).

The Court ruled that the prohibition and restrictions relating to the processing of those special categories of data apply to the operator of a search engine, in the same way as any other controller of personal data. The purpose of those prohibitions and restrictions is to ensure enhanced protection as regards such processing, which, because of the particular sensitivity of the data, is liable to constitute a particularly serious interference with the fundamental rights to privacy and the protection of personal data (paragraphs 42 to 44).

[65] This judgment was included in the 2019 Annual Report, p. 117 and118.
[66] Article 8(1) of Directive 95/46 and Article 9(1) of Regulation (EU) 2016/679.
[67] Article 8(5) of Directive 95/46 and Article 10 of Regulation (EU) 2016/679.

However, the operator of a search engine is responsible not because personal data appear on a web page published by a third party but because of the referencing of that page. In those circumstances, the prohibition and restrictions relating to the processing of sensitive data apply to that operator only by reason of that referencing and thus via a verification, under the supervision of the competent national authorities, on the basis of a request by the data subject (paragraphs 46 and 47).

Second, the Court held that when the operator receives a request for de-referencing relating to sensitive data, he is in principle required, subject to certain exceptions, to accede to that request. As regards those exceptions, the operator may, inter alia, refuse to accede to such a request if he establishes that the links lead to data which are manifestly made public by the data subject [68], provided that the referencing of those links satisfies the other conditions of lawfulness of the processing of personal data and unless the data subject has the right to object to that referencing on grounds relating to the data subject's particular situation [69] (paragraphs 65 and 69).

In any event, when the operator of a search engine receives a request for de-referencing, he must ascertain whether the inclusion in the list of results, displayed following a search on the basis of the data subject's name of the link to a web page on which sensitive data are published, is strictly necessary for protecting the freedom of information of internet users potentially interested in accessing that web page by means of such a search. In that regard, the Court pointed out that, while the rights to privacy and the protection of personal data override, as a general rule, the freedom of information of internet users, that balance may, however, depend, in specific cases, on the nature of the information in question and on its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, depending on the role played by the data subject in public life (paragraphs 66 and 68).

Third, the Court ruled that, in the context of a request for de-referencing in respect of data relating to criminal proceedings brought against the data subject, concerning an earlier stage of the proceedings and no longer corresponding to the current situation, it is for the operator of a search engine to assess whether, in the light of all the circumstances of the case, the data subject has a right to have the information in question no longer, in the present state of things, linked with the data subject's name by a list of results displayed following a search carried out on the basis of that name. However, even if it is not the case because the inclusion of the link in question is strictly necessary for reconciling the data subject's rights to privacy and the protection of personal data with the freedom of information of potentially interested internet users, the operator is required, at the latest on the occasion of the request for de-referencing, to adjust the list of results in such a way that the overall picture it gives the internet user reflects the current legal position, which means in particular that links to web pages containing information on that point must appear in the first place on the list (paragraphs 77 and 78).

[68] Article 8(2)(e) of Directive 95/46 and Article 9(2)(e) of Regulation (EU) 2016/679.
[69] Subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 and Article 21(1) of Regulation (EU) 2016/679.

Judgment of 24 September 2019 (Grand Chamber), Google (Territorial scope of de-referencing) (C-507/17, EU:C:2019:772) [70]

The Commission nationale de l'informatique et des libertés (French Data Protection Authority, France) ('the CNIL') served formal notice on Google that, in the case where that company accedes to a request for de-referencing, it must remove, from the list of results displayed on all its search engine's domain name extensions following a search conducted on the basis of the name of the data subject, links to web pages containing personal data concerning that data subject. Following Google's refusal to comply with that formal notice, the CNIL imposed a penalty of EUR 100 000 on that company. The Conseil d'État (Council of State, France), in the proceedings brought before it by Google, asked the Court to specify the territorial scope of the obligation for a search engine operator to give effect to the right to de-referencing under Directive 95/46.

First of all, the Court recalled the possibility, under EU law, for natural persons to assert their right to de-referencing against a search engine operator who has one or more establishments in the territory of the European Union, regardless of whether or not the processing of personal data (in the present case, the referencing of links to web pages containing personal data concerning the person availing himself of that right) takes place in the European Union [71].

With regard to the scope of the right to de-referencing, the Court took the view that the operator of a search engine is required to carry out the de-referencing not on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States. It noted in this regard that, while a universal de-referencing would, in view of the characteristics of the internet and search engines, meet the EU legislature's objective of guaranteeing a high level of protection of personal data throughout the European Union in full, it is in no way apparent from EU law [72] that, for the purposes of achieving such an objective, the legislature would have chosen to confer a scope on the right to de-referencing which would go beyond the territory of the Member States. In particular, while EU law establishes cooperation mechanisms between the supervisory authorities of the Member States in order that they may come to a joint decision based on a weighing of the right to privacy and of the protection of personal data, on the one hand, against the interest of the public in various Member States in having access to information, on the other, no provision is currently made for such mechanisms as regards the scope of a de-referencing outside the European Union (paragraphs 62 and 73).

As EU law currently stands, it is for the operator of a search engine to carry out the requested de-referencing not only on the version of the search engine corresponding to the Member State of residence of the person benefiting from that de-referencing but on the versions of the search engine corresponding to the Member States, in order, in particular, to ensure a consistent and high level of protection throughout the European Union. Moreover, it is for such an operator to take, if necessary, sufficiently effective measures to prevent or, at the very least, seriously discourage EU internet users from gaining access, as the case may be from a version of the

[70] This judgment was included in the 2019 Annual Report, pp. 118 and-119.
[71] Article 4(1)(a) of Directive 95/46 and Article 3(1) of Regulation (EU) 2016/679.
[72] Articles 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, and Article 17(1) of Regulation (EU) 2016/679.

search engine corresponding to a third country, to the links concerned by the de-referencing, and it is for the national court to ascertain whether the measures adopted by the operator meet that requirement (paragraph 70).

Lastly, the Court emphasised that, although EU law does not require the operator of a search engine to carry out a de-referencing on all the versions of its search engine, it also does not prohibit such a practice. Accordingly, a supervisory or judicial authority of a Member State remains competent to weigh up, in the light of national standards of protection of fundamental rights, a data subject's right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine (paragraphs 65 and 72).

4. Consent by a website user to the storage of information

Judgment of 1 October 2019 (Grand Chamber), Planet49 (C-673/17, EU:C:2019:801) [73]

By this judgment, the Court ruled that consent to the storage of, or access to, information in the form of cookies installed on a website user's terminal equipment is not validly constituted if given by way of a pre-checked checkbox, irrespective of whether or not the information in question constitutes personal data. Furthermore, the Court made clear that the information that the service provider must give to an internet user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies.

The case in the main proceedings concerned a promotional lottery organised by Planet49 on the website www.dein-macbook.de. Internet users wishing to take part in that lottery were required to enter their names and addresses on a web page with checkboxes. The checkbox authorising the installation of cookies contained a preselected tick. In an appeal brought by the German Federation of Consumer Organisations, the Bundesgerichtshof (Federal Court of Justice, Germany) harboured doubts as to the validity of the consent obtained from internet users by means of the preselected checkbox and as to the extent of the information obligation owed by the service provider.

The request for a preliminary ruling concerned, in substance, the concept of consent referred to in the Directive 2002/58 [74], read in conjunction with Directive 95/46 [75], and the GDPR. [76]

First, the Court observed that Article 2(h) of Directive 95/46, to which Article 2(f) of the Directive 2002/58 refers, defines 'consent' as being 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being

[73] This judgment was included in the 2019 Annual Report, p. 120 and 121.
[74] Article 2(f) and Article 5(3) of Directive 2002/58, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009, L 337, p. 11).
[75] Article 2(h) of Directive 95/46.
[76] Article 6(1)(a) of Regulation (EU) 2016/679.

processed'. It noted that the requirement of an 'indication' of the data subject's wishes points clearly to active, rather than passive, behaviour. However, consent given in the form of a preselected tick in a checkbox does not imply active behaviour on the part of a website user. Furthermore, the legislative origins of Article 5(3) of the Directive 2002/58, which, as amended by Directive 2009/136, provides that the user must have 'given his or her consent' to the storage of cookies, appears to indicate that user consent may no longer be presumed but must be the result of active behaviour on the part of the user. Finally, active consent is now provided for by the GDPR [77], Article 4(11) of which requires an indication of the data subject's wishes in the form of 'clear affirmative action' and recital 32 of which expressly precludes 'silence, pre-ticked boxes or inactivity' from constituting consent (paragraphs 49, 52, 56 and 62).

The Court therefore held that consent is not validly given if the storage of information, or access to information already stored in the website user's terminal equipment, is permitted by way of a pre-ticked checkbox which the user must deselect in order to refuse his consent. It added that the fact that a user selects the button to participate in the lottery in question cannot therefore suffice for the conclusion that the user has validly given his or her consent to the storage of cookies (paragraph 63).

Second, the Court stated that Article 5(3) of the Directive 2002/58 seeks to protect the user from interference with his or her private sphere, regardless of whether or not that interference involves personal data. It follows that the concept of consent must not be interpreted differently according to whether or not the information stored or accessed on a website user's terminal equipment constitutes personal data (paragraphs 69 and 71).

Third, the Court noted that Article 5(3) of the Directive 2002/58 requires that the user concerned must have given his or her consent, having been provided with clear and comprehensive information, inter alia, about the purposes of the processing. Clear and comprehensive information implies that a user is in a position to be able to determine easily the consequences of any consent he or she might give and to ensure that the consent given is well informed. In that regard, the Court held that the duration of the operation of the cookies and whether or not third parties may have access to those cookies form part of the clear and comprehensive information that must be provided to a website user by the service provider (paragraphs 73 to 75 and 81).National supervisory authorities.

[77] Idem.

VI. National supervisory authorities

1. Scope of the requirement of independence

Judgment of 9 March 2010 (Grand Chamber), Commission v Germany (C-518/07, EU:C:2010:125) [78]

By its application, the European Commission had requested the Court to declare that, by making the authorities responsible for monitoring the processing of personal data outside the public sector in the different German *Länder* subject to State oversight, and by thus incorrectly transposing the requirement of 'complete independence' of the supervisory authorities responsible for ensuring the protection of those data, the Federal Republic of Germany had failed to fulfil its obligations under the second subparagraph of Article 28(1) of Directive 95/46.

The Federal Republic of Germany contended that the second subparagraph of Article 28(1) of Directive 95/46 requires the supervisory authorities to have functional independence in the sense that those authorities must be independent of the non-public sector under their supervision and that they must not be exposed to external influences. In the view of the Federal Republic of Germany, the State scrutiny exercised in the *Länder* did not constitute such an external influence, but rather the administration's internal monitoring mechanism, implemented by the authorities attached to the same administrative machinery as the supervisory authorities and required, like the latter, to fulfil the aims of Directive 95/46.

The Court held that the guarantee of the independence of national supervisory authorities provided for by Directive 95/46 is intended to ensure the effectiveness and reliability of the monitoring of compliance with the provisions concerning protection of individuals with regard to the processing of personal data and must be interpreted in the light of that aim. It was not established in order to grant a special status to those authorities themselves as well as their agents, but in order to strengthen the protection of individuals and bodies affected by their decisions, the supervisory authorities being consequently required to act objectively and impartially when carrying out their duties (paragraph 25).

The Court found that these supervisory authorities responsible for supervising the processing of personal data outside the public sector must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any directions or any other external influence, whether direct or indirect, which could call into question the performance by those authorities of their task of establishing a fair balance between the protection of the right to private life and the free movement of personal data. The mere risk that the scrutinising authorities could exercise a political influence over the decisions of the competent supervisory authorities is enough to hinder the latter authorities' independent performance of their tasks. First, there could be 'prior compliance' on the part of those authorities in the light of the scrutinising

[78] This judgment was included in the 2010 Annual Report, p. 34.

authority's decision-making practice. Second, for the purposes of the role adopted by those supervisory authorities as guardians of the right to private life, it is necessary that their decisions, and therefore the authorities themselves, remain above any suspicion of partiality. According to the Court, State scrutiny of national supervisory authorities is not, therefore, compatible with the requirement of independence (paragraphs 30, 36, 37 and operative part).

Judgment of 16 October 2012 (Grand Chamber), Commission v Austria (C-614/10, EU:C:2012:631)

By its application, the European Commission had asked the Court to declare that, by failing to take all of the measures necessary to ensure that the legislation in force in Austria met the requirement of independence with regard to the Datenschutzkommission (Data Protection Commission), which was established as a supervisory authority for the protection of personal data, Austria had failed to fulfil its obligations under the second subparagraph of Article 28(1) of Directive 95/46.

The Court declared that Austria had failed to fulfil its obligations, finding, in essence, that a Member State which lays down a regulatory framework under which that authority's managing member is a federal official subject to supervision, whose office is integrated with national government departments, and in respect of which the head of the national government has an unconditional right to information covering all aspects of that authority's work does not meet the requirement of independence of a supervisory authority, laid down by Directive 95/46 (paragraph 66 and operative part).

The Court, first of all, recalled that the words 'with complete independence' in the second subparagraph of Article 28(1) of Directive 95/46 mean that the supervisory authorities must enjoy an independence which allows them to perform their duties free from external influence. The fact that such an authority has functional independence in so far as its members are independent and are not bound by instructions of any kind in the performance of their duties is not by itself sufficient to protect that supervisory authority from all external influence. The independence required in that connection is intended to preclude not only direct influence, in the form of instructions, but also any indirect influence which is liable to have an effect on the supervisory authority's decisions. Moreover, in the light of the role adopted by the supervisory authorities as guardians of the right to private life, their decisions, and therefore the authorities themselves, must remain above any suspicion of partiality (paragraphs 41 to 43 and 52).

The Court stated that, in order to be able to satisfy the criterion of independence set out in the aforementioned provision of Directive 95/46, a national supervisory authority need not be given a separate budget, such as that provided for in Article 43(3) in Regulation Nº 45/2001. Member States are not obliged to reproduce in their national legislation provisions similar to those of Chapter V of Regulation Nº 45/2001 in order to ensure the total independence of their respective supervisory authorities, and they can therefore provide that, from the point of view of budgetary law, the supervisory authorities are to come under a specified ministerial department. However, the attribution of the necessary equipment and staff to such authorities must not

prevent them from acting 'with complete independence' in exercising the functions entrusted to them within the meaning of the second subparagraph of Article 28(1) of Directive 95/46 (paragraph 58).

Judgment of 8 April 2014 (Grand Chamber), Commission v Hungary (C-288/12, EU:C:2014:237) [79]

In this case, the Commission had asked the Court to declare that, by prematurely bringing to an end the term served by the supervisory authority for the protection of personal data, Hungary had failed to fulfil its obligations under Directive 95/46.

The Court held that a Member State fails to fulfil its obligations under Directive 95/46 if it prematurely brings to an end the term served by the supervisory authority for the protection of personal data (paragraph 62 and operative part 1).

According to the Court, the supervisory authorities responsible for supervising the processing of those data must enjoy an independence allowing them to perform their duties free from external influence in whatever form, whether direct or indirect, which may have an effect on their decisions and which could call into question the performance by those authorities of their task of striking a fair balance between the protection of the right to private life and the free movement of personal data (paragraph 51).

The Court also pointed out that, since operational independence is not sufficient in itself to protect supervisory authorities from all external influence, the mere risk that State scrutinising authorities could exercise political influence over the decisions of the supervisory authorities is enough to hinder the latter in the independent performance of their tasks. If it were permissible for every Member State to compel a supervisory authority to vacate office before serving its full term, in contravention of the rules and safeguards established in that regard by the legislation applicable, the threat of such premature termination to which that authority would be exposed throughout its term of office could lead it to enter into a form of prior compliance with the political authority, which is incompatible with the requirement of independence. Moreover, in such a situation, the supervisory authority cannot be regarded as being able, in all circumstances, to operate above all suspicion of partiality (paragraphs 52 to 55).

2. Determination of the applicable law and of the competent supervisory authority

Judgment of 1 October 2015, Weltimmo (C-230/14, EU:C:2015:639) [80]

The Nemzeti Adatvédelmi és Információszabadság Hatóság (National Authority for Data Protection and Freedom of Information, Hungary) imposed a fine on Weltimmo, a company

[79] This judgment was included in the 2014 Annual Report, p. 62.
[80] This judgment was included in the 2015 Annual Report, p. 55.

registered in Slovakia running property-dealing websites concerning Hungarian properties, on the ground that it had not deleted the personal data of advertisers on those sites, despite their requests to that effect, and had forwarded those data to debt-collection agencies for the purpose of obtaining settlement of unpaid bills. According to the Hungarian supervisory authority, Weltimmo had, in so doing, infringed the Hungarian law transposing Directive 95/46.

On hearing an appeal in cassation, the Kúria (Supreme Court, Hungary) expressed doubts concerning the determination of the applicable law and the powers of the Hungarian data protection authority under Articles 4(1) and 28 of Directive 95/46. It therefore referred a number of questions to the Court for a preliminary ruling.

As regards the national law applicable, the Court ruled that Article 4(1)(a) of Directive 95/46 permits the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity — even a minimal one — in the context of which that processing is carried out. In order to ascertain whether that is the case, the referring court may, in particular, take account of the fact that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property-dealing websites concerning properties situated in the territory of that Member State and written in that Member State's language and that it is, as a consequence, mainly or entirely directed at that Member State. The referring court may, moreover, also take account of the fact that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to the processing of the data concerned. By contrast, the Court made clear that the issue of the nationality of the persons concerned by such data processing is irrelevant (paragraph 41 and operative part 1).

As regards the competence and powers of the supervisory authority to which complaints have been submitted in accordance with Article 28(4) of Directive 95/46, the Court held that that authority may examine those complaints irrespective of the applicable law and before even knowing which national law is applicable to the processing in question (paragraph 54). However, if it reaches the conclusion that the law of another Member State is applicable, it cannot impose penalties outside the territory of its own Member State. In such a situation, it must, in fulfilment of the duty of cooperation laid down in Article 28(6) of that directive, request the supervisory authority of that other Member State to establish whether there has been an infringement of that law and to impose penalties if that law permits, based, where necessary, on the information which the authority of the first Member State has transmitted to the authority of that other Member State (paragraphs 57, 60 and operative part 2).

3. Powers of the national supervisory authorities

Judgment of 6 October 2015 (Grand Chamber), Schrems (C-362/14, EU:C:2015:650)

In this case (see also Section IV 'Transfer of personal data to third countries'), the Court ruled, inter alia, that national supervisory authorities have the power to control transfers of personal data to third countries.

In that regard, the Court found, first of all, that national supervisory authorities have a wide range of powers and that those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means by which to perform their duties. Thus, those authorities possess, in particular, investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to engage in legal proceedings (paragraph 43).

As regards the power to control transfers of personal data to third countries, the Court ruled that it is, admittedly, apparent from Article 28(1) and (6) of Directive 95/46 that the powers of the national supervisory authorities concern processing of personal data carried out on the territory of their own Member State, with the result that they do not have powers on the basis of Article 28 in respect of the processing of such data in a third country (paragraph 44).

However, the operation consisting in 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. Consequently, as, in accordance with Article 8(3) of the Charter and Article 28 of Directive 95/46, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data, each of them is vested with the power to check whether a transfer of those data from its own Member State to a third country complies with the requirements laid down by that directive (paragraphs 45 and 47).

Judgment of 5 June 2018 (Grand Chamber), Wirtschaftsakademie Schleswig — Holstein (C-210/16, EU:C:2018:388)

In this judgment (see also Section II.5. 'Concept of a "controller of the processing of personal data"') relating to, inter alia, the interpretation of Articles 4 and 28 of Directive 95/46, the Court ruled on the extent of the powers of intervention of supervisory authorities with regard to the processing of personal data which involves the participation of several parties.

Thus, the Court held that where an undertaking established outside the European Union (such as the US company Facebook) has several establishments in different Member States, the supervisory authority of a Member State is entitled to exercise the powers conferred on it by Article 28(3) of that directive with respect to an establishment of that undertaking situated in the territory of that Member State (in this case, Facebook Germany) even if, as a result of the division

of tasks within the group, first, that establishment is responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State and, secondly, exclusive responsibility for collecting and processing personal data belongs, for the entire territory of the European Union, to an establishment situated in another Member State (in this case, Facebook Ireland) (paragraph 64 and operative part 2).

Furthermore, the Court stated that where the supervisory authority of a Member State intends to exercise, with respect to an entity established in the territory of that Member State, the powers of intervention referred to in Article 28(3) of Directive 95/46, on the ground of infringements of the rules on the protection of personal data committed by a third party responsible for the processing of that data whose seat is in another Member State (in this case, Facebook Ireland), that supervisory authority is competent to assess, independently of the supervisory authority of the other Member State (Ireland), the lawfulness of such data processing and may exercise its powers of intervention with respect to the entity established in its territory without first calling on the supervisory authority of the other Member State to intervene (paragraph 74 and operative part 3).

Judgment of 15 June 2021 (Grand Chamber), Facebook Ireland and Others (C-645/19, EU:C:2021:483)

On 11 September 2015, the President of the Belgian Privacy Commission ('the Privacy Commission') brought an action before the Nederlandstalige rechtbank van eerste aanleg Brussel (Dutch-language Court of First Instance, Brussels, Belgium), seeking an injunction against Facebook Ireland, Facebook Inc. and Facebook Belgium, aiming to put an end to alleged infringements of data protection laws by Facebook. Those infringements consisted, inter alia, of the collection and use of information on the browsing behaviour of Belgian internet users, whether or not they were Facebook account holders, by means of various technologies, such as cookies, social plug-ins [81] or pixels.

On 16 February 2018, that court held that it had jurisdiction to give a ruling on that action and, on the substance, held that the Facebook social network had not adequately informed Belgian internet users of the collection and use of the information concerned. Further, the consent given by the internet users to the collection and processing of that data was held to be invalid.

On 2 March 2018, Facebook Ireland, Facebook Inc. and Facebook Belgium brought an appeal against that judgment before the Hof van beroep te Brussel (Court of Appeal, Brussels, Belgium), the referring court in the present case. Before that court, the Belgian Data Protection Authority ('the DPA') acted as the legal successor of the President of the Privacy Commission. The referring court held that it solely has jurisdiction to give a ruling on the appeal brought by Facebook Belgium.

[81] For example, the 'Like' or 'Share' buttons.

The referring court was uncertain as to the effect of the application of the 'one-stop shop' mechanism provided for by the GDPR [82]on the competences of the DPA and, in particular, as to whether, with respect to the facts subsequent to the date of entry into force of the GDPR, namely 25 May 2018, the DPA may bring an action against Facebook Belgium, since it is Facebook Ireland which has been identified as the controller of the data concerned. Since that date, and in particular under the 'one-stop shop' rule laid down by the GDPR, only the Data Protection Commissioner (Ireland) is competent to bring injunction proceedings, subject to review by the Irish courts (paragraphs 36 et 37).

In its Grand Chamber judgment, the Court of Justice specifies the powers of national supervisory authorities within the scheme of the GDPR. Thus, it considers, inter alia, that that regulation authorises, under certain conditions, a supervisory authority of a Member State to exercise its power to bring any alleged infringement of the GDPR before a court of that State and to initiate or engage in legal proceedings in relation to an instance of cross-border data processing, [83] although that authority is not the lead supervisory authority with regard to that processing (operative part 1).

In the first place, the Court specifies the conditions governing whether a national supervisory authority, which does not have the status of lead supervisory authority in relation to an instance of cross-border processing, must exercise its power to bring any alleged infringement of the GDPR before a court of a Member State and, where necessary, to initiate or engage in legal proceedings in order to ensure the application of that regulation. Thus, the GDPR must confer on that supervisory authority a competence to adopt a decision finding that that processing infringes the rules laid down by that regulation and, in addition, that power must be exercised with due regard to the cooperation and consistency procedures provided for by that regulation [84] (paragraph 75, operative part 1).

With respect to cross-border processing, the GDPR provides for the 'one-stop shop' mechanism, [85] which is based on an allocation of competences between one 'lead supervisory authority' and the other national supervisory authorities concerned. That mechanism requires close, sincere and effective cooperation between those authorities in order to ensure consistent and homogeneous protection of the rules for the protection of personal data, and thus preserve its effectiveness. As a general rule, the GDPR guarantees in this respect the competence of the lead supervisory authority for the adoption of a decision finding that an instance of cross-border processing is an infringement of the rules laid down by that regulation, [86] whereas the competence of the other supervisory authorities concerned for the adoption of such a decision, even provisionally, constitutes the exception to the rule. [87] However, in the exercise of its competences, the lead supervisory authority cannot eschew essential dialogue and sincere and

82 Under the terms of the article 56(1) of the GDPR: 'Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor'

83 Within the meaning of Article 4(23) of the GDPR.

84 Laid down in Articles 56 and 60 of the GDPR.

85 Article 56(1) of the GDPR.

86 Article 60(7) of the GDPR.

87 Article 56(2) and Article 66 of the GDPR set out exceptions to the general rule that it is the lead supervisory authority that is competent to adopt such decisions.

effective cooperation with the other supervisory authorities concerned. Accordingly, in the context of that cooperation, the lead supervisory authority may not ignore the views of the other supervisory authorities concerned, and any relevant and reasoned objection made by one of the other supervisory authorities has the effect of blocking, at least temporarily, the adoption of the draft decision of the lead supervisory authority (paragraphs 50 to 53, 56 to 59 and 63 to 65).

The Court also adds that the fact that a supervisory authority of a Member State which is not the lead supervisory authority with respect to an instance of cross-border data processing may exercise the power to bring any alleged infringement of the GDPR before a court of that State and to initiate or engage in legal proceedings only when that exercise complies with the rules on the allocation of competences between the lead supervisory authority and the other supervisory authorities [88] is compatible with Articles 7, 8 and 47 of the Charter, which guarantee data subjects the right to the protection of his or her personal data and the right to an effective remedy, respectively (paragraph 67).

In the second place, the Court holds that, in the case of cross-border data processing, it is not a prerequisite for the exercise of the power of a supervisory authority of a Member State, other than the lead supervisory authority, to initiate or engage in legal proceedings [89] that the controller or the processor with respect to the cross-border processing of personal data to which that action relates has a main establishment or another establishment on the territory of that Member State. However, the exercise of that power must fall within the territorial scope of the GDPR, [90] which presupposes that the controller or the processor with respect to the cross-border processing has an establishment in the European Union (paragraphs 80, 83, 84 and disp 2).

In the third place, the Court rules that, in the event of cross-border data processing, the power of a supervisory authority of a Member State, other than the lead supervisory authority, to bring any alleged infringement of the GDPR before a court of that Member State and, where appropriate, to initiate or engage in legal proceedings, may be exercised both with respect to the main establishment of the controller which is located in that authority's own Member State and with respect to another establishment of that controller, provided that the object of the legal proceedings is a processing of data carried out in the context of the activities of that establishment and that that authority is competent to exercise that power.

However, the Court adds that the exercise of that power presupposes that the GDPR is applicable. In this instance, since the activities of the establishment of the Facebook group located in Belgium are inextricably linked to the processing of personal data at issue in the main proceedings, with respect to which Facebook Ireland is the controller within the European Union, that processing is carried out 'in the context of the activities of an establishment of the controller' and, therefore, does fall within the scope of the GDPR (paragraphs 94 to 96 and operative part 3).

---

88 Laid down in Articles 55 and 56, read together with Article 60 of the GDPR.

89 Pursuant to Article 58(5) of the GDPR.

90 Article 3(1) of the GDPR provides that that regulation is applicable to the processing of personal data 'in the context of the activities of an establishment of a controller or a processor in the [European] Union, regardless of whether the processing takes place in the [European] Union or not'.

In the fourth place, the Court holds that, where a supervisory authority of a Member State which is not the 'lead supervisory authority' brought, before the date of entry into force of the GDPR, legal proceedings concerning an instance of cross-border processing of personal data, that action may be continued, under EU law, on the basis of the provisions of Directive 95/46, which remains applicable in relation to infringements of the rules laid down in that directive committed up to the date when that directive was repealed. In addition, that action may be brought by that authority with respect to infringements committed after the date of entry into force of the GDPR, provided that that action is brought in one of the situations where, exceptionally, that regulation confers on that authority a competence to adopt a decision finding that the processing of data in question is in breach of the rules laid down by that regulation, and that the cooperation and consistency procedures provided for by the regulation are respected (paragraph 105 and operative part 4).

In the fifth and last place, the Court recognises the direct effect of the provision of the GDPR under which each Member State is to provide by law that its supervisory authority is to have the power to bring infringements of that regulation to the attention of the judicial authorities and, where appropriate, to initiate or engage otherwise in legal proceedings. Consequently, such an authority may rely on that provision in order to bring or continue a legal action against private parties, even where it has not been specifically implemented in the legislation of the Member State concerned (paragraph 113 and operative part 5).

VII. Territorial application of EU legislation

Judgment of 13 May 2014 (Grand Chamber), Google Spain and Google (C-131/12, EU:C:2014:317)

In this judgment (see also Sections II.3. 'Concept of "processing of personal data"' and V.1. 'Right to object to the processing of personal data ("right to be forgotten")', the Court also ruled on the territorial scope of Directive 95/46.

Thus, the Court held that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of Directive 95/46, when the operator of a search engine, despite having its seat in a third State, sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State (paragraphs 55, 60 and operative part 2).

In such circumstances, the activities of the operator of the search engine and those of its establishment situated in a Member State, although separate, are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed (paragraph 56).

VIII. Right of public access to documents of the institutions of the European Union and protection of personal data

Judgment of 29 June 2010 (Grand Chamber), Commission v Bavarian Lager (C-28/08 P, EU:C:2010:378)

Bavarian Lager, a company established for the importation of German beer for public houses and bars in the United Kingdom, had been unable to sell its product, since a large number of publicans in the United Kingdom were tied by exclusive purchasing contracts obliging them to obtain their supplies of beer from certain breweries.

Under United Kingdom legislation on the supply of beer, known as the Guest Beer Provision ('the GBP'), British breweries were required to allow pub managers the possibility of buying a beer from another brewery, on condition that it had been conditioned in a cask. However, most beers produced outside the United Kingdom could not be regarded as 'cask-conditioned beers' within the meaning of the GBP, and thus did not fall within its scope. Bavarian Lager took the view that that legislation constituted a measure having equivalent effect to a quantitative restriction on imports and lodged a complaint with the Commission.

During the infringement proceedings initiated by the Commission against the United Kingdom, representatives of the Community and United Kingdom administrative authorities and of the Confédération des Brasseurs du Marché Commun (CBMC) had attended a meeting held on 11 October 1996. The United Kingdom authorities informed the Commission that the legislation in question was to be amended, so as to allow bottle-conditioned beer to be sold as a guest beer as well as cask-conditioned beer. Thereupon, the Commission had told Bavarian Lager that the infringement proceedings were to be suspended.

Bavarian Lager had lodged an application requesting the full minutes of the October 1996 meeting, including the names of all the participants, which the Commission had subsequently refused by decision of 18 March 2004, invoking in particular the privacy of those individuals, as guaranteed by the legislation 45/2001.

Bavarian Lager then brought an action before the General Court seeking annulment of that Commission decision. By judgment of 8 November 2007, the General Court annulled the Commission's decision, finding in particular that the mere inclusion of the names of persons on the list of participants at a meeting, acting on behalf of the bodies they represented, did not adversely affect or jeopardise their privacy. The Commission, supported by the United Kingdom and the Council, then lodged an appeal with the Court against that judgment of the General Court.

The Court noted, first of all, that where a request based on Regulation Nº 1049/2001 [91], regarding access to documents, seeks to obtain access to documents including personal data,

[91] Regulation (EC) Nº 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents (OJ 2001, L 145, p. 43).

the provisions of Regulation Nº 45/2001 become applicable in their entirety, including the provision requiring the recipient of personal data to establish the need for their disclosure and the provision which confers on the data subject the right to object at any time, on compelling legitimate grounds relating to his or her particular situation, to the processing of data relating to him or her (paragraph 63).

The Court then went on to find that the list of participants at a meeting held in the context of infringement proceedings which appeared in the minutes of that meeting contained personal data for the purposes of Article 2(a) of Regulation Nº 45/2001, since the persons who participated in that meeting could be identified (paragraph 70).

Last, it concluded that, in requiring, in respect of those persons who had not given their express consent to the disclosure of personal data concerning them contained in those minutes, that the necessity of having the personal data transferred be established, the Commission had complied with the provisions of Article 8(b) of that regulation (paragraph 77).

Where, in the context of a request for access to those minutes under Regulation Nº 1049/2001, no express or legitimate justification or any convincing argument is provided in order to demonstrate the necessity for those personal data to be transferred, the Commission is unable to weigh up the various interests of the parties concerned. Nor can it verify whether there is any reason to assume that the data subjects' legitimate interests might be prejudiced by that transfer, as required by Article 8(b) of Regulation Nº 45/2001 (paragraph 78) [92].

Judgment of 16 July 2015, ClientEarth and PAN Europe v EFSA (C-615/13 P, EU:C:2015:489)

The European Food Safety Authority (EFSA) had established a working group to develop guidance as to how to implement Article 8(5) of Regulation (EC) Nº 1107/2009 [93], according to which an applicant for authorisation to place a plant protection product on the market is to add to the dossier scientific peer-reviewed open literature, as determined by EFSA, on the active substance and its relevant metabolites dealing with side-effects on health, the environment and non-target species.

The draft guidance was submitted for public consultation, and ClientEarth and Pesticide Action Network Europe (PAN Europe) submitted comments on it. In that context, they had jointly submitted to EFSA an application requesting access to a number of documents related to the preparation of the draft guidance, including the comments of the external experts.

EFSA granted ClientEarth and PAN Europe access to, inter alia, the individual comments of the external experts on the draft guidance document. It stated, however, that it had redacted the names of those experts, in accordance with Article 4(1)(b) of Regulation Nº 1049/2001 and the EU legislation on the protection of personal data, in particular Regulation Nº 45/2001. It stated in that regard that the disclosure of the names of those experts was a transfer of personal data,

92 This judgment was included in the 2010 Annual Report, p. 14.

93 Regulation (EC) Nº 1107/2009 of the European Parliament and of the Council of 21 October 2009 concerning the placing of plant protection products on the market and repealing Council Directives 79/117/EEC and 91/414/EEC (OJ 2009, L 309, p. 1).

within the meaning of Article 8 of Regulation Nº 45/2001, and that the conditions for such a transfer laid down in that article were not fulfilled in this case.

Consequently, ClientEarth and PAN Europe brought an action for annulment of that EFSA decision before the General Court. Following the General Court's dismissal of that action, ClientEarth and PAN Europe brought an appeal against the General Court's judgment [94] before the Court of Justice.

In the first place, the Court noted that, because the information sought would make it possible to connect to one particular expert or another a particular comment, it concerned identified natural persons and accordingly constituted a set of personal data, within the meaning of Article 2(a) of Regulation Nº 45/2001. Since the concepts of 'personal data' within the meaning of Article 2(a) of Regulation Nº 45/2001 and of 'data relating to private life' are not to be confused, the Court further considered the claim made by ClientEarth and PAN Europe that the information at issue did not fall within the scope of the private life of the experts concerned to be ineffective (paragraphs 29 and 32).

The Court examined, in the second place, the argument of ClientEarth and PAN Europe based on the existence of a climate of suspicion in regard to EFSA, often accused of partiality because of its use of experts with vested interests due to their links with industrial lobbies, and on the necessity of ensuring the transparency of EFSA's decision-making process. That argument was supported by a study which identified links between a majority of the expert members of an EFSA working group and industrial lobbies. The Court held that obtaining the information at issue was necessary so that the impartiality of each of those experts in carrying out their tasks as scientists in the service of EFSA could be specifically ascertained. The Court therefore set aside the judgment of the General Court, ruling that the General Court was wrong to hold that the aforementioned argument of ClientEarth and PAN Europe was not sufficient to establish that the transfer of the information at issue was necessary (paragraphs 57 to 59).

In the third place, in order to assess the legality of the EFSA decision at issue, the Court examined whether or not there was any reason to assume that that transfer might have prejudiced the legitimate interests of the data subjects. It found, in that regard, that the allegation by EFSA that the disclosure of the information at issue would have been likely to undermine the privacy and integrity of the experts was a consideration of a general nature which was not otherwise supported by any factor specific to the case. The Court considered, on the contrary, that such disclosure would, by itself, have made it possible for the suspicions of partiality in question to be dispelled or would have afforded experts who might be concerned the opportunity to dispute, if necessary by available legal remedies, the merits of those allegations of partiality. In the light of those points, the Court also annulled EFSA's decision (paragraphs 69 and 73).

94 Judgment of the General Court of 13 September 2013, *ClientEarth and PAN Europe* v *EFSA* (T-214/11, EU:T:2013:483).

* * *

The judgments covered in this fact sheet are indexed in the Directory of case-law under 1.04.03.07, 1.04.03.08, 1.04.03.10, 1.04.03.11, 2.04, 2.05.00, 4.11.01, 4.11.07., 4.11.11.01.