COURT OF JUSTICE
OF THE EUROPEAN UNION

EN

Fact sheet
Protection of personal data

Research and Documentation Directorate

curia.europa.eu

Preface

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 primary law, in particular Article 8 of the Charter of Fundamental Rights of the European Union (hereinafter the 'Charter'), as well as Article 16(1) of the Treaty on the Functioning of the European Union (TFEU).

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

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the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1] repealed since 2018, was the European Union's main legal instrument in this regard.

Directive 2002/58/EC [2] subsequently supplemented Directive 95/46 by harmonising the provisions of Member States' legislation on the protection of the right to privacy, with respect inter alia to the processing of personal data in the electronic communications sector. [3] It should be noted that, in order to take account of new technological and commercial developments, the EU legislature has, as of 2017, undertook a review of Directive 2002/58, [4] which is still ongoing. [5]

1 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31), consolidated version as at 20 November, repealed with effect from 25 May 2018 (see note 6).

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 (Directive on privacy and electronic communications) (OJ 2002, L 201, p. 37), consolidated version as at 19 December 2009.

3 Directive 2002/58 was amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006, L 105, p. 54). That directive was annulled 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 grounds that it seriously infringed the rights to respect for private life and to the protection of personal data (see section I.1. 'Compliance of secondary EU law with the right to the protection of personal data' of this fact sheet).

4 On 10 January 2017, the Commission presented a Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications).

5 On 10 February 2021, the Council of the European Union approved a negotiating mandate for the revision of the rules on the protection of privacy and confidentiality in the use of electronic communications services enabling negotiations to begin with the European Parliament. The text of the Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) is available at this link: *https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_6087_2021_INIT&from=EN*.

In 2016, the European Union comprehensively reformed the legal framework in this area. To that end, it adopted Regulation (EU) 2016/679 [6] on the protection of personal data (the 'GDPR'), which repeals Directive 95/46 and has been applicable since 25 May 2018, and Directive (EU) 2016/680 [7] on the protection of such data in criminal matters, the provisions of which have been applicable since 6 May 2018.

As regards the processing of personal data by EU institutions and bodies, the protection of such data is ensured inter alia, since 11 December 2018, by Regulation (EU) 2018/1725. [8] In the interests of a coherent approach to the protection of personal data throughout the European Union, that regulation aims to align the rules in this area as closely as possible with the regime established by the GDPR.

Finally, in order to meet the challenges raised by new technologies, the EU legislature has, since 2020, launched the adoption of new legislative measures [9] building on that framework of EU law provisions on the protection of personal data.

Given the wealth of Court of Justice case-law on the protection of personal data, the aim of this factsheet is to present a selection of seminal rulings on the subject and rulings that have made a significant contribution to the development of this case-law, with particular emphasis on rulings handed down by the Grand Chamber of the Court. More specifically, this fact sheet is intended to cover both case-law relating to the general rules on the protection of personal data, resulting from the interpretation of Directive 95/46 and the GDPR, and case-law relating to sector-specific rules, particularly in the electronic communications sector and criminal law. In addition, it aims to present a selection of judgments dealing with rules which are applicable across multiple areas, while highlighting from the outset the decisive role of the Charter in the development of the case-law.

---

6 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ 2016 L 119, p. 1).

7 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89).

8 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ 2018 L 295, p. 39).

9 In this context, three legislative initiatives in particular should be noted: (*i)* Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Regulation) (OJ 2022, L 152, p. 1) and Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules concerning fairness in access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Regulation) (OJ 2023, L 2854, p. 1); (*ii)* a legislative package on digital services and markets, consisting of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Regulation) (OJ 2022, L 277, p. 1) and Regulation 2022/1925 of the European Parliament and of the Council of 14 September 2022 on fair and contestable contracts in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Market Regulation) (OJ 2022, L 265, p. 1); and (*iii)* the first ever legislative proposal to create a regulatory framework for artificial intelligence, which materialised in a regulation on artificial intelligence (OJ 2024, L, 1689).

Contents

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

1. Compliance 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)

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) Nos 1290/2005 [10] and 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 concerning the validity of certain provisions of Regulation No 1290/2005 and that of Regulation 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.

---

[10] Council Regulation (EC) No 1290/2005 of 21 June 2005 on the financing of the common agricultural policy (OJ 2005 L 209, 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 2013 L 347, 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 2008 L 76, p. 28), repealed by Commission Implementing Regulation (EU) No 908/2014 of 6 August 2014 laying down detailed rules for the application of Regulation (EU) No 1306/2013 of the European Parliament and of the Council as regards paying agencies and other entities, financial management, clearance of accounts, control rules, guarantees and transparency (OJ 2014 L 255, p. 59).

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. 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.

Thus, the Court declared invalid certain provisions of Regulation No 1290/2005, as well as Regulation No 259/2008 as a whole, insofar as, with regard to natural persons receiving aid from the EAGF and EAFRD, those provisions require the publication of personal data relating to any beneficiary, without making any distinction according to relevant criteria, such as the periods during which they have received such aid, the frequency or the type and amount of that aid. However, the Court did not call into question the effects of the publication of lists of recipients of such aid by the national authorities during the period prior to the date of delivery of the judgment.

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)

This judgment had 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 the company Digital Rights against the Irish authorities regarding the legality of national measures concerning the retention of data relating to electronic communications. In Case C-594/12, a number of constitutional cases came before the Verfassungsgerichtshof (Constitutional Court, Austria), in which annulment was sought of national legislation transposing Directive 2006/24 into Austrian law.

By their requests for a preliminary ruling, the Irish and Austrian courts referred questions to the Court of Justice on the validity of Directive 2006/24 in the light of Articles 7, 8 and 11 of the Charter. More specifically, the referring courts asked the Court 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, inter alia, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, and to identify the time of the communication as well as the place from which that communication took place. They also make it possible to know the frequency of the communications of the subscriber or registered user with certain persons during a given period.

The Court, first of all, held that, by imposing such obligations on those providers, Directive 2006/24 constituted a particularly serious interference with the fundamental rights to respect for private life and the protection of personal data, guaranteed by Articles 7 and 8 of the Charter. In that context, the Court found that that interference may be justified where it pursues an objective of general interest, such as the fight against organised crime. The Court stated in that regard, in the first place, that the retention of data required by the directive was not such as to adversely affect the essence of the fundamental rights to respect for privacy and the protection of personal data, in so far as it did not permit the acquisition of knowledge of the content of the electronic communications as such and set out 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.

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. 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. The directive also failed to lay down any objective criterion by which to ensure that the competent national authorities would have access to the data and be able to use them for the sole purpose of preventing, investigating and prosecuting offences capable of being considered to be sufficiently serious to justify such an interference, or the substantive and procedural conditions relating to such access or such use. 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 among the categories of data according to the data subjects or on the basis of the possible usefulness of the data for the purposes of the objective pursued.

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

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

Judgment of 21 June 2022 (Grand Chamber), Ligue des droits humains (C-817/19, EU:C:2022:491)

PNR (Passenger Name Record) data are reservation information stored by air carriers in their reservation and departure control systems. The PNR Directive [12] requires those carriers to transfer the data of any passenger on an extra-EU flight operated between a third country and the European Union to the Passenger Information Unit ('PIU') of the Member State of destination or departure of the flight concerned, for the purposes of the fight against terrorist offences and serious crime. The PNR data thus transferred are subject to advance assessment by the PIU [13] and are then retained for the purposes of a possible subsequent assessment by the competent authorities of the Member State concerned or those of another Member State. A Member State may decide to apply that directive also to intra-EU flights. [14]

An action for annulment of the Belgian law transposing both the PNR Directive and the API Directive [15] was brought before the Constitutional Court (Belgium) by the Ligue des droits humains. According to the applicant, that law infringed the right to respect for private life and to the protection of personal data. It criticised, first, the very broad nature of PNR data and, second, the general nature of the collection, transfer and processing of those data. The law also allegedly infringed the free movement of persons in that it indirectly restored border controls by extending the PNR system to intra-EU flights and to transport operations carried out by other means within the European Union.

12 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (OJ 2016 L 119, p. 132) (the 'PNR Directive').

13 The purpose of this prior assessment is to identify persons for whom further examination by the competent authorities is required, taking into account the fact that these persons may be involved in a terrorist offence or a serious form of crime. It is carried out systematically and by automated means, by comparing PNR data with 'useful' databases or by processing them in accordance with the criteria set out in Article 6(2)(a) and (3) of the PNR directive.

14 Making use of the possibility provided for in Article 2 of the PNR Directive.

15 Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (OJ 2004 L 261, p. 24) (the 'API directive'). This directive governs the transmission of advance passenger information (such as the number and type of travel document used and nationality) by air carriers to the competent national authorities, with a view to improving border controls and combating illegal immigration.

In this context, the Belgian Constitutional Court referred questions to the Court of Justice for a preliminary ruling, relating in particular to the validity of the PNR Directive.

In its judgment, delivered by the Grand Chamber, the Court confirmed the validity of the PNR Directive insofar as it can be interpreted in accordance with the Charter.

In that regard, the Court held that, since the Court's interpretation of the provisions of the PNR Directive in the light of the fundamental rights guaranteed in Articles 7, 8 and 21 as well as Article 52(1) of the Charter [16] ensures that that directive is consistent with those articles, the examination of the questions referred revealed nothing capable of affecting the validity of that directive.

As a preliminary point, it recalled that an EU act must be interpreted, as far as possible, in such a way as not to affect its validity and in conformity with primary law as a whole and, in particular, with the provisions of the Charter, and the Member States must thus ensure that they do not rely on an interpretation thereof that would be in conflict with the fundamental rights protected by the EU legal order or with the other general principles recognised by EU law. As regards the PNR Directive, the Court stated that many recitals and provisions of that directive require such a consistent interpretation, stressing the importance that the EU legislature, by referring to the high level of data protection, gives to the full respect for the fundamental rights enshrined in the Charter.

The Court found that the PNR Directive entails undeniably serious interferences with the rights guaranteed in Articles 7 and 8 of the Charter, in so far, inter alia, as it seeks to introduce a surveillance regime that is continuous, untargeted and systematic, including the automated assessment of the personal data of everyone using air transport services. It pointed out that the question whether Member States may justify such an interference must be assessed by measuring its seriousness and by verifying that the importance of the objective of general interest pursued is proportionate to that seriousness.

The Court concluded that the transfer, processing and retention of PNR data provided for by that directive may be considered to be limited to what is strictly necessary for the purposes of combating terrorist offences and serious crime, provided that the powers provided for by that directive are interpreted restrictively. In that regard, the judgment delivered stated, inter alia, that:

- The system established by the PNR Directive must cover only clearly identifiable and circumscribed information under the headings set out in Annex I to that directive, which relates to the flight operated and the passenger concerned,

[16] In accordance with that provision, any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law and respect the essence of those rights and freedoms. In addition, limitations may be made to those rights and freedoms only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others.

which means, for some of the headings set out in that annex, that only the information expressly referred to is covered. [17]

- Application of the system established by the PNR Directive must be limited to terrorist offences and only to serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air. As regards such serious crime, the application of that system cannot be extended to offences which, although meeting the criterion laid down by that directive relating to the threshold of severity and being referred to in, inter alia, Annex II to that directive, amount to ordinary crime having regard to the particular features of the domestic criminal justice system.
- Any extension of the application of the PNR Directive to selected or all intra-EU flights, which a Member State may decide by exercising the power provided for in that directive, must be limited to what is strictly necessary. For that purpose, it must be open to effective review either by a court or by an independent administrative body whose decision is binding. In that regard, the Court stated:
- Only in a situation where that Member State finds that there are sufficiently solid grounds for considering that it is confronted with a terrorist threat which is shown to be genuine and present or foreseeable, the application of that directive to all intra-EU flights from or to the said Member State, for a period of time that is limited to what is strictly necessary but which may be extended, does not exceed what is strictly necessary. [18]
- In the absence of such a terrorist threat, the application of that directive cannot cover all intra-EU flights, but must be limited to intra-EU flights relating, inter alia, to certain routes or travel patterns or to certain airports in respect of which there are, according to the assessment of the Member State concerned, indications that are such as to justify that application. The strictly necessary nature of that application to intra-EU flights thus selected must be reviewed regularly, in accordance with changes in the circumstances that justified their selection.
- For the purposes of the advance assessment of PNR data, the objective of which is to identify persons who require further examination before their arrival or departure and is carried out, as a first step, by means of automated processing, the PIU may, on the one hand, compare those data only against the databases on

[17] Thus, in particular, 'forms of payment information' (heading 6 of the annex) must be limited to the payment methods and billing of the air ticket, to the exclusion of any other information not directly relating to the flight, and the 'general remarks' (heading 12) can relate only to the information expressly listed in that heading, relating to passengers who are minors.

[18] Indeed, the existence of such a threat is of such a nature, in itself, as to establish a relationship between the transfer and processing of the data concerned and the fight against terrorism. Accordingly, providing for the application of the PNR Directive to all intra-EU flights from or to the Member State concerned, for a limited period, does not exceed the limits of what is strictly necessary, since the decision providing for that application must be capable of being reviewed by a court or an independent administrative body.

persons or objects sought or under alert. [19] Those databases must be non-discriminatory and exploited, by the competent authorities, in relation to the fight against terrorist offences and serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air. As regards, on the other hand, the advance assessment against pre-determined criteria, the PIU cannot use artificial intelligence technology in self-learning systems ('machine learning'), capable of modifying, without human intervention and review, the assessment process and, in particular, the assessment criteria on which the result of the application of that process is based, as well as the weighting of those criteria. Those criteria must be determined in such a way that their application targets, specifically, individuals who might be reasonably suspected of involvement in terrorist offences or serious crime and takes into consideration both 'incriminating' as well as 'exonerating' circumstances, while not giving rise to direct or indirect discrimination. [20]

- In view of the margin of error inherent in such automated processing of PNR data and the fairly substantial number of 'false positives', resulting from the application thereof in 2018 and 2019, the appropriateness of the system established by the PNR Directive for the purpose of attaining the objectives pursued essentially depends on the proper functioning of the verification of positive results obtained under those processing operations, which the PIU carries out, as a second step, by non-automated means. In that regard, the Member States must lay down clear and precise rules capable of providing guidance and support for the analysis carried out by the PIU agents in charge of that individual review for the purposes of ensuring full respect for the fundamental rights enshrined in Articles 7, 8 and 21 of the Charter and, in particular, guarantee a uniform administrative practice within the PIU that observes the principle of non-discrimination. In particular, they must ensure that the PIU establishes objective review criteria enabling its agents to verify, on the one hand, whether and to what extent a positive match ('hit') concerns effectively an individual who may be involved in terrorist offences or serious crime, as well as, on the other hand, the non-discriminatory nature of automated processing operations. In that context, the Court also pointed out that the competent authorities must ensure that the data subject is able to understand how those pre-determined assessment criteria and programmes applying those criteria work, so that it is possible for that person to decide with full knowledge of the

[19] Namely, databases relating to on persons or objects sought or under alert, within the meaning of Article 6(3)(a) of the PNR Directive. On the other hand, analyses based on various databases could take the form of data mining and could give rise to a disproportionate use of these data, providing the means to establish the precise profile of data subjects for the sole reason that they intend to travel by air.

[20] The pre-established criteria must be targeted, proportionate and specific, and be reviewed at regular intervals (Article 6(4) of the PNR Directive). Prior assessment against pre-established criteria must be carried out in a non-discriminatory manner. According to the fourth sentence of Article 6(4) of the PNR Directive, the criteria shall in no case be based on a person's racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, state of health, sex life or sexual orientation.

relevant facts, whether or not to exercise his or her right to a judicial redress. Similarly, in the context of such an action, the court responsible for reviewing the legality of the decision adopted by the competent authorities as well as, except in the case of threats to State security, the data subjects themselves must have an opportunity to examine both all the grounds and the evidence on the basis of which the decision was taken, including the pre-determined assessment criteria and the operation of the programmes applying those criteria.

- The subsequent disclosure and assessment of PNR data, that is to say, after the arrival or departure of the person concerned, may be made only on the basis of new circumstances and objective evidence capable of either giving rise to a reasonable suspicion that that person is involved in serious crime having an objective link, even if only an indirect one, with the carriage of passengers by air, or from which it can be inferred that those data could, in a given case, contribute effectively to the fight against terrorist offences having such a link. The disclosure of PNR data for the purposes of such a subsequent assessment must, as a general rule, except in the event of duly justified urgency, be subject to a prior review carried out either by a court or by an independent administrative authority, upon reasoned request by the competent authorities and irrespective of whether that request was introduced before or after the expiry of the six-month time limit after the transfer of those data to the PIU. [21]

Judgment of 22 November 2022 (Grand Chamber), Luxembourg Business Registers (C-37/20 and C-601/20, EU:C:2022:912)

For the purposes of combating and preventing money laundering and terrorist financing, the anti-money-laundering directive [22] requires Member States to keep a register containing information on the beneficial ownership [23]of companies and of other legal entities incorporated within their territory. Following an amendment of that directive by Directive 2018/843, [24] some of that information must be made accessible in all cases to any member of the general public. In accordance with the anti-money-laundering directive as amended ('the amended anti-money-laundering directive'), Luxembourg legislation established a Register of Beneficial Ownership (RBO) designed

[21] Under Article 12(1) and (3) of the PNR Directive, such a check is expressly provided for only in respect of requests for communication of PNR data made after the period of six months following the transfer of those data to the PIU.

[22] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ 2015 L 141, p. 73, the 'anti-money laundering directive').

[23] In accordance with Article 3(6) of the anti-money laundering directive, a beneficial owner is any natural person who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted.

[24] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU (OJ 2018 L 156, p. 43).

to retain and make available a series of information on the beneficial ownership of registered entities, access to which is open to any person.

In that context, the tribunal d'arrondissement de Luxembourg (Luxembourg District Court) was seized of two actions, brought by WM and Sovim SA, respectively, challenging the rejection by Luxembourg Business Registers, the administrator of the RBO, of their applications seeking to preclude the general public's access to information relating, in the first case, to WM as the beneficial owner of a real estate company and, in the second case, to the beneficial owner of Sovim SA. In those two cases, since it had doubts in particular as to the validity of the provisions of EU law establishing the system of public access to information relating to beneficial ownership, the Tribunal d'arrondissement de Luxembourg (Luxembourg District Court) made a reference to the Court of Justice for a preliminary ruling.

By its judgment, the Court, sitting as the Grand Chamber, declared Directive 2018/843 invalid in so far as it amended the anti-money-laundering directive in such a way that Member States must ensure that information on the beneficial ownership of companies and of other legal entities incorporated within their territory is accessible in all cases to any member of the general public. [25]

In the first place, the Court found that the general public's access to information on beneficial ownership, provided for in the amended anti-money-laundering directive, constitutes a serious interference with the fundamental rights to respect for private life and to the protection of personal data, enshrined in the Charter's Articles 7 and 8, respectively.

In that regard, the Court observed that, since the data concerned include information on identified individuals, namely the beneficial owners of companies and other legal entities incorporated within the Member States' territory, the access by any member of the general public to those data affects the fundamental right to respect for private life. In addition, making available those data to the general public constitutes the processing of personal data. It added that making personal data available to the general public in that manner constitutes an interference with the above-mentioned fundamental rights, whatever the subsequent use of the information communicated.

As regards the seriousness of that interference, the Court noted that, in so far as the information made available to the general public relates to the identity of the beneficial owner, as well as to the nature and extent of the beneficial interest held in corporate or other legal entities, that information is capable of enabling a profile to be drawn up concerning certain personal identifying data, the state of the person's wealth and the economic sectors, countries and specific undertakings in which he or she has invested.

[25] Invalidity of Article 1(15)(c), of Directive 2018/843, amending Article 30(5), point (c) of the first subparagraph of the anti-money laundering directive.

In addition, that information becomes accessible to a potentially unlimited number of persons, with the result that such processing of personal data is liable to enable that information to be freely accessed also by persons who, for reasons unrelated to the objective pursued by that measure, seek to find out about, inter alia, the material and financial situation of a beneficial owner. That possibility is all the easier when the data in question can be consulted on the internet. Furthermore, the potential consequences for the data subjects resulting from possible abuse of their data are exacerbated by the fact that, once those data have been made available to the general public, they can not only be freely consulted, but also retained and disseminated and that it thereby becomes increasingly difficult, or even illusory, for those data subjects to defend themselves effectively against abuse.

In the second place, as part of the examination of the justification for the interference at issue, first, the Court noted that, in the present case, the principle of legality is respected. The limitation on the exercise of the above-mentioned fundamental rights, resulting from the general public's access to information on beneficial ownership, is provided for by a legislative act, namely the amended anti-money-laundering directive. In addition, that directive specifies that those data must be adequate, accurate and current, and expressly lists certain data to which the public must be allowed access. It also lays down the conditions under which Member States may provide for exemptions from such access.

Secondly, the Court clarified that the interference in question does not undermine the essence of the fundamental rights guaranteed in Articles 7 and 8 of the Charter. While it is true that the amended anti-money-laundering directive does not contain an exhaustive list of the data which any member of the general public must be permitted to access, and that Member States are entitled to provide for access to additional information, the fact remains that only adequate information on beneficial owners and beneficial interests held may be obtained, held and, therefore, potentially made accessible to the public, which excludes, inter alia, information which is not adequately related to the purposes of the amended anti-money-laundering directive. However, it does not appear that making such information available to the general public would in any way undermine the essential content of the fundamental rights in question.

Thirdly, the Court pointed out that, by providing for the general public's access to information on beneficial ownership, the EU legislature seeks to prevent money laundering and terrorist financing by creating, by means of increased transparency, an environment less likely to be used for those purposes, which constitutes an objective of general interest that is capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter.

Fourth, in examining whether the interference at issue is appropriate, necessary and proportionate, the Court found that, admittedly, public access to information on beneficial owners is capable of contributing to the attainment of that objective.

However, it deemed that such interference cannot be regarded as limited to what is strictly necessary. First, the strict necessity of that interference cannot be demonstrated by relying on the fact that the 'legitimate interest' criterion which any person wishing to have access to information on beneficial owners had to have - according to the Anti-Money Laundering Directive, in its version prior to its amendment by Directive 2018/843 - was difficult to implement and that its application could lead to arbitrary decisions. The fact that it may be difficult to provide a detailed definition of the circumstances and conditions under which the public may access information on beneficial ownership is no reason for the EU legislature to provide for the general public to access that information.

Secondly, nor can the explanations set out in Directive 2018/843 establish that the interference at issue is strictly necessary. [26] To the extent that, according to those explanations, the general public's access to beneficial ownership information is intended to allow greater scrutiny of information by civil society, in particular by the press and civil society organisations, the Court found that both the press and civil society organisations that are connected with the prevention and combating of money laundering and terrorist financing have a legitimate interest in accessing the information concerned. The same is true of the persons who wish to know the identity of the beneficial owners of a company or other legal entity because they are likely to enter into transactions with them, or of the financial institutions and authorities involved in combating offences of money laundering or terrorist financing.

Nor, moreover, is the interference in question proportionate. In that regard, the Court found that the substantive rules governing that interference do not meet the requirement of clarity and precision. The amended anti-money-laundering directive provides that any member of the general public may have access to 'at least' the data referred to therein and provides that Member States may provide for access to additional information, including 'at least' the date of birth or the contact details of the beneficial owner concerned. However, by using the expression 'at least', that directive allows for data to be made available to the public which are not sufficiently defined and identifiable.

Furthermore, as regards the balancing of the seriousness of that interference against the importance of the objective of general interest referred to, the Court recognised that, in view of its importance, that objective is capable of justifying even serious interferences with the fundamental rights enshrined in Articles 7 and 8 of the Charter.

Nevertheless, first, combating money laundering and terrorist financing is as a priority a matter for the public authorities and for entities such as credit or financial institutions which, by reason of their activities, are subject to specific obligations in that regard. For that reason, the amended anti-money-laundering directive provides that information on beneficial ownership must be accessible, in all cases, to competent authorities and

[26] This refers to the explanations set out in recital 30 of Directive 2018/843.

Financial Intelligence Units, without any restriction, as well as to obliged entities, within the framework of customer due diligence. [27]

Secondly, in comparison with the former regime – which provided, in addition to access by the competent authorities and certain entities, for access by any person or organisation capable of demonstrating a legitimate interest – the regime introduced by Directive 2018/843 amounts to a considerably more serious interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter, without that increased interference being capable of being offset by any benefits which might result from the latter regime as compared against the former regime, in terms of combating money laundering and terrorist financing.

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)

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

[27] Article 30(5), points (a) and (b) of the first subparagraph of the anti-money laundering directive as amended.

and Wales) (Civil Division) (United Kingdom), the Court 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 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. In the Court's view, such legislation exceeds the limits of what is strictly necessary and cannot be considered to be justified in a democratic society, as required by Article 15(1) of the directive read in the light of the above-mentioned articles of the Charter.

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.

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 data subjects 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 is 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.

II. Processing of personal data within the meaning of the relevant general rules

1. Scope of the general rules

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 [28] 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 [29] approving the conclusion of an agreement between the European Community and the United States on the processing and transfer of PNR data to the CBP by air carriers located within the territory of the Member States of the European Community.

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

As regards the decision on adequacy, the Court examined, first of all, whether the Commission could validly adopt its decision on the basis of Directive 95/46. In that context, it noted that it was apparent from the decision on adequacy that the transfer of PNR data to the CBP constituted processing operations concerning public security and the activities of the State in areas of criminal law. According to the Court, although PNR data were initially collected by airlines in the course of an activity which fell within the scope of EU law, namely the sale of an aeroplane ticket which provided entitlement to a

[28] 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 2004, L 235, p. 11).

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

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.

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.

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

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

In 2010, a Spanish national 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 the La Vanguardia 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 rejected the complaint against La Vanguardia, taking the view that the information in question had been lawfully published by it. However, it 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.

In this judgment, the Court also ruled on the territorial scope of Directive 95/46.

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

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.

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

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

On appeal by Mr Ryneš against a decision of the Městský soud v Praze (Municipal Court, Prague, Czechia) upholding the Office's decision, the Nejvyšší správní soud (Supreme Administrative Court, Czechia) asked the Court whether the recording made by Mr Ryneš in order to protect his life, health and property constituted processing of data not covered by Directive 95/46, on the ground that that recording had been made by a natural person for the purpose of carrying out exclusively purely personal or household activities, 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.

It noted in that regard that the protection of the fundamental right to private life guaranteed under Article 7 of the Charter requires that derogations and limitations in relation to the protection of personal data apply only in so far as is strictly necessary.

Since the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of the fundamental rights set out in the Charter, the exception provided for in the second indent of Article 3(2) of that directive must be narrowly construed. 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.

Judgment of 16 January 2024 (Grand Chamber), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

In order to examine whether there was any political influence over the Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (Federal Office for the Protection of the Constitution and for Counterterrorism, Austria), [30] the Nationalrat (National Council, Austria) set up a committee of inquiry ('the BVT Committee of Inquiry'). That committee heard WK as a witness. Despite his request for anonymisation, the minutes of his hearing, referring to his full family and first names, were published on the website of the Parlament Österreich (Austrian Parliament). Claiming that that disclosure of his identity was contrary to the GDPR and to Austrian legislation, WK lodged a complaint with the Österreichische Datenschutzbehörde (Data Protection Authority, Austria) ('the Datenschutzbehörde'). By a decision of 18 September 2019, the Datenschutzbehörde declared that it had no jurisdiction to decide on the complaint, stating that the principle of the separation of powers precluded it, as a body of the executive, from being able to exercise scrutiny over the BVT Committee of Inquiry, which is part of the legislature.

Following the decision of the Bundesverwaltungsgericht (Federal Administrative Court, Austria), which had upheld WK's action and annulled the decision of the Datenschutzbehörde, the latter brought an appeal on a point of law (Revision) before the Verwaltungsgerichtshof (Supreme Administrative Court) against the decision of the Bundesverwaltungsgericht (Federal Administrative Court).

In that context, the referring court asked the Court whether the activities of a committee of inquiry set up by the parliament of a Member State fall within the scope of the GDPR and whether that regulation applies where those activities concern the protection of national security.

[30] On 1 December 2021, this entity became the 'Direktion Staatsschutz und Nachrichtendienst' (Directorate for State Security and Intelligence Services, Austria).

In the first place, the Court recalled that Article 2(2)(a) of the GDPR, which provides that that regulation does not apply to the processing of personal data in the course of an activity which falls outside the scope of EU law, has the sole purpose of excluding from its scope the processing carried out by State authorities in the course of an activity which is intended to safeguard national security or which can be classified in the same category. Thus, the mere fact that an activity is characteristic of the State or of a public authority is not sufficient automatically to preclude the application of the GDPR to such an activity.

That interpretation, which follows from the absence of any distinction depending on the identity of the controller concerned, is borne out by Article 4(7) of the GDPR. [31]

The Court stated that the parliamentary nature of the BVT Committee of Inquiry does not mean that its activities fall outside the scope of the GDPR. The exception provided for in Article 2(2)(a) of that regulation refers only to categories of activities which, by their nature, fall outside the scope of EU law, and not to categories of persons. Accordingly, the fact that the processing of personal data is carried out by a committee of inquiry set up by the parliament of a Member State in the exercise of its power of scrutiny over the executive does not make it possible, as such, to establish that that processing is carried out in the course of an activity which falls outside the scope of EU law.

In the second place, the Court stated that, although it is for the Member States to define their essential security interests and to take appropriate measures to ensure them, [32] the mere fact that a national measure has been taken for the purpose of protecting national security cannot render EU law inapplicable and exempt the Member States from the need to comply with EU law. The exception provided for in Article 2(2)(a) of the GDPR refers only to categories of activities which, by their nature, fall outside the scope of EU law. In that regard, the fact that the controller is a public authority whose main activity is to safeguard national security cannot suffice, as such, to exclude from the scope of the GDPR the processing of personal data that it carries out in the course of its other activities.

In the present case, the political scrutiny exercised by the BVT Committee of Inquiry does not appear to constitute, as such, an activity intended to safeguard national security or falling within the same category. Accordingly, subject to verification by the referring court, that activity does not fall outside the scope of the GDPR.

That said, a parliamentary committee of inquiry can have access to personal data which, for reasons of national security, must enjoy specific protection. In that regard, restrictions on the obligations and rights flowing from the GDPR may be laid down, by

[31] This defines the concept of 'controller' as referring to 'the natural or legal person, public authority, department or other body which, alone or jointly with others, determines the purposes and means of the processing'.

[32] In accordance with Article 4(2) TEU.

way of a legislative measure, to safeguard, inter alia, national security. [33] Restrictions concerning the collection of personal data, the provision of information to data subjects and their access to those data, or the disclosure of those data, without the consent of the data subjects, to persons other than the controller, could thus be justified on that basis, on the condition that such restrictions respect the essence of the fundamental rights and freedoms of data subjects and are a necessary and proportionate measure in a democratic society.

The Court noted that it is nevertheless not apparent from the information available to it that the BVT Committee of Inquiry alleged that the disclosure of the personal data of the data subject was necessary for the safeguarding of national security and had its basis in a national legislative measure laid down to that end, which it is for the referring court to ascertain.

2. Concept of 'personal data'

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

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.

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

[33] Under Article 23 of the GDPR.

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

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

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

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

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

In the first place, the Court noted that, for information to be treated as 'personal data' within the meaning of Article 2(a) of Directive 95/46, there is no requirement that all the information enabling the identification of the data subject must be in the hands of one person. Furthermore, in the event that the examiner does not know the identity of the candidate when marking the answers submitted by that candidate in an examination, the body that set the examination, in this case the Institute of Chartered Accountants, does, nevertheless, have available the information needed to enable it easily and infallibly to identify that candidate through his or her 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 or her 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 or her intellect, thought processes, and judgment. In addition, the purpose of collecting those answers is to evaluate the candidate's professional abilities and his or her 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 or her 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 or her 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 held that the written answers provided by a candidate in a professional examination and any annotations by the examiner relating thereto can be verified, in particular, as to their accuracy and the need for their retention, within the meaning of Article 6(1)(d) and (e) of Directive 95/46 and may be rectified or erased under Article 12(b) thereof. Giving the candidate a right of access to those answers and annotations, under Article 12(a) of that directive, serves the purpose of the directive, which is to ensure the protection of that candidate's right to privacy with regard to the processing of data concerning him or her, irrespective of whether or not the candidate also has such a right of access under the national rules applicable to the examination procedure. However, the Court pointed out that the rights of access and rectification, under Article 12(a) and (b) of Directive 95/46, do not extend to the examination questions, which do not as such constitute the candidate's personal data.

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 (Grand Chamber), Lindqvist (C-101/01, EU:C:2003:596)

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

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

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

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

In that judgment (see also section II.1., entitled 'Scope of the general rules'), the Court had the opportunity to clarify the concept of 'processing of personal data' on the internet under Directive 95/46.

The Court held that the activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as processing of personal data when that information contains personal data. 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.

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

The Finnish data protection authority had adopted a decision prohibiting the Jehovah's Witnesses community from collecting or processing personal data in the course of door-to-door preaching carried out by its members unless the requirements for processing such data laid down in Finnish law were satisfied. The members of that community take notes in the course of their door-to-door preaching about visits to persons who are unknown to themselves or that community. Those data are collected, without the knowledge or consent of the data subjects, as a memory aid and in order to be retrieved for any subsequent visit. In that regard, the Jehovah's Witness community has given its members guidelines for taking such notes, which appear in at least one of its magazines devoted to preaching.

The Court held that the collection of personal data by members of a religious community in the context of door-to-door preaching and the subsequent processing of those data do not fall within the exceptions to the scope of Directive 95/46, since they constitute neither processing of personal data carried out in the exercise of activities referred to in the first indent of Article 3(2) of that directive, nor processing of personal data carried out by natural persons in the exercise of an activity which is solely personal or domestic in nature, within the meaning of the second indent of Article 3(2) of that directive.

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

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

Under the Latvian Law on road traffic, [34] information relating to the penalty points imposed on drivers of vehicles entered in that register is accessible to the public and disclosed by the CSDD to any person who so requests, without that person having to establish a specific interest in obtaining that information, including to economic operators for re-use. Uncertain as to the lawfulness of that legislation, B brought a constitutional appeal before the Latvijas Republikas Satversmes tiesa (Constitutional

[34] Article 14(2) of the Ceļu satiksmes likums (Law on road traffic) of 1 October 1997 (Latvijas Vēstnesis 1997, No 274/276).

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

The Latvijas Republikas Satversmes tiesa (Constitutional Court, Latvia) held that it must take account of the GDPR in its assessment of that constitutional law. Thus, it asked the Court to clarify the scope of several provisions of the GDPR with the aim of determining whether the Latvian Law on road traffic was compatible with that regulation.

In its judgment, the Court (Grand Chamber) held that the processing of personal data relating to penalty points constitutes 'processing of personal data relating to criminal convictions and offences', [35] for which the GDPR provides enhanced protection due to the particular sensitivity of the data involved.

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

Thus, first, that processing is not covered by the exception relating to the non-applicability of the GDPR to processing carried out in the course of an activity which falls outside the scope of EU law. [36] That exception must be regarded as being designed solely to exclude from the scope of that regulation the processing of personal data carried out by State authorities in the course of an activity which is intended to safeguard national security or of an activity which can be classified in the same category. Those activities encompass, in particular, those that are intended to protect essential State functions and the fundamental interests of society. Activities relating to road safety do not pursue that objective and consequently cannot be classified in the category of activities having the aim of safeguarding national security.

Secondly, the disclosure of personal data relating to penalty points is not processing covered by the exception providing for the non-applicability of the GDPR to processing of personal data carried out by the competent authorities in criminal matters either. [37] The Court found, in fact, that in carrying out that disclosure, the CSDD cannot be regarded as such a 'competent authority'. [38]

In order to determine whether access to personal data relating to road traffic offences, such as penalty points, amounts to processing of personal data relating to 'offences', [39]

---

35 Article 10 of the GDPR.

36 Article 2(2)(a) of the GDPR.

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

38 Article 3(7) of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89).

39 Article 10 of the GDPR.

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

Judgment of 5 December 2023 (Grand Chamber), Nacionalinis visuomenės sveikatos centras (C-683/21,* EU:C:2023:949*)

In 2020, in order better to manage the COVID-19 pandemic, the Lithuanian authorities decided to organise the acquisition of a mobile IT application. That application was to contribute to epidemiological follow-up by allowing for the registration and monitoring of the data of persons exposed to the COVID-19 virus.

To that end, the Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (National Public Health Centre under the Ministry of Health, Lithuania; 'the NVSC'), which was entrusted with that acquisition, contacted the company UAB 'IT sprendimai sėkmei' ('the company ITSS'), asking it to create such a mobile application. Emails concerning, inter alia, the questions to be included in that application were subsequently sent to that company by employees of the NVSC.

During the period from April to May 2020, the mobile application created by the company ITSS was made available to the public. As a result, 3 802 persons used that application and provided various data relating to them, as requested by the application. However, due to a lack of funding, the NVSC did not award any public contract to the company ITSS for the official acquisition of its mobile application and terminated the procedure relating thereto.

In the meantime, the national supervisory authority initiated an investigation concerning the processing of personal data resulting from the use of that application. By decision of that authority, adopted following the investigation, administrative fines were imposed both on the NVSC and on the company ITSS, which was considered to be a joint controller.

The NVSC has challenged that decision before the Vilniaus apygardos administracinis teismas (Regional Administrative Court, Vilnius, Lithuania). Having doubts as to the interpretation of several provisions of the GDPR, that court has made a request for a preliminary ruling to the Court of Justice.

In its ruling, the Grand Chamber of the Court clarified, among other things, the concept of 'processing'. In that regard, it stated that the use of personal data for the purposes of computer testing of a mobile application constitutes processing within the meaning of the GDPR. However, that is not the case where such data have been rendered anonymous in such a manner that the subject of those data is not or is no longer identifiable, or where it involves fictitious data which do not relate to an existing natural person.

Indeed, on the one hand, the question whether personal data are used for the purposes of IT testing or for another purpose has no bearing on whether the operation is classified as 'processing'. On the other hand, only processing that involves personal data can be described as 'processing' within the meaning of the GDPR. However, fictitious or anonymous data do not constitute personal data.

4. Concept of 'personal data filing system'

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

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

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

5. Concept of 'personal data controller'

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

In this case (see also sections II.3 and II.4, entitled 'Concept of "processing of personal data"' and 'Concept of "personal data filing system"'), the Court ruled on the responsibility of a religious community regarding the processing of personal data carried out in the context of a door-to-door preaching activity organised, coordinated and encouraged by that community.

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

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

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

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

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

In this case, the Court had the opportunity to develop the concept of 'controller' with regard to the integration of a 'plug-in' into a web page.

In this case, Fashion ID, a German company selling fashion clothing online, had inserted the 'like' social module of the Facebook social network on its website. The consequence of this insertion appears to be that, when a visitor consults the Fashion ID website, that visitor's personal data are transmitted to Facebook Ireland. It seems that that transmission occurs without that visitor being aware of it regardless of whether or not he or she is a member of the social network Facebook or has clicked on the Facebook 'Like' button.

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

The Court found, first of all, that the operator of a website, such as Fashion ID, may be regarded as a controller within the meaning of Article 2(d) of Directive 95/46. That liability is, however, limited to the operation or set of operations involving the processing of personal data in respect of which it actually determines the purposes and means, that is to say, the collection and disclosure by transmission of the data at issue. On the other hand, according to the Court, in the light of that information, it seems, at the outset, impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter, meaning that Fashion ID cannot be considered to be a controller in respect of those operations within the meaning of Article 2(d).

In addition, the Court emphasised that it is necessary for the operator of a website and the provider of a social module, such as Facebook Ireland, to each pursue a legitimate interest in those processing operations, within the meaning of Article 7(f) of Directive 95/46, in order for them to be justified.

Finally, the Court specified that the consent of the data subject, referred to in Article 2(h) and Article 7(a) of Directive 95/46, must be obtained by the operator of a website only in respect of the personal data processing operations for which that operator determines the purposes and means. In such a situation, the obligation to provide information set out in Article 10 of the Directive also applies to the data controller, although the information that must be provided to the data subject must relate only to the personal data processing operation or operations for which it determines the purposes and means.

Judgment of 5 December 2023 (Grand Chamber), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

In that case (see also section II.3, entitled 'Concept of "processing of personal data"'), the Court noted that an entity which has commissioned an undertaking to develop a mobile computer application and which has, in that context, participated in determining the purposes and means of the processing of personal data carried out by means of that application may be regarded as being responsible for the processing. [40] That finding cannot be called into question by the fact that that entity has not itself performed any processing operations in respect of such data, has not expressly agreed to the performance of specific operations for such processing or to that mobile application being made available to the public, and has not acquired the above-mentioned mobile application, unless, prior to that application being made available to the public, that entity expressly objected to such making available and to the processing of personal data resulting therefrom.

6. Concept of 'joint controller'

Judgment of 5 December 2023 (Grand Chamber), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

In this case (see also sections II.3 and II.5, entitled 'Concept of "processing of personal data"' and 'Concept of "personal data controller"'), the Court noted that the classification of two entities as being jointly responsible for processing does not presuppose either the existence of an agreement between those entities on the determination of the purposes and means of the processing of personal data or the existence of an agreement which lays down the conditions relating to joint responsibility for the processing. It is true that, under the GDPR, [41] joint controllers must, by means of an arrangement between them, determine in a transparent manner their respective responsibilities for compliance with the obligations under that regulation. However, the existence of such an arrangement constitutes not a precondition for two or more entities to be classified as 'joint controllers', but rather an obligation which the GDPR imposes on joint controllers, once they have been classified as such, for the purposes of compliance with their obligations under that regulation. Thus, such classification arises

[40] Within the meaning of Article 4(7) of the GDPR.
[41] Article 26(1) of the GDPR, read in the light of recital 79.

solely from the fact that several entities have participated in the determination of the purposes and means of processing.

As regards the joint determination, by the entities concerned, of the purposes and means of processing, the Court stated that their participation in that determination can take different forms and can result from a common decision taken by them or from converging decisions on their part. However, where the latter is the case, those decisions must complement each other in such a manner that they each have a tangible impact on the determination of the purposes and means of the processing.

7. Conditions governing the lawfulness of the processing of personal data

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

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

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

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

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

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.

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

In this judgment (see also section II.2.entitled "Concept of "personal data"'), the Court also ruled on whether Article 7(f), of Directive 95/46 precludes a provision of national law under which the provider of online media services may collect and use personal data relating to a user without that user's consent only in so far as that is necessary to enable and charge for the actual use of the online medium by the user in question and under which the purpose of ensuring the general operability of the online medium cannot justify the use of the data after the end of the current browsing session.

The Court held that Article 7(f) of Directive 95/46 precluded the legislation in question. Under that provision, personal data may be processed as provided for by that provision if processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject. In that instance, the German legislation had excluded, categorically and in general, the possibility of processing certain categories of personal data, without allowing the opposing rights and interests at issue to be balanced against each other in

a particular case. In doing so, it unlawfully reduced the scope of that principle laid down in Article 7(f) of Directive 95/46 by excluding the possibility of balancing the objective of ensuring the general operability of the online media against the interests or fundamental rights and freedoms of users.

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

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

In those circumstances, the Najvyšší súd Slovenskej republiky (Supreme Court of the Slovak Republic) referred to the Court, inter alia, the question whether the right to respect for private and family life, home and communications, enshrined in Article 7, and the right to the protection of personal data, enshrined in Article 8 of the Charter, could be interpreted as meaning that they do not permit a Member State to create, without the consent of the data subject, lists of personal data for the purposes of tax collection, with the result that the obtaining of personal data by the public authorities for the purposes of combating tax fraud would in itself present 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 are satisfied.

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.

The Court further held that the fact that a person is placed on the list at issue is likely to infringe some of his or her rights. Indeed, inclusion in that list could harm his or her reputation and affect his or her 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 data subject of fictitiously acting as a company director of the legal persons associated with him or her and of thus undermining the collection of taxes and the combating of tax fraud.

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.

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

Orange România SA provides mobile telecommunications services on the Romanian market. On 28 March 2018, the Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal (National Supervisory Authority for Personal Data Processing, Romania, the 'ANSPDCP') fined it for collecting and storing copies of its customers' identity documents without their express consent.

According to the ANSPDCP, during the period from 1 to 26 March 2018, Orange România entered into contracts for the provision of mobile telecommunication services that contain a clause stating that customers were informed and consented to the collection and retention of a copy of their identity document for identification purposes. The box relating to this clause was ticked by the data controller before the contract was signed.

It was against this background that the Tribunalul București (District Court, Bucharest, Romania) asked the Court to clarify the conditions under which the consent of customers to the processing of personal data may be considered valid.

The Court, recalled, first of all, that EU law [42] provides for a list of cases in which processing of personal data may be regarded as lawful. In particular, the data subject's

[42] Article 7 of Directive 95/46 and Article 6, of the GDPR.

consent must be free, specific, informed and unambiguous. [43] In that regard, consent is not validly given in the event of silence, boxes ticked by default or inactivity.

In addition, where the data subject's consent is given in a written statement which also covers other matters, this statement must be presented in a comprehensible and easily accessible form and be worded in clear and simple terms. To ensure that the data subject has genuine freedom of choice, the contractual stipulations must not mislead him or her as to the possibility of entering into the contract even if he or she refuses to consent to the processing of his or her data.

The Court stated that, since Orange România is the data controller, it must be able to demonstrate the lawfulness of the processing of personal data and therefore, in this case, the existence of valid consent from its customers. In that regard, given that the customers concerned did not appear to have ticked the box relating to the collection and storage of copies of their identity documents, the mere fact that this box was ticked was not such as to establish a positive expression of their consent. It is for the national court to carry out the necessary investigations to that end.

According to the Court, it is also for the national court to assess whether or not the contractual provisions at issue were liable to mislead the customers concerned as to the possibility of entering into the contract notwithstanding any refusal to consent to the processing of their data, in the absence of any details on this. Furthermore, in the event of a customer's refusal to consent to the processing of his or her data, the Court observed that Orange România required the customer to declare in writing that he or she did not consent to the collection and storage of the copy of his or her identity document. In the Court's view, such an additional requirement is likely to unduly affect the freedom to object to such collection and storage. In any event, as the company is required to establish that its customers have actively given their consent to the processing of their personal data, it cannot require them to actively refuse.

The Court therefore concluded that a contract relating to the provision of telecommunications services which contains a clause to the effect that the data subject has been informed of and has consented to the collection and storage of a copy of his or her identity document for identification purposes is not such as to demonstrate that that person has validly given his or her consent to that collection and storage, where the box referring to that clause was ticked by the data controller before the contract was signed, where the contractual stipulations of this contract are likely to mislead the data subject as to the possibility of entering into the contract in question even if he or she refuses to consent to the processing of his or her data, or when the free choice to oppose such collection and storage is unduly affected by this data controller, in that it requires the data subject to complete, in order to express his or her refusal to give consent to such processing, an additional form stating such refusal.

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

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

In that judgment (see also section II.3., entitled 'Concept of "processing of personal data"'), the Court held that the GDPR precludes the regulations requiring the Ceļu satiksmes drošības direkcija (Road Safety Directorate, Latvia) (the 'CSDD') to make data relating to penalty points imposed on vehicle drivers for road traffic offences accessible to the public, without the person requesting access having to show a specific interest in obtaining them. It noted that it had not been established that disclosure of personal data relating to the penalty points imposed for road traffic offences was necessary, particularly with regard to the objective of improving road safety invoked by the Latvian Government. Furthermore, according to the Court, neither the right of public access to official documents nor the right to freedom of information justified such legislation.

In that regard, the Court pointed out that the improvement of road safety, referred to in the Latvian legislation, is an objective of general interest recognised by the European Union and that Member States are therefore justified in classifying road safety as a 'task carried out in the public interest'. [44] However, it is not established that the Latvian scheme of disclosing personal data relating to penalty points is necessary to achieve the objective pursued. Indeed, on the one hand the Latvian legislature has a large number of methods which would have enabled it to achieve that objective by other means less restrictive of the fundamental rights of the data subjects. On the other hand, account must be taken of the sensitivity of the data relating to penalty points and of the fact that their public disclosure is liable to constitute a serious interference with the rights to respect for private life and to the protection of personal data, since it may give rise to social disapproval and result in stigmatisation of the data subject.

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

Moreover, for the same reasons, the Court held that the GDPR also precludes the Latvian legislation in so far as it authorises the CSDD to disclose the data on penalty points imposed on drivers of vehicles for road traffic offences to economic operators in order for the data to be re-used and disclosed to the public by them.

Finally, the Court stated that the principle of the primacy of EU law precludes the referring court, before which the action had been brought challenging the Latvian legislation classified by the Court as incompatible with EU law, from deciding that the

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

legal effects of that legislation be maintained until the date of delivery of its final judgment.

III. Processing of personal data within the meaning of sector-specific regulations

1. Processing of personal data in the electronic communications sector

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

At issue in this case was the refusal by a Spanish investigating magistrate to grant a request made in the context of an investigation into the robbery of a wallet and mobile telephone. More specifically, the judicial police had asked the judge to grant them access to user identification data for telephone numbers activated from the stolen phone for a period of 12 days from the date of the theft. The rejection was based on the grounds that the facts giving rise to the criminal investigation did not constitute a 'serious' offence - that is, under Spanish law, an offence punishable by a prison sentence of more than five years - since access to identification data is only possible for this type of offence.

After pointing out that access by public authorities to personal data held by electronic communications service providers in the context of criminal investigation proceedings falls within the scope of Directive 2002/58, the Court held that access to data intended to identify the holders of SIM cards activated on a stolen mobile telephone, such as the surnames, forenames and potentially addresses of those data subjects, constitutes interference with the fundamental rights to respect for private life and data protection enshrined in the Charter, in the absence of circumstances enabling that interference to be classified as 'serious', and regardless of whether or not the information relating to private life concerned is of a sensitive nature or whether or not the data subjects have suffered any disadvantages as a result of that interference. However, the Court made clear that such interference is not sufficiently serious to entail that access being limited - in the area of prevention, investigation, detection and prosecution of criminal offences - to the objective of fighting serious crime. Although Directive 2002/58 contains an exhaustive list of the objectives capable of justifying national legislation governing public authorities' access to the data concerned and thereby derogating from the principle of confidentiality of electronic communications, it being necessary for such access to correspond, genuinely and strictly, to one of those objectives, the Court observed that as regards the objective of preventing, investigating, detecting and prosecuting criminal

offences, the wording of Directive 2002/58 does not limit that objective to the fight against serious crime alone, but refers to 'criminal offences' generally.

Against that background, the Court stated that although, in its judgment in *Tele2 Sverige and Watson and Others*, [45] it had held that only the objective of fighting serious crime is capable of justifying public authorities' access to personal data retained by providers of communications services which, taken as a whole, allow precise conclusions to be drawn concerning the private lives of the persons whose data are concerned, such interpretation was based on the fact that the objective pursued by legislation governing that access must be proportionate to the seriousness of the interference with the fundamental rights in question that such access entails. Thus, in accordance with the principle of proportionality, serious interference in this area can only be justified by the objective of combating crime that must also be qualified as 'serious'. By contrast, when the interference is not serious, that access is capable of being justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally.

In the case at hand, the Court considered that access to only the data referred to in the request at issue could not be defined as a 'serious' interference with the fundamental rights of the persons whose data are concerned, as those data do not allow precise conclusions to be drawn in respect of their private lives. The Court concluded that the interference that access to such data entails can therefore be justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally, without it being necessary that those offences be defined as 'serious'.

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

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

It is against that background that proceedings were brought before the Investigatory Powers Tribunal (United Kingdom) (*Privacy International*, C-623/17), the Conseil d'État (Council of State, France) (*La Quadrature du Net and Others*, Joined Cases C-511/18 and C-512/18) and the Cour constitutionnelle (Constitutional Court, Belgium) (*Ordre des barreaux francophones et germanophone and Others*, C-520/18) concerning the lawfulness

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

of legislation adopted by certain Member States in those fields, imposing in particular an obligation on providers of electronic communications services to forward users' traffic and location data to a public authority or to retain such data in a general or indiscriminate way.

In two judgments delivered by the Grand Chamber on 6 October 2020, the Court held, firstly, that national regulations requiring providers of electronic communications services to retain traffic and location data or to transmit such data to the national security and intelligence authorities for that purpose fall within the scope of Directive 2002/58.

Next, the Court recalled that Directive 2002/58 [46] does not permit the exception to the obligation of principle to ensure the confidentiality of electronic communications and the related data and to the prohibition on storage of such data to become the rule. This means that the directive does not authorise the Member States to adopt, inter alia for the purposes of national security, legislative measures intended to restrict the scope of rights and obligations provided for in that directive, in particular the obligation to ensure the confidentiality of communications and traffic data, [47] unless such measures comply with the general principles of EU law, including the principle of proportionality, and the fundamental rights guaranteed by the Charter. [48]

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

Those obligations to forward and to retain such data in a general and indiscriminate way constitute particularly serious interferences with the fundamental rights guaranteed by the Charter, where there is no link between the conduct of the persons whose data are affected and the objective pursued by the legislation at issue. Similarly, the Court interpreted Article 23(1) of the GDPR, read in the light of the Charter, as precluding national legislation requiring providers of access to online public communication services and hosting service providers to retain, generally and indiscriminately, inter alia, personal data relating to those services.

---

46 Article 15(1) and (3) of Directive 2002/58.
47 Article 5(1) of Directive 2002/58.
48 In particular, Articles 7, 8 and 11 and Article 52(1) of the Charter.

By contrast, the Court held that, in situations where the Member State concerned is facing a serious threat to national security that is shown to be genuine and present or foreseeable, Directive 2002/58, read in the light of the Charter, does not preclude recourse to an order requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data. In that context, the Court specified that the decision imposing such an order, for a period that is limited in time to what is strictly necessary, must be subject to effective review either by a court or by an independent administrative body whose decision is binding, in order to verify that one of those situations exists and that the conditions and safeguards laid down are observed. In those circumstances, that directive also does not preclude the automated analysis of the data, inter alia traffic and location data, of all users of electronic communications systems.

The Court added that Directive 2002/58, read in the light of the Charter, does not preclude legislative measures that allow recourse to the targeted retention, limited in time to what is strictly necessary, of traffic and location data, which is limited, on the basis of objective and non-discriminatory factors, according to the categories of data subjects or using a geographical criterion. Likewise, that directive does not preclude legislative measures that provide for the general and indiscriminate retention of IP addresses assigned to the source of a communication, provided that the retention period is limited to what is strictly necessary, or measures that provide for such retention of data relating to the civil identity of users of electronic communications systems, the Member States not being required in the latter case to limit the retention period. Moreover, that directive does not preclude a legislative measure that allows recourse to the expedited retention of data available to service providers, where situations arise in which it becomes necessary to retain that data beyond statutory data-retention periods in order to shed light on serious criminal offences or acts adversely affecting national security, where such offences or acts have already been established or where their existence may reasonably be suspected.

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

Lastly, the Court addressed the issue of maintaining the temporal effects of national legislation held to be incompatible with EU law. In that regard, it ruled that a national court may not apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality which it is bound to make in respect of national

legislation imposing on providers of electronic communications services an obligation requiring the general and indiscriminate retention of traffic and location data that is incompatible with Directive 2002/58 read in the light of the Charter.

That being said, in order to give a useful answer to the referring court, the Court of Justice recalled that, as EU law currently stands, it is for national law alone to determine the rules relating to the admissibility and assessment, in criminal proceedings against persons suspected of having committed serious criminal offences, of evidence obtained by the retention of data in breach of EU law. However, the Court specified that Directive 2002/58, interpreted in the light of the principle of effectiveness, requires national criminal courts to disregard evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of such criminal proceedings, where those persons suspected of having committed criminal offences are not in a position to comment effectively on that evidence.

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

Criminal proceedings were brought in Estonia against H. K. on counts of theft, use of another person's bank card and violence against persons party to court proceedings. A court of first instance convicted H. K. of those offences and imposed a custodial sentence of two years. That judgment was then upheld on appeal. The reports relied upon in order to find H. K. guilty of those offences were drawn up, inter alia, on the basis of personal data generated in the context of the provision of electronic communications services. The Riigikohus (Supreme Court, Estonia), before which H. K. had lodged an appeal on a point of law, expressed doubts as to whether the conditions under which the investigating authority had access to those data were compatible with EU law. [49]

Those doubts concerned, first, whether the length of the period in respect of which the investigating authority has had access to the data is a criterion for assessing the seriousness of the interference, constituted by that access, with the fundamental rights of the data subjects. Thus, the referring court raised the question whether, where that period is very short or the quantity of data gathered is very limited, the objective of combating crime in general, and not only combating serious crime, is capable of justifying such an interference. Second, the referring court had doubts as to whether it is possible to regard the Estonian public prosecutor's office, in the light of the various duties which are assigned to it by national legislation, as an 'independent' administrative authority, within the meaning of the judgment in *Tele2 Sverige and Watson and Others*, [50] that is capable of authorising access of the investigating authority to the data concerned.

[49] More specifically, with Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.
[50] Judgment of 21 December 2016, *Tele2 Sverige and Watson and Others* (C-203/15 and C-698/15, EU:C:2016:970, paragraph 120).

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

So far as concerns the objective of preventing, investigating, detecting and prosecuting criminal offences, which is pursued by the legislation at issue, in accordance with the principle of proportionality the Court held that only the objectives of combating serious crime or preventing serious threats to public security are capable of justifying public authorities having access to a set of traffic or location data, that are liable to allow precise conclusions to be drawn concerning the private lives of the data subjects, and other factors relating to the proportionality of a request for access, such as the length of the period in respect of which access to such data is sought, cannot have the effect that the objective of preventing, investigating, detecting and prosecuting criminal offences in general is capable of justifying such access.

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

According to the Court, in order to ensure, in practice, that those conditions are fully observed, it is essential that access of the competent national authorities to retained data be subject to a prior review carried out either by a court or by an independent

administrative body, and that the decision of that court or body be made following a reasoned request by those authorities submitted, inter alia, within the framework of procedures for the prevention, detection or prosecution of crime. In cases of duly justified urgency, the review must take place within a short time.

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

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

Judgment of 5 April 2022 (Grand Chamber), Commissioner of An Garda Síochána and Others (C-140/20, EU:C:2022:258)

In this case, the request for a preliminary ruling was submitted by the Supreme Court (Ireland) in the context of civil proceedings brought by a person sentenced to life imprisonment for a murder committed in Ireland. The latter challenged the compatibility with EU law of certain provisions of the national law on the retention of data generated in the context of electronic communications. Under this law, traffic and location data relating to the defendant's telephone calls had been stored by electronic communication service providers and made accessible to the police authorities. The referring court's doubts related in particular to the compatibility with Directive 2002/58, read in the light of the Charter, of a system of the general and indiscriminate retention of those data, in connection with combating serious crime.

In its judgment, the Court, sitting as the Grand Chamber, confirmed, while also providing detail as to its scope, the case-law resulting from the judgment in *La Quadrature du Net and Others*, [51] by recalling that the general and indiscriminate retention of traffic and location data relating to electronic communications is not permitted for the purposes of combating serious crime and preventing serious threats to public security. It also confirms the case-law resulting from the judgment in *Prokuratuur (Conditions of access to data relating to electronic communications)*, [52] in particular as regards the obligation to make access by the competent national authorities to those retained data subject to a prior review carried out either by a court or by an administrative body that is independent in relation to a police officer.

The Court held, in the first place, that Directive 2002/58, read in the light of the Charter, precludes legislative measures which, as a preventive measure, for the purposes of combating serious crime and preventing serious threats to public security, provide for the general and indiscriminate retention of traffic and location data. Having regard, first, to the dissuasive effect on the exercise of the fundamental rights [53] which is liable to result from the retention of those data, and second, to the seriousness of the interference entailed by such retention, it is necessary for that retention to be the exception and not the rule in the system established by that directive, such that those data should not be retained systematically and continuously. Crime, even particularly serious crime, cannot be treated in the same way as a threat to national security, since to treat those situations in the same way would be likely to create an intermediate category between national security and public security for the purpose of applying to the latter the requirements inherent in the former.

However, Directive 2002/58, read in the light of the Charter, does not preclude legislative measures which provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of data subjects or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended. It adds that such a retention measure covering places or infrastructures that regularly receive a very high volume of visitors, or strategic locations, such as airports, stations, maritime ports or tollbooth areas, may allow the competent authorities to obtain information as to the presence in those places or geographical areas of persons using a means of electronic communication within those areas and to draw conclusions as to their presence and activity in those places or geographical areas for the purposes of combating serious crime. In any event, the fact that it may be difficult to provide a detailed definition of the circumstances and

---

51 Judgment of 6 October 2020, *La Quadrature du Net and Others* (C-511/18, C-512/18 and C-520/18, EU:C:2020:791).

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

53 Enshrined in Articles 7 to 11 of the Charter.

conditions under which targeted retention may be carried out is no reason for the Member States, by turning the exception into a rule, to provide for the general retention of traffic and location data.

That directive, read in the light of the Charter, also does not preclude legislative measures that provide, for the same purposes, for the general and indiscriminate retention of IP addresses assigned to the source of an internet connection for a period that is limited in time to what is strictly necessary, as well as data relating to the civil identity of users of electronic communications systems. As regards that latter aspect, the Court held more specifically that neither Directive 2002/58 nor any other act of EU law precludes national legislation, which has the purpose of combating serious crime, pursuant to which the purchase of a means of electronic communication, such as a pre-paid SIM card, is subject to a check of official documents establishing the purchaser's identity and the registration, by the seller, of that information, with the seller being required, should the case arise, to give access to that information to the competent national authorities.

The same is the case for legislative measures which allow, also for the purposes of combating serious crime and preventing serious threats to public security, recourse to an instruction requiring providers of electronic communications services by means of a decision of the competent authority that is subject to effective judicial review, to undertake, for a specified period of time, the expedited retention (quick freeze) of traffic and location data in their possession. Only actions to combat serious crime and, a fortiori, to safeguard national security are such as to justify that retention, on the condition that the measure and access to the retained data comply with the limits of what is strictly necessary. The Court recalled that such a retention measure may be extended to traffic and location data relating to persons other than those who are suspected of having planned or committed a serious criminal offence or acts adversely affecting national security, provided that those data can, on the basis of objective and non-discriminatory factors, shed light on such an offence or acts adversely affecting national security, such as data concerning the victim thereof, and his or her social or professional circle.

However, the Court indicated next that all the above-mentioned legislative measures must ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the data subjects have effective safeguards against risks of abuse. The various measures for the retention of traffic and location data may, at the choice of the national legislature and subject to the limits of what is strictly necessary, be applied concurrently.

In addition, the Court stated that to authorise, for the purposes of combating serious crime, access to those data retained generally and indiscriminately in order to address a serious threat to national security would be contrary to the hierarchy of objectives of public interest which may justify a measure taken pursuant to Directive 2002/58. That would be to allow access to be justified for an objective of lesser importance than that

which justified its retention, namely the safeguarding of national security, which would risk depriving of any effectiveness the prohibition on a general and indiscriminate retention for the purpose of combating serious crime.

In the second place, the Court held that Directive 2002/58, read in the light of the Charter, precludes national legislation pursuant to which the centralised processing of requests for access to data retained by providers of electronic communications services, issued by the police in the context of the investigation or prosecution of serious criminal offences, is the responsibility of a police officer, who is assisted by a unit established within the police service which enjoys a degree of autonomy in the exercise of its duties, and whose decisions may subsequently be subject to judicial review. First, such a police officer does not fulfil the requirements of independence and impartiality which must be met by an administrative body carrying out the prior review of requests for access issued by the competent national authorities, as he or she does not have the status of a third party in relation to those authorities. Second, while the decision of that officer may be subject to subsequent judicial review, that review cannot be substituted for a review which is independent and, except in duly justified urgent cases, undertaken beforehand.

In the third place, lastly, the Court confirmed its case-law according to which EU law precludes a national court from limiting the temporal effects of a declaration of invalidity which, pursuant to national law, it is bound to make as regards national legislation requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data, owing to the incompatibility of that legislation with Directive 2002/58. However, the Court recalled that the admissibility of evidence obtained by means of such retention is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness.

Judgment of 20 September 2022 (Grand Chamber), VD and SR (C-339/20 and C-397/20, EU:C:2022:703)

Following an investigation by the Autorité des marchés financiers (Financial Markets Authority, France; 'AMF'), criminal proceedings were brought against VD and SR, two natural persons charged with insider dealing, concealment of insider dealing, aiding and abetting, corruption and money laundering. In the course of that investigation, the AMF had used personal data from telephone calls made by VD and SR, generated on the basis of the French *Code des postes et des communications électroniques* (Post and Electronic Communications Code), in connection with the provision of electronic communications services.

In so far as the investigation into them was based on the traffic data provided by the AMF, VD and SR each brought an action before the Cour d'appel de Paris (Court of Appeal, Paris, France), relying on a plea alleging, in essence, infringement of Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the

Charter. Specifically, VD and SR, relying on the case-law arising from the judgment in *Tele2 Sverige and Watson and Others*, [54] challenged the fact that the AMF took the national provisions at issue as its legal basis for the collection of those data, whereas, according to them, those provisions, first, did not comply with EU law in so far as they provided for general and indiscriminate retention of connection data and, second, laid down no restrictions on the powers of the AMF's investigators to require the retained data to be provided to them.

By two judgments of 20 December 2018 and 7 March 2019, the Paris Court of Appeal rejected the action brought by VD and SR. When it rejected the plea referred to above, the court adjudicating on the substance of the case relied, inter alia, on the fact that the Market Abuse Regulation [55] allows the competent authorities to require, in so far as permitted by national law, existing data traffic records held by operators providing electronic communications services, where there is a reasonable suspicion of an infringement of the prohibition on insider dealing and where such records may be relevant to the investigation of that infringement.

VD and SR then brought an appeal before the Cour de cassation (Court of Cassation, France), the referring court in the present cases.

In that context, that court was uncertain how to reconcile Article 15(1) of Directive 2002/58, read in the light of the Charter, with the requirements under Article 12(2)(a) and (d) of the Market Abuse Directive [56] and Article 23(2)(g) and (h) of the Market Abuse Regulation. That uncertainty arose from the legislative measures at issue in the main proceedings, which provide, as a preventive measure, that operators providing electronic communications services are to retain traffic data generally and indiscriminately for one year from the day of recording for the purposes of combating market abuse offences including insider dealing. Should the Court of Justice find that the legislation on the retention of the connection data at issue in the main proceedings does not comply with EU law, the referring court was uncertain as to whether that legislation retains its effects provisionally, in order to avoid legal uncertainty and to allow the data previously collected and retained to be used for the purpose of detecting insider dealing and bringing criminal proceedings in respect of it.

By its judgment, the Court, sitting as the Grand Chamber, held that the general and indiscriminate retention of traffic data for a year from the date on which they were recorded by operators providing electronic communications services is not authorised, as a preventive measure, in order to combat market abuse offences. Furthermore, it confirmed its case-law to the effect that EU law precludes a national court from

---

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

55 Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Market Abuse Regulation) and repealing Directive 2003/6 and Commission Directives 2003/124/EC, 2003/125/EC and 2004/72/EC (OJ 2014 L 173, p. 1).

56 Directive 2003/6/EC of the European Parliament and of the Council of 28 January 2003 on insider dealing and market manipulation (market abuse) (OJ 2003 L 96, p. 16).

restricting the temporal effects of a declaration of invalidity which it is required to make with respect to provisions of national law that are incompatible with EU law.

The Court noted, first of all, that, in interpreting a provision of EU law, it is necessary not only to refer to its wording but also to consider its context and the objectives of the legislation of which it forms part.

As regards the wording of the provisions that are the subject of the reference for a preliminary ruling, the Court stated that, while Article 12(2)(d) of the Market Abuse Directive refers to the AMF's power to 'require existing telephone and existing data traffic records', Article 23(2)(g) and (h) of the Market Abuse Regulation refers to the power of that authority to require, first, 'data traffic records held by investment firms, credit institutions or financial institutions' and, second, to require, 'in so far as permitted by national law, existing data traffic records held by a telecommunications operator'. According to the Court, it is clear from the wording of those provisions that they merely provide a framework for the AMF's power to 'require' the data available to those operators, which corresponds to access to those data. Furthermore, the reference made to 'existing' records, such as those 'held' by those operators, suggests that the EU legislature did not intend to lay down rules governing the option open to the national legislature to impose an obligation to retain such records. According to the Court, that interpretation is, moreover, supported both by the context of those provisions and by the objectives pursued by the rules of which those same provisions form part.

As regards the context of the provisions that are the subject of the questions referred, the Court observed that, although, under the relevant provisions of the Market Abuse Directive and the Market Abuse Regulation, [57] the EU legislature intended to require the Member States to take the necessary measures to ensure that the competent financial authorities have a set of effective tools, powers and resources as well as the necessary supervisory and investigatory powers to ensure the effectiveness of their duties, those provisions make no mention of any option open to Member States of imposing, for that purpose, an obligation on operators providing electronic communications services to retain generally and indiscriminately traffic data, nor do they set out the conditions in which those data must be retained by those operators so that they can be submitted to the competent authorities where appropriate.

As regards the objectives pursued by the legislation at issue, the Court found that it is apparent, first, from the Market Abuse Directive and, second, from the Market Abuse Regulation [58] that the purpose of those instruments is to protect the integrity of EU financial markets and to enhance investor confidence in those markets, a confidence which depends, inter alia, on investors being placed on an equal footing and being

[57] Respectively, Article 12(1) of the Market Abuse Directive and Article 23(3) of the Market Abuse Regulation, read in the light of its recital 62.
[58] Respectively, recitals 2 and 12 of the Market Abuse Directive and Article 1 of the Market Abuse Regulation, read in the light of the latter's recitals 2 and 24.

protected against the improper use of inside information. The purpose of the prohibition on insider dealing laid down in those instruments [59] is to ensure equality between the contracting parties in stock-market transactions by preventing one of them that possesses inside information - and that is, therefore, in an advantageous position vis-à-vis other investors - from profiting from that information to the detriment of those that are unaware of it. Although, according to the Market Abuse Regulation, [60] connection data records constitute crucial, and sometimes the only, evidence to detect and prove the existence of insider dealing and market manipulation, the fact remains that that regulation makes reference only to records 'held' by operators providing electronic communications services and to the power of that competent financial authority to 'require' those operators to send 'existing' data. Thus, it is in no way apparent from the wording of that regulation that the EU legislature intended, by that regulation, to give Member States the power to impose on operators providing electronic communications services a general obligation to retain data. It follows that neither the Market Abuse Directive nor the Market Abuse Regulation can constitute the legal basis for a general obligation to retain the data traffic records held by operators providing electronic communications services for the purposes of exercising the powers conferred on the competent financial authority under those measures.

Next, the Court pointed out that Directive 2002/58 constitutes the reference act in relation to the retention and, more generally, the processing of personal data in the electronic communications sector, so that its interpretation, as given in the light of that directive, also governs the recordings of traffic data held by operators of electronic communications services which the authorities competent in financial matters, within the meaning of the Market Abuse Directive and the Market Abuse Regulation, [61] may order be delivered to them by those operators. The assessment of the lawfulness of the processing of recordings held by operators of electronic communications services [62] must, therefore, be made in the light of the conditions laid down by Directive 2002/58, as well as the Court's interpretation of that Directive in its case-law.

The Court found that the Market Abuse Directive and the Market Abuse Regulation, read in conjunction with Directive 2002/58 and in the light of the Charter, preclude legislative measures which, as a preventive measure, in order to combat market abuse offences including insider dealing, provide for the temporary, albeit general and indiscriminate, retention of traffic data, namely for a year from the date on which they were recorded, by operators providing electronic communications services.

Lastly, the Court confirmed its case-law according to which EU law precludes a national court from restricting the temporal effects of a declaration of invalidity which it is

59 Article 2(1) of the Market Abuse Directive and Article 8(1) of the Market Abuse Regulation.
60 Recital 62 of the Market Abuse Regulation.
61 Respectively, Article 11 of the Market Abuse Directive and Article 22 of the Market Abuse Regulation.
62 Within the meaning of Article 12(2)(d) of the Market Abuse Directive and Article 23(2)(g) and (h) of the Market Abuse Regulation.

required to make, under national law, with respect to provisions of national law which, first, require operators providing electronic communications services to retain generally and indiscriminately traffic data and, second, allow such data to be submitted to the competent financial authority, without prior authorisation from a court or independent administrative authority, owing to the incompatibility of those provisions with Directive 2002/58 read in the light of the Charter. However, the Court recalled that the admissibility of evidence obtained by means of such retention is, in accordance with the principle of procedural autonomy of the Member States, a matter for national law, subject to compliance, inter alia, with the principles of equivalence and effectiveness. The latter principle requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of data in breach of EU law if the data subjects are not in a position to comment effectively on that information and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact.

Ruling of 30 April 2024 (plenary session), La Quadrature du Net and others (Personal data and action to combat counterfeiting) (C-470/21, EU:C:2024:370)

Ruling on a preliminary ruling from the Conseil d'État (Council of State, France), the Court, sitting as the full Court, developed its case-law on Directive 2002/58 by providing clarifications concerning (i) the conditions under which the general retention of IP addresses by providers of electronic communications services cannot be regarded as entailing a serious interference with the rights to respect for private life, to the protection of personal data and to freedom of expression guaranteed by the Charter [63] and (ii) the possibility, for a public authority, to access certain personal data retained in accordance with those conditions, in the context of combating infringements of intellectual property rights committed online.

In that case, four associations submitted a request to the Premier ministre (Prime Minister, France) seeking the repeal of the decree relating to the automated processing of personal data. [64] As that request was not acted upon, those associations brought an action before the Conseil d'État (Council of State) seeking the annulment of that implicit rejection decision. In their view, that decree and the provisions which constitute its legal basis [65] infringe EU law.

Under French law, the Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet (High Authority for the dissemination of works and the protection of

63 Articles 7, 8 and 11 of the Charter.

64 Decree no. 2010-236, of 5 March 2010, relating to the automated processing of personal data authorised by Article L. 331-29 of the Intellectual Property Code entitled 'Système de gestion des mesures pour la protection des œuvres sur internet' (System for the management of measures to protect works on the Internet) (JORF [Official Journal of the French Republic] No. 56 of 7 March 2010, text No. 19), as amended by Decree No. 2017-924, of 6 May 2017, on the management of copyright and related rights by a rights management organisation and amending the Intellectual Property Code (JORF No. 109 of 10 May 2017, text No. 176).

65 In particular, the third to fifth paragraphs of Article L. 331-21 of the Intellectual Property Code.

rights on the internet) ('Hadopi') is authorised – in order to be able to identify those responsible for infringements of copyright or related rights committed online – to access certain data that providers of electronic communications services are required to retain. Those data relate to the civil identity of a data subject associated with his or her IP address previously collected by right-holder organisations. Once the holder of the IP address used for activities constituting such infringements is identified, Hadopi follows the 'graduated response' procedure. Specifically, it is empowered to send that person two recommendations, which are similar to warnings, and, if the activities persist, a letter notifying him or her that those activities are subject to criminal prosecution. Finally, it is entitled to refer the matter to the public prosecution service with a view to the prosecution of that person. [66]

In that context, the Conseil d'État (Council of State, France) referred questions to the Court concerning the interpretation of Directive 2002/58, read in the light of the Charter. [67]

In the first place, as regards the retention of data relating to civil identity and the associated IP addresses, the Court stated that the general and indiscriminate retention of IP addresses does not necessarily constitute, in every case, a serious interference with the rights to respect for private life, protection of personal data and freedom of expression guaranteed by the Charter.

The obligation to ensure such retention may be justified by the objective of combating criminal offences in general, where it is genuinely ruled out that that retention could give rise to serious interferences with the private life of the data subject due to the possibility of drawing precise conclusions about that person by, inter alia, linking those IP addresses with a set of traffic or location data.

Accordingly, a Member State which intends to impose such an obligation on providers of electronic communications services must ensure that the arrangements for the retention of those data are such as to rule out the possibility that precise conclusions could be drawn about the private lives of the data subjects.

The Court specified that, to that end, the retention arrangements must relate to the very manner in which the retention is structured; in essence, that retention must be organised in such a way as to guarantee a genuinely watertight separation of the different categories of data retained. Accordingly, the national rules relating to those arrangements must ensure that each category of data, including data relating to civil identity and IP addresses, is kept completely separate from other categories of retained data and that that separation is genuinely watertight, by means of a secure and reliable

[66] With effect from 1 January 2022, Hadopi was merged with the Conseil supérieur de l'audiovisuel (Higher Council for the audiovisual sector, 'CSA'), another independent public authority, to form the Autorité de régulation de la communication audiovisuelle et numérique (Authority for the Regulation of Audiovisual and Digital Communications, 'ARCOM'). The graduated response procedure has, however, remained essentially unchanged.

[67] Article 15(1) of Directive 2002/58.

computer system. In addition, in so far as those rules provide for the possibility of linking the retained IP addresses with the civil identity of the data subject for the purpose of combating infringements, they must permit such linking only through the use of an effective technical process which does not undermine the effectiveness of the watertight separation of those categories of data. The reliability of that separation must be subject to regular review by a third-party public authority. Provided that the applicable national legislation lays down such strict requirements, the interference resulting from the retention of IP addresses cannot be regarded as 'serious'.

Consequently, the Court concluded that, in the presence of a legislative framework ensuring that no combination of data will allow precise conclusions to be drawn about the private life of the persons whose data are retained, Directive 2002/58, read in the light of the Charter, does not preclude a Member State from imposing an obligation to retain IP addresses, in a general and indiscriminate manner, for a period not exceeding what is strictly necessary, for the purposes of combating criminal offences in general.

In the second place, as regards access to data relating to the civil identity associated with IP addresses, the Court held that Directive 2002/58, read in the light of the Charter, does not preclude, in principle, national legislation which allows a public authority to access those data retained by providers of electronic communications services separately and in a genuinely watertight manner, for the sole purpose of enabling that authority to identify the holders of those addresses suspected of being responsible for infringements of copyright and related rights on the internet and to take measures against them. In that case, the national legislation must prohibit the officials having such access (i) from disclosing in any form whatsoever information concerning the content of the files consulted by those holders except for the sole purpose of referring the matter to the public prosecution service, (ii) from tracking in any way the browsing route of those holders and (iii) from using those IP addresses for purposes other than the adoption of those measures.

In that context, the Court noted inter alia that, even though the freedom of expression and the confidentiality of personal data are primary considerations, those fundamental rights are nevertheless not absolute. In balancing the rights and interests at issue, those fundamental rights must yield on occasion to other fundamental rights or public-interest imperatives, such as the maintenance of public order and the prevention of crime or the protection of the rights and freedoms of others. This is, in particular, the case where the weight given to those primary considerations is such as to hinder the effectiveness of a criminal investigation, in particular by making it impossible or excessively difficult to identify effectively the perpetrator of a criminal offence and to impose a penalty on him or her.

In the same context, the Court also referred to its case-law according to which, as regards the combating of criminal offences infringing copyright or related rights committed online, the fact that accessing IP addresses may be the only means of investigation enabling the data subject to be identified tends to show that the retention

of and access to those addresses is strictly necessary for the attainment of the objective pursued and therefore meets the requirement of proportionality. Moreover, not to allow such access would carry a real risk of systemic impunity for criminal offences committed online or the commission or preparation of which is facilitated by the specific characteristics of the internet. The existence of such a risk constitutes a relevant factor for the purposes of assessing, when balancing the various rights and interests in question, whether an interference with the rights to respect for private life, protection of personal data and freedom of expression is a proportionate measure in the light of the objective of combating criminal offences.

In the third place, ruling on whether access by the public authority to data relating to the civil identity associated with an IP address must be subject to a prior review by a court or an independent administrative body, the Court considered that the requirement of such prior review applies where, within the framework of national legislation, that access carries the risk of a serious interference with the fundamental rights of the data subject in that it could allow that public authority to draw precise conclusions about the private life of that person and, as the case may be, to establish a detailed profile of that person. Conversely, that requirement of prior review is not intended to apply where the interference with fundamental rights cannot be classified as serious.

In that regard, the Court stated that, where a retention framework which ensures a watertight separation of the various categories of retained data is put in place, access by the public authority to the data relating to the civil identity associated with the IP addresses is not, in principle, subject to the requirement of a prior review. Such access for the sole purpose of identifying the holder of an IP address does not, as a general rule, constitute a serious interference with the above-mentioned rights.

However, the Court did not rule out the possibility that, in atypical situations, there is a risk that, in the context of a procedure such as the graduated response procedure at issue in the main proceedings, the public authority may be able to draw precise conclusions about the private life of the data subject, in particular where that person engages in activities infringing copyright or related rights on peer-to-peer networks repeatedly, or on a large scale, in connection with protected works of particular types, revealing potentially sensitive information about aspects of that person’s private life.

In the present case, an IP address holder may be particularly exposed to such a risk when the public authority must decide whether or not to refer the matter to the public prosecution service with a view to the prosecution of that person. The intensity of the infringement of the right to respect for private life is likely to increase as the graduated response procedure, which is a sequential process, progresses through its various stages. The competent authority’s access to all the data relating to the data subject and accumulated during the various stages of this procedure may make it possible to draw precise conclusions about the data subject’s private life. Consequently, national legislation must provide for a prior check to be carried out before the public authority can link civil identity data to such a set of data, and before any letter of notification is

sent stating that the data subject has committed acts liable to result in criminal proceedings. That review must, moreover, preserve the effectiveness of the graduated response procedure by making it possible, in particular, to identify cases where the unlawful conduct in question has been again repeated. To that end, that procedure must be organised and structured in such a way that the civil identity data of a person associated with IP addresses previously collected on the internet cannot automatically be linked, by the persons responsible for the examination of the facts within the competent public authority, with information which the latter already has and which could enable precise conclusions to be drawn about the private life of that person.

Furthermore, as regards the object of the prior review, the Court noted that, where the data subject is suspected of having committed an offence which falls within the scope of criminal offences in general, the court or independent administrative body responsible for that review must refuse access where that access would allow the public authority to draw precise conclusions about the private life of that person. However, even access allowing such precise conclusions to be drawn should be authorised in cases where the data subject is suspected of having committed an offence considered by the Member State concerned to undermine a fundamental interest of society and which thus constitutes a serious crime.

The Court also stated that a prior review may in no case be entirely automated since, in the case of a criminal investigation, such a review requires that a balance be struck between, on the one hand, the legitimate interests relating to combating crime and, on the other hand, respect for private life and protection of personal data. That balancing requires the intervention of a natural person, all the more so where the automatic nature and large scale of the data processing in question poses privacy risks.

Thus, the Court concluded that the possibility, for the persons responsible for examining the facts within that public authority, of linking such data relating to the civil identity of a person associated with an IP address with files containing information that reveals the title of protected works the making available of which on the internet justified the collection of IP addresses by right-holder organisations is subject, in cases where the same person again repeats an activity infringing copyright or related rights, to review by a court or an independent administrative body. That review cannot be entirely automated and must take place before any such linking, as such linking is capable, in such circumstances, of enabling precise conclusions to be drawn about the private life of the person whose IP address has been used for activities that may infringe copyright or related rights.

In the fourth and last place, the Court noted that the data processing system used by the public authority must be subject, at regular intervals, to a review by an independent body acting as a third party in relation to that public authority. The purpose of that control is to verify the integrity of the system, including the effective safeguards against the risks of abusive or unlawful access to or use of those data, and its effectiveness and reliability in detecting potential offending conduct.

In that context, the Court observed that, in the present case, the automated processing of personal data carried out by the public authority on the basis of the information relating to instances of counterfeiting detected by the right-holder organisations is likely to involve a certain number of false positives and, above all, the risk that a potentially very significant amount of personal data may be misused by third parties for unlawful or abusive purposes, which explains the need for such a review. In addition, it added that that processing must comply with the specific rules for the protection of personal data laid down by Directive 2016/680. In this case, even if the public authority does not have decision-making powers of its own in the context of the 'graduated response' procedure, it must be classified as a 'public authority' involved in the prevention and detection of criminal offences and therefore falls within the scope of that directive. Thus, the persons involved in such a procedure must enjoy a set of substantive and procedural safeguards referred to in Directive 2016/680; it is for the referring court to ascertain whether the national legislation provides for those safeguards.

2. Processing of personal data in criminal matters

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

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

However, even before that red notice was published, a procedure investigating WS, which related, according to the referring court, to the same acts as those which formed the basis for that notice, had been carried out in Germany. That procedure was definitively discontinued in 2010 after a sum of money had been paid by WS as part of a specific settlement procedure provided for under German criminal law. The Bundeskriminalamt (Federal Criminal Police Office, Germany) subsequently informed INTERPOL that, in its view, as a result of that earlier procedure, the ne bis in idem principle was applicable in the present case. That principle, which is enshrined in both Article 54 of the Convention implementing the Schengen Agreement [68] and Article 50 of

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

the Charter prohibits a person whose trial has been finally disposed of from being prosecuted again for the same offence.

In 2017, WS brought an action against the Federal Republic of Germany before the Verwaltungsgericht Wiesbaden (Administrative Court, Wiesbaden, Germany) seeking an order requiring that Member State to take the measures necessary to arrange for that red notice to be withdrawn. In that regard, WS relied not only on an infringement of the ne bis in idem principle, but also on an infringement of his right to freedom of movement, as guaranteed under Article 21 TFEU, since he could not travel to any State that is a party to the Schengen Agreement or to any Member State without risking arrest. He also argued that, due to those infringements, the processing of his personal data appearing in the red notice was contrary to Directive 2016/680, which concerns the protection of personal data in criminal matters. [69]

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

In its Grand Chamber judgment, the Court found, inter alia, that the provisions of Directive 2016/680, read in the light of Article 54 of the CISA and Article 50 of the Charter, must be interpreted as not precluding the processing of personal data appearing in a red notice issued by INTERPOL in the case where it has not been established, by means of such a judicial decision, that the ne bis in idem principle applies in respect of the acts on which that notice is based, provided that such processing satisfies the conditions laid down by that directive.

As regards the matter of personal data appearing in an INTERPOL red notice, the Court noted that any operation performed on those data, such as registering them in a Member State's filing system of wanted persons, constitutes 'processing' which falls under Directive 2016/680. [70] Additionally, the Court found, first, that that processing pursues a legitimate objective and, secondly, that it cannot be regarded as unlawful solely on the ground that the ne bis in idem principle may apply to the acts on which that red notice is based. [71] That processing, by the authorities of the Member States, may indeed be indispensable precisely in order to determine whether that principle applies.

---

[69] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89).

[70] See Article 2(1) and Article 3(2) of Directive 2016/680.

[71] See Article 4(1)(b) and Article 8(1) of Directive 2016/680.

In those circumstances, the Court also found that Directive 2016/680, read in the light of Article 54 of the CISA and Article 50 of the Charter, does not preclude the processing of personal data appearing in a red notice where no final judicial decision has established that the ne bis in idem principle applies in the relevant case. However, such processing must be carried out in compliance with the conditions laid down by that directive. In that regard, it must, inter alia, be necessary for the performance of a task carried out by a competent national authority for purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. [72]

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

Judgment of 21 June 2022 (Grand Chamber), Ligue des droits humains (C-817/19, EU:C:2022:491)

In this case (see also section I.1., entitled 'Compliance of secondary EU law with the right to the protection of personal data'), after finding the PNR Directive valid, the Court clarified the interpretation of some of its provisions. [73]

First, it pointed out that the directive lists exhaustively the objectives pursued by the processing of PNR data. Therefore, that directive precludes national legislation which authorises PNR data to be processed for purposes other than the fight against terrorist offences and serious crime. Thus, national legislation that includes, among the purposes for which PNR data are to be processed, monitoring activities within the remit of the intelligence and security services is liable to disregard the exhaustive nature of that list. Likewise, the system established by the PNR Directive cannot be provided for the purposes of improving border controls and combating illegal immigration. It also follows that PNR data may not be retained in a single database that may be consulted both for the purposes of the PNR Directive as well as for other purposes.

Second, the Court explained the concept of an independent national authority, competent to verify whether the conditions for the disclosure of PNR data, for the purposes of their subsequent assessment, are met and to approve such disclosure. In

[72] See Article 1(1) and Article 8(1) of Directive 2016/680.

[73] In particular, Article 2 ('Application of this Directive to intra-EU flights'), Article 6 ('Processing of PNR data') and Article 12 ('Period of data retention and depersonalisation') of the PNR Directive.

particular, the authority put in place as the PIU cannot be classified as such since it is not a third party in relation to the authority which requests access to the data. Since the members of its staff may be agents seconded from the authorities entitled to request such access, the PIU appears necessarily linked to those authorities. Accordingly, the PNR Directive precludes national legislation pursuant to which the authority put in place as the PIU is also designated as a competent national authority with power to approve the disclosure of PNR data upon expiry of the period of six months after the transfer of those data to the PIU.

Third, as regards the retention period of PNR data, the Court held that Article 12 of the PNR Directive, read in the light of Articles 7 and 8 as well as Article 52(1) of the Charter, precludes national legislation which provides for a general retention period of five years for PNR data, applicable indiscriminately to all air passengers.

According to the Court, after expiry of the initial retention period of six months, the retention of PNR data does not appear to be limited to what is strictly necessary in respect of those air passengers for whom neither the advance assessment nor any verification carried out during the initial six-month retention period nor any other circumstance have revealed the existence of objective evidence – such as the fact that the PNR data of the passengers concerned gave rise to a verified positive match during the advance assessment – that would be capable of establishing a risk that relates to terrorist offences or serious crime having an objective link, even if only an indirect one, with those passengers' air travel. By contrast, it took the view that, during the initial period of six months, the retention of the PNR data of all air passengers subject to the system established by that directive does not appear, as a matter of principle, to go beyond what is strictly necessary.

Fourth, the Court provided guidance on the possible application of the PNR Directive, for the purposes of combating terrorist offences and serious crime, to other modes of transport carrying passengers within the European Union. The directive, read in the light of Article 3(2) TEU, Article 67(2) TFEU and Article 45 of the Charter, precludes a system for the transfer and processing of the PNR data of all transport operations carried out by other means within the European Union in the absence of a genuine and present or foreseeable terrorist threat with which the Member State concerned is confronted. In such a situation, as in the case of intra-EU flights, the application of the system established by the PNR Directive must be limited to PNR data of transport operations relating, inter alia, to certain routes or travel patterns, or to certain stations or certain seaports for which there are indications that are such as to justify that application. It is for the Member State concerned to select the transport operations for which there are such indications and to review regularly that application in accordance with changes in the circumstances that justified their selection.

IV. Transfer of personal data to third countries

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

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

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

Given, first, the state of development of the internet at the time Directive 95/46/was drawn up and, second, the absence of criteria applicable to use of the internet in Chapter IV in which Article 25 appears and which is intended to allow the Member States to monitor transfers of personal data to third countries and to prohibit such transfers where those countries do not offer an adequate level of protection, 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.

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

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, [74] found that, in the context of the 'safe harbour regime', [75] the United States ensured an adequate level of protection for the personal data transferred.

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

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

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

The Court declared the Commission 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, Article 1 of that decision failed to comply with the requirements laid down in Article 25(6) of Directive 95/46, 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 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.

In addition, the Court declared Article 3 of Decision 2000/520 to be invalid in so far as it denied the national supervisory authorities the powers which they derive from Article 28 of Directive 95/46, where a person puts forward matters that may call 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. The Court concluded that the invalidity of Articles 1 and 3 of Decision 2000/520 affected the validity of that decision in its entirety.

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 that data.

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. 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 has 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 its subsequent use, for purposes which are specific, strictly restricted and capable of justifying the interference which both access to that data and its 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.

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

On 26 July 2017, the Court ruled for the first time on the compatibility of a draft international agreement with the Charter, and in particular with the provisions relating to respect for privacy and the protection of personal data.

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

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

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

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

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

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 data subjects, 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.).

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 is 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.

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.

In the third place, the Court found that the fundamental right to respect for private life, enshrined in Article 7 of the Charter, implies that the data subject must be able to ensure that his or her personal data are processed accurately and lawfully. 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 Passenger Name Record 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, such 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.

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

The GDPR provides that the transfer of such data to a third country may, in principle, take place only if the third country in question ensures an adequate level of data protection. According to the GDPR, the Commission may find that a third country ensures, by reason of its domestic law or its international commitments, an adequate level of protection. [76] In the absence of an adequacy decision, such a transfer may take place only if the personal-data exporter established in the European Union has provided appropriate safeguards, which may arise, in particular, from standard data-protection clauses adopted by the Commission, and if data subjects have enforceable rights and

[76] Article 45 of the GDPR.

effective legal remedies. [77] Furthermore, the GDPR details the conditions under which such a transfer may take place in the absence of an adequacy decision or appropriate safeguards. [78]

Maximillian Schrems, an Austrian national residing in Austria, began using Facebook in 2008. As in the case of other users residing in the European Union, some or all of Mr Schrems's personal data were transferred by Facebook Ireland to servers belonging to Facebook Inc., located in the United States, to undergo processing. Mr Schrems lodged a complaint with the Irish supervisory authority seeking, in essence, to prohibit those transfers. He claimed that the law and practices in the United States do not offer sufficient protection against access by the public authorities to the data transferred to that country. That complaint was rejected on the ground, inter alia, that, in Decision 2000/520 [79] the Commission had found that the United States ensured an adequate level of protection. In a judgment delivered on 6 October 2015, the Court of Justice, before which the High Court (Ireland) had referred questions for a preliminary ruling, declared that decision invalid ('the *Schrems I* judgment'). [80]

Following the *Schrems I* judgment and the subsequent annulment by the referring court of the decision rejecting Mr Schrems's complaint, the Irish supervisory authority asked Mr Schrems to reformulate his complaint in the light of the declaration by the Court that Decision 2000/520 was invalid. In his reformulated complaint, Mr Schrems claimed that the United States does not offer sufficient protection of data transferred to that country. He sought the suspension or prohibition of future transfers of his personal data from the European Union to the United States, which Facebook Ireland then carried out pursuant to the standard data-protection clauses set out in the annex to Decision 2010/87. [81] Taking the view that the outcome of Mr Schrems' complaint depended, in particular, on the validity of Decision 2010/87, the Irish supervisory authority brought proceedings before the High Court, requesting that it refer questions to the Court of Justice for a preliminary ruling. Following the opening of this procedure, the Commission adopted Decision (EU) 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield. [82]

By its request for a preliminary ruling, the referring court asked the Court of Justice whether the GDPR applies to transfers of personal data pursuant to the standard data-protection clauses in Decision 2010/87, what level of protection is required by the GDPR

77 Article 46(1) and (2)(c) of the GDPR.
78 Article 49 of the GDPR.
79 Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (OJ 2000 L 215, p. 7).
80 Judgment of the Court of 6 October 2015, *Schrems*, C-362/14, EU:C:2015:650.
81 Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (OJ 2010 L 39, p. 5), as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 (OJ 2016 L 344, p. 100).
82 Commission Implementing Decision of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (OJ 2016, L 207, p. 1).

in connection with such a transfer and what obligations are incumbent on supervisory authorities in those circumstances. The High Court also raised the question of the validity both of Decision 2010/87 and of Decision 2016/1250.

The Court found that an examination of Decision 2010/87 in the light of the Charter did not reveal any factor of such a kind as to affect its validity. However, the Court declared Decision 2016/1250 invalid.

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

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

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

Next, the Court examined the validity of Decision 2010/87. The Court considered that the validity of that decision was not called into question by the mere fact that the standard data-protection clauses in that decision do not, given that they are contractual in nature, bind the authorities of the third country to which data may be transferred. However, that validity, the Court added, depends on whether the decision includes effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law and that transfers of personal data pursuant to

such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them. The Court found that Decision 2010/87 establishes such mechanisms. In that regard, the Court pointed out, in particular, that that decision imposes an obligation on a data exporter and the recipient of the data to verify, prior to any transfer, whether that level of protection is respected in the third country concerned and that the decision requires the recipient to inform the data exporter of any inability to comply with the standard data-protection clauses, the latter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the former.

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

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

V. Protection of personal data on the Internet

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

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

In this judgment (see also sections II.1. and II.3., entitled 'Scope of the general rules' and 'Concept of "processing of personal data"'), the Court clarified the scope of the rights of access to and opposition to the processing of personal data on the Internet, as provided for in Directive 95/46.

Thus, when ruling on the question of the extent of the responsibility of the operator of a search engine on the internet, the Court held, in essence, that, in order to comply with the right of access and the right to object guaranteed by Articles 12(b) and 14(a) of Directive 95/46, and in so far as the conditions laid down by those provisions are satisfied, that operator is, in certain circumstances, obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages published by third parties and containing information relating to that person. The Court stated that such an obligation may also exist where that name or the information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

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. 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. 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.

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 access to the information in question, on account of inclusion in the list of results.

2. Processing of personal data and intellectual property rights

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

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 data subjects.

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

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

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'), [83] Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, [84] Directive 2004/48/EC on the

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

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

enforcement of intellectual property rights, [85] 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.

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

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

In that context, the Högsta domstolen, hearing an appeal in cassation, asked the Court whether EU law precludes the application of a national provision which is based on Article 8 of Directive 2004/48/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

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

applicant had adduced clear evidence of the infringement of a particular copyright and that the measure was proportionate.

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

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.

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

3. De-referencing of personal data

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

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

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

an operator of a search engine when handling a request for de-referencing under Directive 95/46.

First, the Court recalled that the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of data concerning health or sex life, is prohibited, [86] subject to certain exceptions and derogations. As regards the processing of data relating to offences, criminal convictions or security measures, such processing may in principle be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law. [87]

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

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

Secondly, the Court held that when the operator receives a request for de-referencing relating to sensitive data, it is in principle required, subject to certain exceptions, to accede to that request. As regards those exceptions, the operator may, inter alia, refuse to accede to such a request if it establishes that the links lead to data which are manifestly made public by the data subject, [88] provided that the referencing of those links satisfies the other conditions of lawfulness of the processing of personal data and unless the data subject has the right to object to that referencing on grounds relating to the data subject's particular situation. [89]

In any event, when the operator of a search engine receives a request for de-referencing, it must ascertain whether the inclusion in the list of results displayed following a search on the basis of the data subject's name of the link to a web page on which sensitive data are published is strictly necessary for protecting the freedom of information of internet users potentially interested in accessing that web page by means of such a search. In that regard, the Court pointed out that while the rights to privacy

86 Article 8(1) of Directive 95/46 and Article 9(1) of Regulation 2016/679.
87 Article 8(5) of Directive 95/46 and Article 10 of Regulation 2016/679.
88 Article 8(2)(e) of Directive 95/46 and Article 9(2)(e) of Regulation 2016/679.
89 Article 14(a) of Directive 95/46 and Article 21(1) of Regulation 2016/679.

and the protection of personal data override, as a general rule, the freedom of information of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

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

Judgment of 24 September 2019 (Grand Chamber), Google (Territorial scope of dereferencing) (C-507/17,* EU:C:2019:772*)

The CNIL served formal notice on Google that, where that company grants a request for de-referencing, it must remove from the list of results displayed on all its search engine's domain name extensions, following a search conducted on the basis of the name of the data subject, links to web pages containing personal data concerning that data subject. Following Google's refusal to comply with that formal notice, the CNIL imposed a penalty of EUR 100 000 on that company. The French Council of State, in the proceedings brought before it by Google, asked the Court to clarify the territorial scope of the obligation for a search engine operator to give effect to the right to de-referencing under Directive 95/46.

First of all, the Court recalled the possibility, under EU law, for natural persons to assert their right to de-referencing against a search engine operator that has one or more establishments in the territory of the European Union, regardless of whether or not the processing of personal data (in that case, the referencing of links to web pages containing personal data concerning the person availing himself or herself of that right) takes place in the European Union. [90]

[90] Article 4(1)(a) of Directive 95/46 and Article 3(1) of Regulation 2016/679.

As regards the scope of the right to de-referencing, the Court considered that the operator of a search engine is required to carry out the de-referencing not on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States. It noted in that regard that while a universal de-referencing would, in view of the characteristics of the internet and search engines, meet in full the EU legislature's objective of guaranteeing a high level of protection of personal data throughout the European Union, it is in no way apparent from EU law [91] that, for the purposes of achieving such an objective, the legislature chose to confer a scope on the right to de-referencing which goes beyond the territory of the Member States. In particular, while EU law establishes cooperation mechanisms between the supervisory authorities of the Member States so that they may come to a joint decision based on weighing the right to privacy and the protection of personal data, on the one hand, against the interest of the public in various Member States in having access to information, on the other, no provision is currently made for such mechanisms as regards the scope of a de-referencing outside the European Union.

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

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

[91] Article 12(b) and Article 14(a) of Directive 95/46 and Article 17(1) of Regulation 2016/679.

Judgment of 8 December 2022 (Grand Chamber), Google (De-referencing of allegedly inaccurate content) (C-460/20, EU:C:2022:962)

The applicants in the main proceedings, TU, who occupies leadership positions and holds shares in various companies, and RE, who was his cohabiting partner and, until May 2015, held general commercial power of representation in one of those companies, were the subject of three articles published on a website in 2015 by G-LLC, the operator of that website. Those articles, one of which was illustrated by four photographs of the applicants and suggested that they led a life of luxury, criticised the investment model of a number of their companies. It was possible to access those articles by entering into the search engine operated by Google LLC ('Google') the surnames and forenames of the applicants, both on their own and in conjunction with certain company names. The list of results provided a link to those articles and to photographs in the form of thumbnails.

The applicants in the main proceedings requested Google, as the controller of personal data processed by its search engine, first, to de-reference the links to the articles at issue from the list of search results, on the ground that they contained inaccurate claims and defamatory opinions, and second, to remove the thumbnails from the list of search results. Google refused to accede to that request.

Since they were unsuccessful at first instance and on appeal, the applicants in the main proceedings brought an appeal on a point of law before the Bundesgerichtshof (Federal Court of Justice, Germany), in the context of which the Bundesgerichtshof (Federal Court of Justice) made a request to the Court of Justice for a preliminary ruling on the interpretation of the GDPR and Directive 95/46. [92]

By its judgment, delivered by the Grand Chamber, the Court developed its case-law on the conditions which apply to requests for de-referencing addressed to the operator of a search engine based on rules regarding the protection of personal data. It examines, in particular, first, the extent of the obligations and responsibilities incumbent on the operator of a search engine in processing a request for de-referencing based on the alleged inaccuracy of the information in the referenced content and, second, the burden of proof imposed on the data subject as regards that inaccuracy. The Court also gave a ruling on the need, for the purposes of examining a request to remove photographs displayed in the form of thumbnails in the list of results of an image search, to take account of the original context of the publication of those photographs on the internet.

In the first place, the Court ruled that, in the context of striking a balance between, on the one hand, the right to respect for private life and the protection of personal data, and on the other hand, the right to freedom of expression and information, [93] for the purposes of examining a request for de-referencing made to the operator of a search

[92] Respectively, Article 17(3)(a) of the GDPR and Article 12(b) and Article 14(a) of Directive 95/46.
[93] Fundamental rights guaranteed by Articles 7, 8 and 11 of the Charter, respectively.

engine seeking the removal from the list of search results of a link to content containing allegedly inaccurate information, such de-referencing is not subject to the condition that the question of the accuracy of the referenced content has been resolved, at least provisionally, in an action brought by the person making that request against the content provider.

As a preliminary point, in order to examine the conditions in which the operator of a search engine is required to accede to a request for de-referencing and thus to remove from the list of results displayed following a search on the basis of the data subject's name, the link to an internet page on which allegations appear which that person regards as inaccurate, the Court stated, in particular, as follows:

• inasmuch as the activity of a search engine is liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of that search engine, as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the guarantees laid down by Directive 95/46 and the GDPR may have full effect and that effective and complete protection of data subjects may actually be achieved;

• where the operator of a search engine receives a request for de-referencing, it must ascertain whether the inclusion of the link to the internet page in question in the list of results is necessary for exercising the right to freedom of information of internet users potentially interested in accessing that internet page by means of such a search, a right protected by the right to freedom of expression and of information;

• the GDPR expressly lays down the requirement to strike a balance between the fundamental rights to privacy and protection of personal data, on the one hand, and the fundamental right of freedom of information on the other.

First of all, the Court found that while the data subject's rights to respect for private life and the protection of personal data override, as a general rule, the legitimate interest of internet users who may be interested in accessing the information in question, that balance may, however, depend on the relevant circumstances of each case, in particular on the nature of that information and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

The question of whether or not the referenced content is accurate also constitutes a relevant factor when making that assessment. Accordingly, in certain circumstances, the right of internet users to information and the content provider's freedom of expression may override the rights to private life and to protection of personal data, in particular where the data subject plays a role in public life. However, that relationship is reversed where, at the very least, a part – which is not minor in relation to the content as a whole – of the information referred to in the request for de-referencing proves to be inaccurate. In such a situation, the right to inform and the right to be informed cannot

be taken into account, since they cannot include the right to disseminate and have access to such information.

Next, as regards, first, the obligations relating to establishing whether or not the information found in the referenced content is accurate, the Court clarified that the person requesting the de-referencing on account of the inaccuracy of such information is required to establish the manifest inaccuracy of such information or, at the very least, of a part – which is not minor in relation to the content as a whole – of that information. However, in order to avoid imposing on that person an excessive burden which is liable to undermine the practical effect of the right to de-referencing, that person has to provide only evidence that, in the light of the circumstances of the particular case, can reasonably be required of him or her to try to find. In principle, that person cannot be required to produce, as from the pre-litigation stage, in support of his or her request for de-referencing, a judicial decision made against the publisher of the website, even in the form of a decision given in interim proceedings.

Second, as regards the obligations and responsibilities imposed on the operator of the search engine, the Court pointed out that the operator of a search engine must, in order to determine whether content may continue to be included in the list of search results carried out using its search engine following a request for de-referencing, take into account all the rights and interests involved and all the circumstances of the case. However, that operator cannot be obliged to investigate the facts and, to that end, to organise an adversarial debate with the content provider seeking to obtain missing information concerning the accuracy of the referenced content. An obligation to contribute to establishing whether or not the referenced content is accurate would impose on that operator a burden in excess of what can reasonably be expected of it in the light of its responsibilities, powers and capabilities. That solution would entail a serious risk that content meeting the public's legitimate and compelling need for information would be de-referenced and would thereby become difficult to find on the internet. There would, accordingly, be a real risk of a deterrent effect on the exercise of freedom of expression and of information if such an operator undertook such de-referencing quasi-systematically, in order to avoid having to bear the burden of investigating the relevant facts for the purpose of establishing whether or not the referenced content was accurate.

Therefore, where the person who has made a request for de-referencing submits evidence establishing the manifest inaccuracy of the information found in the referenced content or, at the very least, of a part – which is not minor in relation to the content as a whole – of that information, the operator of the search engine is required to accede to that request. The same applies where the person making that request submits a judicial decision made against the publisher of the website, which is based on the finding that information found in the referenced content – which is not minor in relation to that content as a whole – is, at least prima facie, inaccurate. By contrast, where the inaccuracy of such information is not obvious, in the light of the evidence

provided by the person making the request, the operator of the search engine is not required, where there is no such judicial decision, to accede to such a request for de-referencing. Where the information in question is likely to contribute to a debate of public interest, it is appropriate, in the light of all the circumstances of the case, to place particular importance on the right to freedom of expression and of information.

Lastly, the Court added that, where the operator of a search engine does not grant a request for de-referencing, the data subject must be able to bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders that controller to adopt the necessary measures. In that regard, the judicial authorities must ensure a balance is struck between competing interests, since they are best placed to carry out a complex and detailed balancing exercise, which takes account of all the criteria and all the factors established by the relevant case-law.

In the second place, the Court ruled that, within the context of weighing up fundamental rights mentioned above, for the purposes of examining a request for de-referencing seeking the removal from the results of an image search carried out on the basis of the name of a natural person of photographs displayed in the form of thumbnails representing that person, account must be taken of the informative value of those photographs regardless of the original context of their publication on the internet page from which they are taken. However, it is necessary to take into consideration any text element which accompanies directly the display of those photographs in the search results and which is capable of casting light on the informative value of those photographs.

In reaching that conclusion, the Court noted that image searches carried out by means of an internet search engine on the basis of a person's name are subject to the same principles as those which apply to internet page searches and the information contained in them. It states that displaying, following a search by name, photographs of the data subject in the form of thumbnails, is such as to constitute a particularly significant interference with the data subject's rights to private life and that person's personal data.

Consequently, when the operator of a search engine receives a request for de-referencing which seeks the removal, from the results of an image search carried out on the basis of the name of a person, of photographs displayed in the form of thumbnails representing that person, it must ascertain whether displaying the photographs in question is necessary for exercising the right to freedom of information of internet users who are potentially interested in accessing those photographs by means of such a search.

In so far as the search engine displays photographs of the data subject outside the context in which they are published on the referenced internet page, most often in order to illustrate the text elements contained in that page, it is necessary to establish whether that context must nevertheless be taken into consideration when striking a balance between the competing rights and interests. In that context, the question

whether that assessment must also include the content of the internet page containing the photograph displayed in the form of a thumbnail, the removal of which is sought, depends on the purpose and nature of the processing at issue.

As regards, first, the purpose of the processing at issue, the Court noted that the publication of photographs as a non-verbal means of communication is likely to have a stronger impact on internet users than text publications. Photographs are, as such, an important means of attracting internet users' attention and may encourage an interest in accessing the articles they illustrate. Since, in particular, photographs are often open to a number of interpretations, displaying them in the list of search results as thumbnails may result in a particularly serious interference with the data subject's right to protection of his or her image, which must be taken into account when weighing up competing rights and interests. A separate weighing up exercise is required depending on whether the case concerns, on the one hand, articles containing photographs which are published on an internet page and which, when placed into their original context, illustrate the information provided in those articles and the opinions expressed in them, or, on the other hand, photographs displayed in the list of results in the form of thumbnails by the operator of a search engine outside the context in which they were published on the original internet page.

In that regard, the Court recalled that not only does the ground justifying the publication of a piece of personal data on a website not necessarily coincide with that which is applicable to the activity of search engines, but also, even where that is the case, the outcome of the weighing up of the rights and interests at issue may differ according to whether the processing carried out by the operator of a search engine or that carried out by the publisher of that internet page is at issue. The legitimate interests justifying such processing may be different and, also, the consequences of the processing for the data subject, and in particular for his or her private life, are not necessarily the same.

As regards second, the nature of the processing carried out by the operator of the search engine, the Court observed that, by retrieving the photographs of natural persons published on the internet and displaying them separately, in the results of an image search, in the form of thumbnails, the operator of a search engine offers a service in which it carries out autonomous processing of personal data which is distinct both from that of the publisher of the internet page from which the photographs are taken and from that, for which the operator is also responsible, of referencing that page.

Therefore, an autonomous assessment of the activity of the operator of the search engine, which consists of displaying results of an image search, in the form of thumbnails, is necessary, as the additional interference with fundamental rights resulting from such activity may be particularly intense owing to the aggregation, in a search by name, of all information concerning the data subject which is found on the internet. In the context of that autonomous assessment, account must be taken of the fact that that display constitutes, in itself, the result sought by the internet user, regardless of his or her subsequent decision to access the original internet page or not.

The Court observed, however, that such a specific weighing up exercise, which takes account of the autonomous nature of the data processing performed by the operator of the search engine, is without prejudice to the possible relevance of text elements which may directly accompany the display of a photograph in the list of search results, since such elements are capable of casting light on the informative value of that photograph for the public and, consequently, of influencing the weighing up of the rights and interests involved.

4. Website users consent to the storage of information

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

In this judgment, the Court ruled that consent to the storage of information or access to information via cookies installed on the terminal device of a website user is not validly given when the authorisation results from a box being ticked by default, regardless of whether or not the information in question constitutes personal data. Furthermore, the Court made clear that the service provider must inform a website user of the duration of the operation of cookies and whether or not third parties may have access to those cookies.

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

The request for a preliminary ruling essentially concerned the interpretation of the concept of 'consent' referred to in Directive 2002/58, [94] read in conjunction with Directive 95/46/EC, [95] as well as with the GDPR. [96]

First, the Court observed that Article 2(h) of Directive 95/46/EC, to which Article 2(f) of Directive 2002/58 refers, defines 'consent' as being 'any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed'. It noted that the requirement of an 'indication' of the data subject's wishes clearly points to active, rather than passive, behaviour. However, consent given in the form of a pre-ticked check box does not imply

[94] Articles 2(f) and 5(3) of Directive 2002/58, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (OJ 2009 L 337, p. 11).
[95] Article 2(h) of Directive 95/46.
[96] Article 6(1)(a) of Regulation 2016/679.

active behaviour on the part of a website user. Furthermore, the legislative origins of Article 5(3) of Directive 2002/58, which provides – as amended by Directive 2009/136 – that the user must have 'given his or her consent' to the storage of cookies, seems to indicate that user consent may no longer be presumed but must be the result of active behaviour on the part of the user. Finally, active consent is now provided for in the GDPR, [97] Article 4(11) of which requires an indication of the data subject's wishes in the form of 'clear affirmative action' and recital 32 of which expressly precludes 'silence, pre-ticked boxes or inactivity' from constituting consent.

The Court therefore held that consent is not validly constituted if the storage of information, or access to information already stored in the website user's terminal equipment, is permitted by way of a pre-ticked check box which the user must deselect to refuse giving consent. It added that the fact that the user selects the button to participate in the lottery in question cannot be sufficient for it to be concluded that the user validly gave consent to the storage of cookies.

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

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

5. Processing personal data on online social networks

Judgment of 4 July 2023 (Grand Chamber), Meta Platforms and Others (General terms of use of a social network) (C-252/21, EU:C:2023:537)

Meta Platforms owns the online social network Facebook, which is free of charge for private users. The business model of that social network is based on financing through

[97] IDEM.

online advertising, which is tailored to its individual users. That advertising is made possible in technical terms by the automated production of detailed profiles in respect of the network users and the users of the online services offered at the level of the Meta group. In order to be able to use that social network, when they register, users must accept the general terms drawn up by Meta Platforms, which refer to the data and cookies policies set by that company. Under those policies, in addition to the data which those users provide directly when they register, Meta Platforms also collects data about user activities on and off the social network and links the data with the Facebook accounts of the users concerned. The latter data, also known as 'off-Facebook data', are data concerning visits to third-party web pages and apps as well as data concerning the use of other online services belonging to the Meta group (including Instagram and WhatsApp). The aggregate view of the data thus collected allows detailed conclusions to be drawn about those users' preferences and interests.

By decision of 6 February 2019, the Bundeskartellamt (Federal Cartel Office, Germany), prohibited Meta Platforms, first, from making, in the general terms in force at the time, the use of the social network Facebook by private users resident in Germany subject to the processing of their off-Facebook data and, second, from processing those data without their consent. In addition, the Federal Cartel Office required Meta Platforms to adapt those general terms in such a way that it is made clear that those data will neither be collected nor linked with Facebook user accounts nor used without the consent of the users concerned. Last, the office clarified that such a consent was not valid if it was a condition for using the social network. It based its decision on the fact that the processing of the data at issue, which it found to be inconsistent with the GDPR, constitutes an abuse of Meta Platforms' dominant position on the market for online social networks.

Meta Platforms brought an action against that decision before the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany). The Higher Regional Court, Düsseldorf, Germany referred a number of questions to the Court for a preliminary ruling, including those concerning the interpretation and application of certain provisions of the GDPR.

In its judgment, the Grand Chamber of the European Court of Justice clarified whether a social network operator may process the 'sensitive' personal data of its users, the conditions under which data processing by such an operator is lawful, and the validity of consent given for the purposes of such processing by those users to an undertaking holding a dominant position on the national market for online social networks.

In the second place, with regard to the processing of special categories of personal data, [98] the Court found that, where the user of an online social network visits websites or apps to which one or more of those categories relate and, as the case may be, enters information into them when registering or when placing online orders, the processing of personal data by the operator of that online social network [99] must be regarded as 'processing of special categories of personal data' within the meaning of Article 9(1) of the GDPR, where it allows information falling within one of those special categories to be revealed, irrespective of whether that information concerns a user of that network or any other natural person. Such data processing is in principle prohibited, subject to certain derogations. [100]

In the latter regard, the Court stated that, where the user of an online social network visits websites or apps to which one or more of those special categories relate, the user does not manifestly make public [101] the data relating to those visits collected by the operator of that online social network via cookies or similar storage technologies. Moreover, where he or she enters information into such websites or apps or where he or she clicks or taps on buttons integrated into those sites and apps, such as the 'Like' or 'Share' buttons or buttons enabling the user to identify himself or herself on those sites or apps using login credentials linked to his or her social network user account, his or her telephone number or email address, that user manifestly makes public the data thus entered or resulting from the clicking or tapping on those buttons only in the circumstance where he or she has explicitly made the choice beforehand, as the case may be on the basis of individual settings selected with full knowledge of the facts, to make the data relating to him or her publicly accessible to an unlimited number of persons.

As regards more generally the conditions for the lawful processing of personal data, the Court recalled that, under the GDPR, data processing is lawful if and to the extent that the data subject has given consent for one or more specific purposes. [102] In the absence of such a consent, or where that consent was not freely given, specific, informed and unambiguous, such processing is nevertheless justified if it meets one of the requirements of necessity, [103] which must be interpreted strictly. The processing of the

---

98 Referred to in Article 9(1) of the GDPR. Under this provision, 'processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited'. '

99 That processing entails the collection – by means of integrated interfaces, cookies or similar storage technologies – of data from visits to those sites and apps and of the information entered by the user, the linking of all those data with the user's social network account and the use of those data by that operator.

100 Provided for in Article 9(2) of the GDPR. That provision reads: 'Paragraph 1 shall not apply if one of the following applies:

a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; [...]

e) processing relates to personal data which are manifestly made public by the data subject;

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; [...]'.

101 Within the meaning of Article 9(2)(e) of the GDPR.

102 Within the meaning of point (a) of the first subparagraph of Article 6(1) of the GDPR.

103 Referred to in points (b) to (f) of the first subparagraph of Article 6(1) of the GDPR. Under those provisions, processing is lawful only if and to the extent that it is, inter alia, necessary for the performance of a contract to which the data subject is party (point (b) of the first

personal data of its users by the operator of an online social network can be regarded as necessary for the performance of a contract to which those users are party only on condition that the processing is objectively indispensable for a purpose that is integral to the contractual obligation intended for those users, such that the main subject matter of the contract cannot be achieved if that processing does not occur.

In addition, according to the Court, the data processing at issue can be regarded as necessary for the purposes of the legitimate interests pursued by the controller or by a third party only on condition that the operator has informed the users from whom the data have been collected of a legitimate interest that is pursued by the data processing, that such processing is carried out only in so far as is strictly necessary for the purposes of that legitimate interest and that it is apparent from a balancing of the opposing interests, having regard to all the relevant circumstances, that the interests or fundamental freedoms and rights of those users do not override that legitimate interest of the controller or of a third party. The Court found, inter alia, that in the absence of consent on their part, the interests and fundamental rights of those users override the interest of the operator of an online social network in personalised advertising through which it finances its activity.

Last, the Court specified that the processing of personal data at issue is justified where it is actually necessary for compliance with a legal obligation to which the controller is subject, pursuant to a provision of EU law or the law of the Member State concerned, where that legal basis meets an objective of public interest and is proportionate to the legitimate aim pursued and where that processing is carried out only in so far as is strictly necessary.

As regards the validity of the consent of the users concerned to the processing of their data under the GDPR, the Court held that the fact that the operator of an online social network holds a dominant position on the market for online social networks does not, as such, preclude the users of such a network from being able validly to consent to the processing of their personal data by that operator. However, since that position is liable to affect the freedom of choice of those users and to create a clear imbalance between them and the controller, it is an important factor in determining whether the consent was in fact validly and, in particular, freely given, which it is for that operator to prove. [104]

In particular, the users of the social network in question must be free to refuse individually, in the context of the contractual process, to give their consent to particular data processing operations not necessary for the performance of the contract, without being obliged to refrain entirely from using that online social network, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent

subparagraph of Article 6(1) of the GDPR), for compliance with a legal obligation to which the controller is subject (point (c) of the first subparagraph of Article 6(1) of the GDPR) or for the purposes of the legitimate interests pursued by the controller or by a third party (point (f) of the first subparagraph of Article 6(1) of the GDPR).

[104] Pursuant to Article 7(1) of the GDPR.

alternative not accompanied by such data processing operations. Moreover, it must be possible to give separate consent for the processing of off-Facebook data.

VI. National supervisory authorities

1. Scope of the independence requirement

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

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

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

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

The Court found that these supervisory authorities responsible for supervising the processing of personal data outside the public sector must enjoy an independence allowing them to perform their duties free from external influence. That independence precludes not only any influence exercised by the supervised bodies, but also any

directions or any other external influence, whether direct or indirect, which could call 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.

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

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

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

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

The Court stated that, in order to be able to satisfy the criterion of independence set out in the aforementioned provision of Directive 95/46, a national supervisory authority need not be given a separate budget, such as that provided for in Article 43(3) in Regulation No 45/2001. Member States are not obliged to reproduce in their national legislation provisions similar to those of Chapter V of Regulation No 45/2001 in order to ensure the total independence of their respective supervisory authorities, and they can therefore provide that, from the point of view of budgetary law, the supervisory authorities are to come under a specified ministerial department. However, the attribution of the necessary equipment and staff to such authorities must not prevent them from acting 'with complete independence' in exercising the functions entrusted to them within the meaning of the second subparagraph of Article 28(1) of Directive 95/46.

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

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

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.

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

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

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

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.

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

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

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. 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 the 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, relying, where necessary, on the information which the authority of the first Member State has transmitted to the authority of that other Member State.

3. Powers of the national supervisory authorities

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

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

The Court found, first of all, that national supervisory authorities have a wide range of powers and that those powers, listed on a non-exhaustive basis in Article 28(3) of Directive 95/46, constitute necessary means 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.

As regards the power to control transfers of personal data to third countries, the Court ruled that it is, admittedly, apparent from Article 28(1) and (6) of Directive 95/46 that the powers of the national supervisory authorities concern processing of personal data carried out on the territory of their own Member State, 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.

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

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

In this judgment (see also section II.5., entitled 'Concept of "personal data controller"'), which concerned, among other things, the interpretation of Articles 4 and 28 of Directive

95/46, the Court ruled on the scope of the supervisory authorities' powers of intervention with regard to the processing of personal data involving several parties.

Thus, the Court held that where an undertaking established outside the European Union (such as the US company Facebook) has several establishments in different Member States, the supervisory authority of a Member State is entitled to exercise the powers conferred on it by Article 28(3) of that directive in respect of an establishment of that undertaking situated within the territory of that Member State (in this case Facebook Germany), even though, by virtue of the division of tasks within the group, on the one hand, that establishment is responsible solely for the sale of advertising space and other marketing activities on the territory of that Member State and, on the other, exclusive responsibility for the collection and processing of personal data lies, for the whole of the territory of the European Union, with an establishment situated in another Member State (in the present case, Facebook Ireland).

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

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

On 11 September 2015, the President of the Belgian Privacy Commission ('the Privacy Commission') brought an action before the Nederlandstalige rechtbank van eerste aanleg Brussel (Dutch-language Court of First Instance, Brussels, Belgium), seeking an injunction against Facebook Ireland, Facebook Inc. and Facebook Belgium, aiming to put an end to alleged infringements of data protection laws by Facebook. Those infringements consisted, inter alia, of the collection and use of information on the browsing behaviour of Belgian internet users, whether or not they were Facebook account holders, by means of various technologies, such as cookies, social plug-ins [105] or pixels.

On 16 February 2018, that court held that it had jurisdiction to give a ruling on that action and, on the substance, held that the Facebook social network had not adequately

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

informed Belgian internet users of the collection and use of the information concerned. Further, the consent given by the internet users to the collection and processing of that data was held to be invalid.

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

The referring court was uncertain as to the effect of the application of the 'one-stop shop' mechanism provided for by the GDPR [106] on the competences of the DPA and, in particular, as to whether, with respect to the facts subsequent to the date of entry into force of the GDPR, namely 25 May 2018, the DPA could bring an action against Facebook Belgium, since it was Facebook Ireland which had been identified as the controller of the data concerned. Since that date, and in particular under the 'one-stop shop' rule laid down by the GDPR, only the Data Protection Commissioner (Ireland) is competent to bring injunction proceedings, subject to review by the Irish courts.

In its Grand Chamber judgment, the Court specified the powers of national supervisory authorities within the scheme of the GDPR. Thus, it considered, inter alia, that that regulation authorises, under certain conditions, a supervisory authority of a Member State to exercise its power to bring any alleged infringement of the GDPR before a court of that State and to initiate or engage in legal proceedings in relation to an instance of cross-border data processing, [107] although that authority is not the lead supervisory authority with regard to that processing.

In the first place, the Court specified the conditions governing whether a national supervisory authority, which does not have the status of lead supervisory authority in relation to an instance of cross-border processing, must exercise its power to bring any alleged infringement of the GDPR before a court of a Member State and, where necessary, to initiate or engage in legal proceedings in order to ensure the application of that regulation. Thus, the GDPR must confer on that supervisory authority a competence to adopt a decision finding that that processing infringes the rules laid down by that regulation and, in addition, that power must be exercised with due regard to the cooperation and consistency procedures provided for by that regulation. [108]

---

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

[107] Within the meaning of Article 4(23) of the GDPR.

[108] Laid down in Articles 56 and 60 of the GDPR.

With respect to cross-border processing, the GDPR provides for the 'one-stop shop' mechanism, [109] which is based on an allocation of competences between one 'lead supervisory authority' and the other national supervisory authorities concerned. That mechanism requires close, sincere and effective cooperation between those authorities in order to ensure consistent and homogeneous protection of the rules for the protection of personal data, and thus preserve its effectiveness. As a general rule, the GDPR guarantees in that regard the competence of the lead supervisory authority for the adoption of a decision finding that an instance of cross-border processing is an infringement of the rules laid down by that regulation, [110] whereas the competence of the other supervisory authorities concerned for the adoption of such a decision, even provisionally, constitutes the exception to the rule. [111] However, in the exercise of its competences, the lead supervisory authority cannot eschew essential dialogue and sincere and effective cooperation with the other supervisory authorities concerned. Accordingly, in the context of that cooperation, the lead supervisory authority may not ignore the views of the other supervisory authorities concerned, and any relevant and reasoned objection made by one of the other supervisory authorities has the effect of blocking, at least temporarily, the adoption of the draft decision of the lead supervisory authority.

The Court also added that the fact that a supervisory authority of a Member State which is not the lead supervisory authority with respect to an instance of cross-border data processing may exercise the power to bring any alleged infringement of the GDPR before a court of that State and to initiate or engage in legal proceedings only when that exercise complies with the rules on the allocation of competences to adopt decisions between the lead supervisory authority and the other supervisory authorities [112] is compatible with Articles 7, 8 and 47 of the Charter, which guarantee data subjects the right to the protection of their personal data and the right to an effective remedy, respectively.

In the second place, the Court held that, in the case of cross-border data processing, it is not a prerequisite for the exercise of the power of a supervisory authority of a Member State, other than the lead supervisory authority, to initiate or engage in legal proceedings [113] that the controller or the processor with respect to the cross-border processing of personal data to which that action relates has a main establishment or another establishment on the territory of that Member State. However, the exercise of that power must fall within the territorial scope of the GDPR, [114] which presupposes that

[109] Article 56(1) of the GDPR.
[110] Article 60(7) of the GDPR.
[111] Article 56(2) and Article 66 of the GDPR set out exceptions to the general rule that it is the lead supervisory authority that is competent to adopt such decisions.
[112] Provided for in Articles 55 and 56, read in conjunction with Article 60 of the GDPR.
[113] Pursuant to Article 58(5) of the GDPR.
[114] Article 3(1) of the GDPR provides that that regulation is applicable to the processing of personal data 'in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not'.

the controller or the processor with respect to the cross-border processing has an establishment in the European Union.

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

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

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

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

Judgment of 16 January 2024 (Grand Chamber), Österreichische Datenschutzbehörde (C-33/22, EU:C:2024:46)

In this case (see also section II.1., entitled 'Scope of the general rules'), the Court noted that the provisions of the GDPR relating to the competence of national supervisory authorities and the right of objection [115] do not require the adoption of national implementing measures and are sufficiently clear, precise and unconditional to produce a direct effect. It follows that, while the GDPR leaves a margin of discretion to the Member States as regards the number of supervisory authorities to be established, [116] it determines, by contrast, the extent of their competences to monitor the application of the GDPR. Thus, where a Member State decides to establish a single national supervisory authority, that authority necessarily has all the competences provided for by that regulation. Any other interpretation would undermine the effectiveness of those provisions and risk weakening the effectiveness of all the other provisions of the GDPR that may be the subject of a complaint.

As regards the fact that national constitutional provisions preclude the possibility for a supervisory authority which is part of the executive branch to monitor the application of the GDPR by a body which is part of the legislature, the Court pointed out that it is precisely with due regard for the constitutional structure of the Member States that the GDPR merely requires Member States to establish at least one supervisory authority, while offering them the possibility of establishing more than one. That regulation thus grants each Member State a margin of discretion enabling it to establish as many supervisory authorities as may be required, in particular, in the light of its constitutional structure.

Furthermore, a Member State's reliance on rules of national law cannot be allowed to undermine the unity and effectiveness of EU law. The effects of the principle of the primacy of EU law are binding on all the bodies of a Member State, without, in particular, provisions of domestic law, including constitutional provisions, being able to prevent that.

Thus, where a Member State has chosen to establish a single supervisory authority, it cannot rely on provisions of national law, be they constitutional in nature, in order to exclude the processing of personal data coming within the scope of the GDPR from the supervision of that authority.

---

115 Respectively, Article 55(1) and Article 77(1) of the GDPR.

116 In accordance with Article 51(1) of the GDPR.

4. Conditions for imposing administrative fines

Judgment of 5 December 2023 (Grand Chamber), Nacionalinis visuomenės sveikatos centras (C-683/21, EU:C:2023:949)

In this case (see also sections II.3., II.5. and II.6., entitled 'Concept of "processing of personal data"', 'Concept of "personal data controller"' and 'Concept of "joint controller"'), the Court found that, under Article 83 of the GDPR, an administrative fine may be imposed on a controller only if an intentional or negligent character of an infringement has been found. [117]

In that regard, the Court clarified that the EU legislature did not leave the Member States a margin of discretion as regards the substantive conditions which must be satisfied by a supervisory authority where that authority decides to impose an administrative fine on a controller under that provision. The fact that the GDPR gives Member States the option of providing for exceptions in relation to public authorities and public bodies established on their territory, [118] as well as requirements regarding the procedure to be followed by supervisory authorities in imposing an administrative fine, [119] in no way means that they would also be empowered to provide for such substantive conditions.

With regard to those conditions, the Court noted that the factors listed in the GDPR, in the light of which the supervisory authority may impose an administrative fine on the controller, include 'the intentional or negligent character of the infringement'. [120] By contrast, none of those factors mention any possibility that the controller will incur liability in the absence of wrongful conduct on its part. Accordingly, only infringements of the provisions of the GDPR committed by the controller intentionally or negligently can result in a fine being imposed on the controller pursuant to Article 83 of that regulation.

The Court added that such interpretation is supported by the general scheme and purpose of the GDPR. In that context, it states that the existence of a system of penalties under the GDPR making it possible to impose, where justified by the specific circumstances of each individual case, an administrative fine creates an incentive for controllers and processors to comply with that regulation and that, through their deterrent effect, administrative fines contribute to strengthening the protection of data subjects. However, the EU legislature did not consider it necessary to provide for administrative fines to be imposed in the absence of wrongdoing. In view of the fact that the GDPR aims for a level of protection which is both equivalent and homogeneous, and

[117] Infringement referred to in Article 83(4) to (6).
[118] By virtue of Article 83(7) of the GDPR, which provides that '... each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State'.
[119] By virtue of Article 83(8) of the GDPR, read in the light of recital 129 thereof.
[120] Article 83(2)(b) of the GDPR.

that it must, to that end, be applied consistently throughout the European Union, it would be contrary to that purpose to allow Member States to provide such a system for the imposition of a fine.

In addition, the Court concluded that such a fine may be imposed on a controller in respect of personal data processing operations performed by a processor on behalf of that controller, unless, in the context of those operations, that processor has carried out processing for its own purposes or has processed such data in a manner incompatible with the framework of, or detailed arrangements for, the processing as determined by the controller, or in such a manner that it cannot reasonably be considered that that controller consented to such processing. In such a situation, the processor must be considered to be a controller in respect of such processing.

Judgment of 5 December 2023 (Grand Chamber), Deutsche Wohnen (C-807/21, EU:C:2023:950)

Deutsche Wohnen SE ('DW') is a real estate company which holds, indirectly via participating interests in various companies, a large number of commercial and housing units. As part of its business activities, it processes personal data of tenants of those units.

Following two inspections carried out in 2017 and in 2019, le Berliner Beauftragte für den Datenschutz (Berlin Data Protection Authority, Germany) found that DW had committed a series of infringements of the GDPR. By decision of 30 October 2019, that supervisory authority imposed administrative fines in respect of such infringements.

DW brought an action against that decision before the Landgericht Berlin (Regional Court, Berlin, Germany), which closed the proceedings without taking further action. That court observed that, under German law, [121] a finding of an administrative infringement can be made only against a natural person and not against a legal person. In addition, in a situation involving a legal person incurring liability, only the actions of representatives of the legal person or of members of bodies thereof can be attributed to that legal person. The Staatsanwaltschaft Berlin (Berlin Public Prosecutor's Office) brought an appeal against that decision before the Kammergericht Berlin (Higher Regional Court, Berlin, Germany). In that context, that court made a reference to the Court of Justice for a preliminary ruling on the interpretation of the GDPR.

In its judgment, the Grand Chamber of the Court ruled on the conditions for imposing administrative fines under the GDPR. In the first place, it examines the question whether the Member States may make the imposition of an administrative fine on a legal person subject to the condition that the infringement of that regulation must first be attributed to an identified natural person. Secondly, it also considers, as in the Nacionalinis

[121] Gesetz über Ordnungswidrigkeiten (Law on Administrative Offences), of 24 May 1968 (BGBl. 1968 I, p. 481), in the version of the communication of 19 February 1987 (BGBl. 1987 I, p. 602), as adapted by the law of 19 June 2020 (BGBl. 2020 I, p. 1350).

visuomenės sveikatos centras judgment (see above), whether a breach penalised by the GDPR provisions must be committed deliberately or through negligence.

As regards the imposition of an administrative fine under the GDPR on a legal person, the Court stated, first of all, that the principles, prohibitions and obligations laid down by the GDPR are directed, in particular, at 'controllers', whose responsibility extends to any processing of personal data which they carry out themselves or which is carried out on their behalf. It is that liability which forms, in the event of infringement of the provisions of the GDPR, the basis for the imposition of an administrative fine on the controller pursuant to Article 83 of that regulation. However, the EU legislature did not distinguish, for the purposes of determining such liability, between natural persons and legal persons, that liability being subject to the sole condition that those persons, alone or jointly with others, determine the purposes and means of processing of personal data. [122] Consequently, as a rule, any person meeting that condition is responsible, inter alia, for any infringement of the GDPR which is committed by that person or on behalf of that person. That implies, first, that legal persons are liable not only for infringements committed by their representatives, directors or managers, but also by any other person acting in the course of the business of those legal persons and on their behalf. Second, the administrative fines provided for by the GDPR in respect of such infringements must be capable of being imposed directly on legal persons where they may be classified as controllers.

Next, the Court observed that no provision of the GDPR permits the inference that the imposition of an administrative fine on a legal person as a controller is subject to a previous finding that that infringement was committed by an identified natural person. In addition, the EU legislature did not provide the Member States with a margin of discretion in that regard. The fact that the GDPR provides them with the possibility to lay down requirements concerning the procedure to be followed by the supervisory authorities in order to impose an administrative fine [123] in no way means that they are also authorised to lay down substantive conditions over and above those set by the GDPR.

In that context, the Court clarified that to allow Member States to make it a requirement, unilaterally and as a necessary condition for the imposition of an administrative fine pursuant to Article 83 of the GDPR on a controller who is a legal person, that the infringement in question is first attributed or attributable to an identified natural person, would be contrary to the purpose of the GDPR. In addition, such an additional requirement would, ultimately, risk weakening the effectiveness and deterrent effect of administrative fines imposed on legal persons as controllers.

---

[122] According to Article 4(7) of the GDPR.

[123] As is apparent from Article 58(4) and Article 83(8) of the GDPR, read in the light of recital 129 thereof.

Lastly, the Court pointed out that the concept of an 'undertaking', within the meaning of Articles 101 and 102 TFEU, [124] has no bearing on whether and under what conditions an administrative fine may be imposed pursuant to the GDPR on a controller who is a legal person and is relevant only for the purpose of determining the amount of such a fine.

Accordingly, the Court concluded that the GDPR [125] precludes national legislation under which an administrative fine may be imposed on a legal person in its capacity as controller in respect of an infringement of that regulation [126] only in so far as that infringement has previously been attributed to an identified natural person.

As regards the question whether the Member States may provide for an administrative fine to be imposed even where the infringement in respect of which a penalty has been imposed has not been committed intentionally or negligently, the Court recalled, first of all, that the substantive conditions which a supervisory authority must satisfy when it imposes such a fine on a controller are governed solely by EU law and that the Member States have no discretion in that regard. Following the same reasoning as in Nacionalinis visuomenės sveikatos centras, the Court found that, under Article 83 of the GDPR, an administrative fine may be imposed only where it is established that the controller, which is both a legal person and an undertaking, intentionally or negligently, committed an infringement of the rules contained in that regulation.

5. Relationship between the powers of national supervisory authorities and those of other national authorities

Judgment of 4 July 2023 (Grand Chamber), Meta Platforms and Others (General terms of use of a social network) (C-252/21, EU:C:2023:537)

In this case (see also section V.5., entitled 'Processing of personal data on online social networks'), in ruling on the power of a competition authority to find that processing of personal data is not compliant with the GDPR, the Court noted that, subject to compliance with its duty of loyal cooperation [127] with data protection supervisory authorities, such an authority may find, in the context of an examination of an abuse of a dominant position on the part of an undertaking, [128] that the general conditions of use laid down by that undertaking with regard to the processing of personal data and their implementation do not comply with that regulation, where that finding is necessary to establish the existence of such an abuse. Nevertheless, where a competition authority

[124] To which reference is made in recital 150 of the GDPR.
[125] Article 58(2)(i) and Article 83(1) to (6) of the GDPR.
[126] Referred to in Article 83(4) to (6) of the GDPR.
[127] Enshrined in Article 4(3) TEU.
[128] Within the meaning of Article 102 TFEU.

identifies an infringement of the GDPR in the context of the finding of an abuse of a dominant position, it does not replace the supervisory authorities.

Thus, in the light of the principle of loyal cooperation, when competition authorities are called upon, in the exercise of their powers, to examine whether an undertaking's conduct is consistent with the provisions of the GDPR, they are required to consult and cooperate earnestly with the national supervisory authorities concerned or with the lead supervisory authority. All of these authorities are then bound to observe their respective powers and competences, in such a way as to ensure that the obligations arising from the GDPR and the objectives of that regulation are complied with and that their effectiveness is safeguarded. It follows that, where, in the context of the examination seeking to establish whether there is an abuse of a dominant position by an undertaking, a competition authority takes the view that it is necessary to examine whether that undertaking's conduct is consistent with the provisions of the GDPR, that authority must ascertain whether that conduct or similar conduct has already been the subject of a decision by the competent national supervisory authority or the lead supervisory authority or the Court. If that is the case, the competition authority cannot depart from it, although it remains free to draw its own conclusions from the point of view of the application of competition law.

Where it has doubts as to the scope of the assessment carried out by the competent national supervisory authority or the lead supervisory authority, where the conduct in question or similar conduct is, simultaneously, under examination by those authorities, or where, in the absence of investigation by those authorities, it takes the view that an undertaking's conduct is not consistent with the provisions of the GDPR, the competition authority must consult these authorities and seek their cooperation in order to dispel its doubts or to determine whether it must wait for the supervisory authority concerned to take a decision before starting its own assessment. In the absence of any objection from them or of a reply within a reasonable time, the competition authority may continue its own investigation.

COURT OF JUSTICE
OF THE EUROPEAN UNION

Research and Documentation Department

July 2024