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of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31); consolidated version: 20.11.2003; repealed from 25 May 2018 (see footnote 5).

Directive 2002/58/EC [2] subsequently supplemented Directive 95/46/EC 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]

In addition, in the area of freedom, security and justice (ex Articles 30 and 31 TEU), Framework Decision 2008/977/JHA [4] regulates (until May 2018) the protection of personal data in the areas of judicial cooperation in criminal matters and police cooperation.

The European Union recently drew up a comprehensive new legal framework. To that end, in 2016 it adopted Regulation (EU) 2016/679 [5] on data protection, which repeals Directive 95/46/EC and will be directly applicable from 25 May 2018, and Directive (EU) 2016/680 [6] on the protection of such data in criminal matters, which repeals Framework Decision 2008/977/JHA and is 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 [7] ensures the protection of such data. In particular, the regulation enabled the European Data Protection Supervisor to be established in 2004. In January 2017, the Commission submitted a proposal [8] for a new regulation repealing Regulation No 45/2001 and Decision No 1247/2002/EC with a view to modernising data protection rules and aligning them with the new regime established by Regulation (EU) 2016/679.

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 L 201, 31.7.2002, p. 37); consolidated version: 19.12.2009.

3 Directive 2002/58/EC 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 L 105, 13.4.2006, 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 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (OJ L 350, 30.12.2008, p. 60), repealed from 6 May 2018 (see footnote 6).

5 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 L 119, 4.5.2016, p. 1), applicable from 25 May 2018.

6 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 L 119, 4.5.2016, p. 89).

7 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 L 8, 12.1.2001, p. 1).

8 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals 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 (COM(2017) 8 final).

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) [9]

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) No 1290/2005 [10] and No 259/2008, [11] 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 of Justice concerning the validity of certain provisions of Regulation (EC) No 1290/2005 and that of Regulation (EC) No 259/2008, which required such information to be made available to the public, in particular through websites operated by the national offices.

The Court of Justice 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 56-64).

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 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, 86).

---

9 This judgment was presented in the 2010 Annual Report, p. 11.

10 Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy (OJ L 209, 11.8.2005, p. 1), repealed by Regulation (EU) No 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 L 347, 20.12.2013, p. 549).

11 Commission Regulation (EC) No 259/2008 of 18 March 2008 laying down detailed rules for the application of Council Regulation (EC) No 1290/2005 as regards the publication of information on the beneficiaries of funds deriving from the EAGF and the EAFRD (OJ L 76, 19.3.2008, p. 28), repealed by Commission Implementing Regulation (EU) No 908/2014 of 6 August 2014 laying down rules for the application of Regulation (EU) No 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 L 255, 28.8.2014, p. 59).

Thus, the Court declared certain provisions of Regulation (EC) No 1290/2005, and Regulation (EC) 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, 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, 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 [12] 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 of Justice 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 (EC) 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 35-38). Next, the taking and storing of fingerprints is 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 42-45).

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 (EC) No 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 54-57, 60, 63).

12 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 L 385, 29.12.2004, p. 1), as amended by Regulation (EC) No 444/2009 of the European Parliament and of the Council of 6 May 2009 (OJ L 142, 6.6.2009, p. 1).

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) [13]

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/EC into Austrian law.

By their requests for a preliminary ruling, the Irish and Austrian courts referred questions to the Court of Justice about the validity of Directive 2006/24/EC in the light of Articles 7, 8 and 11 of the Charter. More specifically, the referring courts asked the Court of Justice 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 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/EC 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 38-44).

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/EC 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 57-59). The directive also failed to lay down any objective criterion by which to ensure that

13 This judgment was presented in the 2014 Annual Report, p. 58.

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 60-62). 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, 64).

Furthermore, as regards the requirements arising under Article 8(3) of the Charter, the Court held that Directive 2006/24/EC 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 66-68).

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) [14]

Following the judgment in *Digital Rights Ireland and Seitlinger and Others* in which Directive 2006/24/EC was declared invalid (see above), two cases were brought before the Court of Justice 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 references 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 of Justice was requested to rule on the interpretation of Article 15(1) of Directive 2002/58/EC (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/EC, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter, precludes national legislation such as the Swedish

14 This judgment was presented in the 2016 Annual Report, p. 59.

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 democratic society, as required by Article 15(1), read in the light of the aforementioned provisions of the Charter (paragraphs 99-105, 107, 112, 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 118-122, 125, operative part 2).

The Court, however, considered that Article 15(1) of Directive 2002/58/EC 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 108-111).

II. The processing of personal data within the meaning of Directive 95/46/EC

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

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 [15] 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 [16] 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 of Justice 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/EC. 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 fell 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, 57).

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, 59).

As regards the Council decision, the Court found that Article 95 EC, read in conjunction with Article 25 of Directive 95/46/EC, 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 67-69).

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

15 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 L 235, 6.7.2004, p. 11).

16 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 L 183, 20.5.2004, p. 83, and corrigendum OJ L 255, 30.9.2005, p. 168).

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 of Justice 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/EC, on the grounds 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/EC, 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 27-29). Furthermore, the actual wording of that provision is such that Directive 95/46/EC 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, 33).

2. Concept of 'personal data'

Judgment of 19 October 2016, Breyer (C-582/14, EU:C:2016:779) [17]

Mr Breyer 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 enable the user to be identified.

17 This judgment was presented in the 2016 Annual Report, p. 59.

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 of Justice 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/EC, 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/EC (paragraphs 43, 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/EC, 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, operative part 1).

Judgment of 20 December 2017, Nowak (C-434/16, ECLI:EU:C:2017:582)

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 of Justice whether Article 2(a) of Directive 95/46/EC 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/EC, 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.

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.

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/EC, 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/EC, do not extend to the examination questions, which do not as such constitute the candidate's personal data.

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/EC.

3. Concept of 'processing of personal data'

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

Ms 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. Ms 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 Ms Lindqvist against that decision, the national court referred questions to the Court of Justice for a preliminary ruling in order, in particular, to ascertain whether Ms Lindqvist had carried out 'the processing of personal data wholly or partly by automatic means' within the meaning of Directive 95/46/EC.

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, 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, 43-48, 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 of Justice.

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

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). 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, 30).

4. Conditions for lawful processing of personal data in the light of Article 7 of Directive 95/46/EC

Judgment of 16 December 2008 (Grand Chamber), Huber (C-524/06, EU:C:2008:724) [18]

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

18 This judgment was presented in the 2008 Annual Report, p. 43.

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 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 of Justice 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, 59).

As regards the concept of the necessity of the processing under Article 7(e) of Directive 95/46/EC, 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/EC 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/EC (paragraphs 52, 66, 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 78-80).

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/EC.

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/EC, 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/EC, 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/EC 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, 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/EC. In consequence, the Court concluded that Article 7(f) of Directive 95/46/EC 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, 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 of Justice also ruled on the question whether Article 7(f) of Directive 95/46/EC 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/EC 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/EC 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 62-64, 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 of Justice whether Article 7(f) of Directive 95/46/EC 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/EC 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 referred, inter alia, a question to the Court of Justice 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/EC 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/EC are satisfied (paragraph 117, operative part 3).

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, 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/EC, 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).

III. Transfer of personal data to third countries

Judgment of 6 November 2003 (Full Court), Lindqvist (C-101/01, EU:C:2003:596) [19]

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

19 This judgment was presented in the 2003 Annual Report, p. 72.

The Court held that there is no 'transfer [of data] to a third country' within the meaning of Article 25 of Directive 95/46/EC 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, operative part 4).

Given, first, the state of development of the internet at the time Directive 95/46/EC 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, one cannot presume 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, 68).

Judgment of 6 October 2015 (Grand Chamber), Schrems (C-362/14, EU:C:2015:650) [20]

Mr Schrems, an Austrian citizen and user of the Facebook social network, had made a complaint to Ireland's Data Protection Commissioner because 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 2000/520/EC, [21] found that, in the context of the 'safe harbour regime', [22] 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 of Justice by the High Court (Ireland) for interpretation of Article 25(6) of Directive 95/46/EC, 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/EC, which was adopted by the Commission on the basis of Article 25(6) of Directive 95/46/EC.

The Court declared the Commission decision to be invalid in its entirety, stating first of all that, in order for the Commission to adopt the decision, it had to find, duly stating reasons, that the third country concerned in fact ensures 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/EC, Article 1 of that decision failed to comply with the requirements laid down in Article 25(6) of Directive 95/46/EC, read in the light of the Charter, and was 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/EC enabled 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 in order to limit any interference with those rights and without referring to the existence of effective legal protection against interference of that kind (paragraphs 82, 87-89, 96-98, operative part 2).

20 This judgment was presented in the 2015 Annual Report, p. 51.

21 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 L 215, 25.8.2000, p. 7).

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

In addition, the Court declared Article 3 of Decision 2000/520/EC 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/EC, where a person puts forward matters that may call in 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 102-104). The Court concluded that the invalidity of Articles 1 and 3 of Decision 2000/520/EC affected the validity of that decision in its entirety (paragraphs 105, 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).

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). 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 an 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. 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, 95).

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

On 26 July 2017, the Court of Justice 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 of Justice 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 non-member 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, 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, 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, a 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 205-207, 209).

In the third place, the Court held that the fundamental right to respect for private life, enshrined in Article 7 of the Charter of Fundamental Rights of the European Union, 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, 224).

IV. 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 of Justice 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/EC.

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/EC, 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, 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, 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, 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) [23]

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 n° 5 de Madrid (Commercial Court No 5, Madrid, Spain) referred a question to the Court of Justice 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.

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'), [24] Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information

23 This judgment was presented in the 2008 Annual Report, p. 43.

24 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 L 178, 17.7.2000, p. 1).

society, [25] Directive 2004/48/EC on the enforcement of intellectual property rights, [26] and Directive 2002/58/EC 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 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) [27]

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 of Justice for a preliminary ruling on whether such an injunction was compatible with EU law.

The Court held that Directives 95/46/EC, 2000/31/EC, 2001/29/EC, 2002/58/EC and 2004/48/EC, 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/EC, 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, 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

25 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 L 167, 22.6.2001, p. 10).

26 Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (OJ L 157, 30.4.2004, p. 45, and corrigendum OJ L 195, 2.6.2004, p. 16).

27 This judgment was presented in the 2011 Annual Report, p. 36.

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. 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/EC and 2004/48/EC 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 of Justice whether EU law precludes the application of a national provision which is based on Article 8 of Directive 2004/48/EC 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/EC, read in conjunction with Article 15(1) of Directive 2002/58/EC, 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, 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/EC and 2004/48/EC do not preclude national legislation such as that at issue in the main proceedings in so far as that legislation enables the national court seised 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).

V. 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) [28]

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/EC.

The Federal Republic of Germany contended that the second subparagraph of Article 28(1) of Directive 95/46/EC 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/EC.

The Court held that the guarantee of the independence of national supervisory authorities provided for by Directive 95/46/EC 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

28 This judgment was presented in the 2010 Annual Report, p. 33.

bodies, but also any directions or any other external influence, whether direct or indirect, which could call in 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 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/EC.

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/EC (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/EC 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 41-43, 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/EC, a national supervisory authority need not be given a separate budget, such as that provided for in Article 43(3) in Regulation (EC) No 45/2001. Member States are not obliged to reproduce in their national legislation provisions similar to those of Chapter V of Regulation (EC) 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/EC (paragraph 58).

Judgment of 8 April 2014 (Grand Chamber), Commission v Hungary (C-288/12, EU:C:2014:237) [29]

In this case, the Commission had asked the Court of Justice 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/EC.

The Court held that a Member State fails to fulfil its obligations under Directive 95/46/EC if it prematurely brings to an end the term served by the supervisory authority for the protection of personal data (paragraph 62, 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 in 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 recalled 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 52-55).

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) [30]

The Nemzeti Adatvédelmi és Információszabadság Hatóság (National Authority for Data Protection and Freedom of Information, Hungary) imposed a fine on Weltimmo, a company 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 the 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 Hungarian law transposing Directive 95/46/EC.

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/EC. It therefore referred a number of questions to the Court of Justice for a preliminary ruling.

29 This judgment was presented in the 2014 Annual Report, p. 60.
30 This judgment was presented in the 2015 Annual Report, p. 52.

As regards the national law applicable, the Court ruled that Article 4(1)(a) of Directive 95/46/EC 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, 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/EC, 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 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, 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 III 'Transfer of personal data to third countries'), the Court of Justice ruled, inter alia, that national supervisory authorities have the power to control transfers of personal data to third countries.

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/EC, constitute necessary means 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/EC that the powers of the national supervisory authorities concern processing of personal data carried out on the territory of their own Member State, so 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/EC, 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 the directive (paragraphs 45, 47).

VI. 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 Parts II.3. 'Concept of "processing of personal data"' and IV.1. 'Right to object to the processing of personal data ("right to be forgotten")', the Court of Justice also ruled on the territorial scope of Directive 95/46/EC.

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/EC, 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, 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).

VII. 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 on the protection of personal data.

Bavarian Lager then brought an action before the General Court seeking annulment of that decision by the Commission. 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 of Justice against that judgment of the General Court.

The Court of Justice noted, first of all, that where a request based on Regulation (EC) No 1049/2001 [31] regarding access to documents seeks to obtain access to documents including personal data, the provisions of Regulation (EC) 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 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 (EC) 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 (EC) 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 (EC) No 45/2001 (paragraph 78). [32]

31 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 L 145, 31.5.2001, p. 43).

32 This judgment was presented in the 2010 Annual Report, p. 14.

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, [33] 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, pursuant to Article 4(1)(b) of Regulation (EC) No 1049/2001 and EU legislation on the protection of personal data, in particular Regulation (EC) No 45/2001. It stated in that regard that the disclosure of the names of those experts was a transfer of personal data, within the meaning of Article 8 of Regulation (EC) 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. The General Court having dismissed the action, ClientEarth and PAN Europe brought an appeal against the General Court's judgment [34] 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 (EC) No 45/2001. Since the concepts of 'personal data' within the meaning of Article 2(a) of Regulation (EC) 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, 32).

The Court examined, in the second place, the argument of ClientEarth and PAN Europe based on the existence of a climate of suspicion of 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 57-59).

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

33 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 L 309, 24.11.2009, p. 1).

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

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, 73).

* * *

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