Handbook on the Techniques of Judicial Interactions in the Application of the EU Charter

DATA PROTECTION

IN THE FRAMEWORK OF THE PROJECT 'E-LEARNING NATIONAL ACTIVE CHARTER TRAINING (E-NACT)'

FUNDED BY THE EUROPEAN COMMISSION FUNDAMENTAL RIGHTS & CITIZENSHIP PROGRAMME

Researcher responsible for the Handbook:
Dr Mariavittoria Catanzariti

NATIONAL EXPERTS AND COLLABORATORS

The e-NACT team would like to thank the following experts and collaborators who contributed to the selection of the national and European case law upon which this Handbook is built.

Federica Casarosa
Madalina Moraru
Karolina Podstawa
Joan Soares Mullor
Sara Azevedo
Afonso Brás
Sergiu Popovici
Rita de Brito Gião Hanek
Diana Lavinia Botău
Francesco Perrone
Florentino Gregorio Ruiz Yamuza

Contents

Acknowledgements
I would like to thank the Project partners and the members of the e-NACT Working Group on Data Protection for sharing their practices and experience with the application of the Charter, as well as for their suggestions on how to improve the e-NACT Handbook so as to make it more useful for them.

Part I - Data protection and privacy as EU fundamental rights

Setting the scene

Data protection in Europe was developed in the 1970s with the adoption of legislation to control the data processing carried out by public authorities, while the right to privacy has an even older tradition in Europe. The earliest mention of the right to privacy is in an article written in 1890 by Warren and Brandeis. These scholars catalogued the harms of privacy invasion into four types: intrusion into one's private life and affairs; public disclosure of embarrassing private facts; unwanted publicity for private individuals; and misappropriation of a name or likeness for financial advantage. Nonetheless, while the US Constitution does not explicitly mention privacy or data protection, protection of both rights is explicitly established at the constitutional level in Europe: in addition to national constitutions, both the European Convention of Human Rights (hereinafter 'ECHR') and the Charter of Fundamental Rights (hereinafter 'CFR') provide for the protection of the right to privacy and data protection[1].

The right to a private and family life had already been recognised as a general principle of EU law prior to the coming into force of the Charter, for example in the case of *National Panasonic* (case C-136/79, ECLI:EU:C:1980:169). The right to the respect for family life and the home is also a general principle of EU law (see *Commission* v *Germany* (case C 249/86, ECLI:EU:C:1989:204) and *Kusionova* (Case C-34/13, ECLI:EU:C:2014:2189).

National courts will be required to interpret retained EU law consistently with the general principle reflected in Article 8 ECHR, so far as this is possible.

The right to data protection reflects the right to respect for private life in Article 8 of the ECHR[2]. Although Article 8 of the ECHR is distinct from Article 8 of the Charter, which has no direct equivalent in the ECHR, Article 8 of the ECHR has been held to encompass personal data protection (see for example *Z* v *Finland*, Judgment 25/02/1997) and the explanation to the Charter confirms that Article 8 of the Charter is based on Article 8 ECHR[3].

Nonetheless, data protection and privacy are different rights although they are closely related. The right to respect for private life consists of a general prohibition on interference whereas the protection of personal data comes into play whenever personal data are processed; it is thus broader than the right to respect for private life. Any processing operation of personal data is subject to appropriate protection. Data protection concerns all kinds of personal data and data processing, irrespective of the relationship and impact on privacy[4].

One of the leading cases for the recognition of data protection as a fundamental right was the judgment of the German Federal Court ('Bundesverfassungsgericht') in 1983, in which the right to data protection was recognised as the right to informational self-determination. In that judgment the Court held that '*the protection of personal data is essential for the free and self-determined development of the individual. At the same time, the self-determined development of the individual is*

[1] J. Kokott and C. Sobotta, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, International Data Privacy Law, 2013, Vol. 3, No 4, at 222.
[2] *Relu Adrian Coman and Others* v *Inspectoratul General pentru Imigări and Ministerul Afacerilor Interne (Case C-673/16)* (ECLI:EU:C:2018:385, par. 49).
[3] Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachmentdata/file/664891/05122017CharterAnalysisFINALVERSION.pdf
[4] Fundamental Rights Agency, *Handbook on European Data Protection law*, Publications Office of the European Union, 2018, at 19-20.

a precondition for a free and democratic communication order. If citizens cannot oversee and control which or even what kind of information about them is openly accessible in their social environment, and if they cannot even appraise the knowledge of possible communication partners, they may be inhibited in making use of their freedom. If citizens are unsure whether dissenting behaviour is noticed and information is being permanently stored, used and passed on, they will try to avoid dissenting behaviour so as not to attract attention. They may even abstain from making use of their basic and human rights. In a potentially all-knowing state, freedom of speech and freedom of choice are virtually impossible.'[5]

International legal instruments - except for the Council of Europe Convention 108 - do not expressely recognise data protection as a human right, but only privacy as such. For example, Article 12 of the Universal Declaration of Human Rights (UDHR) provides that 'No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks', while article 17 of the International Covenant of Civil and Political Rights reads as follows: '1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.'

The Council of Europe Convention 108, which was opened to signature in 1981, is the only international treaty of legally-binding character that deals expressly with data protection.
This Convention is the first binding international instrument which protects the individual against abuses which may accompany the collection and processing of personal data and which seeks to regulate at the same time the cross-border flow of personal data.

In addition to providing guarantees in relation to the collection and processing of personal data, it outlaws the processing of 'sensitive' data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected.

Restrictions on the rights laid down in the Convention are only possible when overriding interests (e.g. state security, defence, etc.) are at stake.

The Convention also imposes some restrictions on transborder flows of personal data to states where the legal regulations do not provide equivalent protection[6].

The frequency with which the CJEU is ruling on the interpretation of the rights to privacy and data protection in EU law is constantly accelerating. The CJEU recognised that the right to the protection of personal information was a general principle of EU law as early as 1969, in the *Stauder* case (Case C- 29/69, ECLI:EU:C:1969:57).

In the pre-Charter era, the protection of personal data was held to form part of the right to privacy in line with how the European Court of Human Rights in Strasbourg has interpreted Article 8 ECHR to date. In the judgment *Rotaru* v *Romania* (Judgment 4 May 2000) the ECtHR extended the scope of private life to all kinds of information about individuals – even public information – that is collected and stored by authorities.

[5] This was the so-called 'Population census case', by which the Bundesverfassungsgericht decided that the Population Census Act was partly unconstitutional and thus it was annulled.
[6] Available at https://www.coe.int/it/web/conventions/full-list/-/conventions/treaty/108?coeconventionsWARcoeconventionsportletlanguageId=enGB.

With the Charter, data protection was introduced as a new and distinct fundamental right - the right to the protection of personal data (Article 8 CFR) - which was derived from EU law and the Council of Europe's legal system.

In parallel to the 'external' scrutiny mechanism foreseen by EC accession to the ECHR in order to ensure the conformity of legislation and policies with fundamental rights, an 'internal' scrutiny mechanism was necessary at EC level to allow for a preliminary and autonomous judicial check by the CJEU. To do so, the existence of a bill of rights specific to the EU was necessary, and at the 1999 European Council in Cologne it was decided to convoke a Convention to draft a Charter of Fundamental Rights.
The Charter was solemnly proclaimed by Parliament, the Council and the Commission in Nice in 2000. After being amended, it was proclaimed again in 2007. However, only with the adoption of the Treaty of Lisbon on 1 December 2009 did the Charter come into direct effect, as provided by Article 6(1) TEU, thereby becoming a binding source of primary law.
The Charter, although based on the ECHR and other European and international instruments, was innovative in various ways, since it notably includes, among other issues, disability, age and sexual orientation as prohibited grounds of discrimination, as well as enshrining access to documents, data protection and good administration among the fundamental rights it affirms.
While the scope of application of the Charter is on the one hand potentially very broad, as most of the rights it recognises are granted to 'everyone', regardless of nationality or status, on the other hand Article 51 limits its application to the EU institutions and bodies and, when they act to implement EU law, to the Member States. This provision serves to draw the boundary between the scope of the Charter and that of national constitutions and the ECHR[7].

From 2000 to 2009, the Charter had not been legally binding until Article 6(1) of the Treaty on European Union (Treaty of Lisbon) incorporated the Charter into EU primary law. The entry into force of the CFR was the second most relevant development in EU law, which is now fully grounded in its own fundamental rights system. The Charter provisions are addressed to the EU institutions and to the Member States when they implement EU law (Article 51(1) CFR)[8].

The legal bases of data protection under EU law are Article 8 CFR and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU), which guarantees everyone's right to the protection of their personal data[9]. Article 8 is based on Article 286 of the Treaty establishing the European Community (now replaced by Article 16 TFEU and Article 39 TEU) and Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of the personal data on the free movement of such data as well as on Article 8 of the ECHR and on the Council of Europe Convention 108, which has been ratified by all Member States. Reference is also made to Regulation (EC) No 45/2001 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.[10]

[7] Available at http://www.europarl.europa.eu/factsheets/en/sheet/146/the-protection-of-fundamental-rights-in-the-eu.
[8] Kristina Irion, *A Special Regard: The Court of Justice and the fundamental rights to privacy and data protection*, Gesellschaftliche Bewegungen - Recht unter Beobachtung und in Aktion. Festschrift für Wolfhard Kohte, Nomos, 2016, 871-887.
[9] Legal Basis, European Research Council, available at https://erc.europa.eu/sites/default/files/document/file/data-protectionpolicylegalbasis.pdf.
[10] Official Journal of the European Union C 303/17 - 14.12.2007, available at https://fra.europa.eu/en/charterpedia/article/8-protection-personal-data.

Article 8

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

The rights guaranteed in Article 7 correspond to those guaranteed by Article 8 of the ECHR. To take account of developments in technology the word 'correspondence' has been replaced by 'communications'.
In accordance with Article 52(3), the meaning and scope of this right are the same as those of the corresponding article of the ECHR. Consequently, the limitations which may legitimately be imposed on this right are the same as those allowed by Article 8 of the ECHR:

Article 7

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[11]

From Directive 95/46/EC to the GDPR

EU data protection has until recently been regulated by various legislative instruments. These include former first-pillar instruments such as Directive 95/46/EC on data protection (replaced by the General Data Protection Regulation in May 2018), Directive 2002/58/EC on e-privacy (modified in 2009; new proposal currently under consideration), Directive 2006/24/EC on data retention (declared invalid by the Court of Justice of the European Union on 8 April 2014 in the case *Digital Rights Ireland* Joined Cases C-293/12 and C-594/12 (ECLI: ECLI:EU:C:2014:238) and Regulation (EC) No 45/2001 on the processing of personal data by Community institutions and bodies (new proposal currently under consideration), as well as former third-pillar instruments such as the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (replaced by the Data Protection Law Enforcement Directive in May 2018).
Data protection was introduced within the first pillar of the EU as an internal market-related issue by Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and of the free movement of such data[12].
Directive 95/46/EC established a regulatory framework that seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal data within the

[11] Official Journal of the European Union C 303/17 - 14.12.2007, available at https://fra.europa.eu/en/charterpedia/article/7-respect-private-and-family-life.
[12] H. Hijmans and A. Scirocco, 'Shortcomings in the EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty be expected to help?', *Common Market Law Review*, 2009, 46: 1485.

European Union (EU). To do so, the Directive sets strict limits on the collection and use of personal data and demands that each Member State sets up an independent national body responsible for the supervision of any activity linked to the processing of personal data[13].

In contrast to the Data Protection Directive, the Regulation directly applies at national level – even though little implementation measures by the EU Member States are required. One of the main aims of the GDPR is to ensure legal uniformity and to remove potential obstacles to the free flow of personal data in order also to benefit national Judiciaries, which can benefit from a consistent data protection framework[14].

Since the adoption in 2001 of the EU Regulation on the protection of individuals with regard to the processing of personal data by the Community institutions, which also established the European Data Protection Supervisor (EDPS), the principles codified in the Directive must also be respected by the EU institutions when processing personal data. Moreover, the principles of the Data Protection Directive, which was enacted before the spread of the internet, were extended to the electronic communications sector by Directive 2002/58, which harmonised the laws of the Member States to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in electronic communications.[15]

The ECJ has increasingly expanded the protection of data privacy, drawing on the legally binding Charter of Fundamental Rights of the European Union to ensure a leading degree of protection in the field.

The nature of data protection as a fundamental right has been deeply embedded in European culture. Recital 1 of the GDPR provides that: '*The protection of natural persons in relation to the processing of personal data is a fundamental right.*'

The European culture of data protection

Following the *Schrems* case, the Court of Justice in 2014 gave a great impulse to the protection of personal data as enshrined in the Charter, by affirming the primacy of the European model of data protection over less protective legal systems[16].

In fact, particularly significant is the Court's ruling that when a claim is lodged with the national supervisory authorities they may, even when the Commission has adopted a decision that finds that a third country affords an adequate level of protection of personal data, examine whether the transfer of a person's data to the third country complies with the requirements of EU legislation on the protection of that data and, in the same way as the person concerned, bring the matter before the national courts, in order that the national courts make a reference for a preliminary ruling for the

[13] Eur-Lex, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l14012&from=IT.
[14] See E. De Marco, Inform Project, *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, 2018, at. 66-79.
[15] Federico Fabbrini, 'The EU Court as a Human Rights Court', in Sybe de Vries (ed), *Five Years of legally binding Fundamental Rights*, 2015, p. 6.
[16] See *Maximillian Schrems* v *Data Protection Commissioner*, Case C-362/14, 6 October 2015, ECLI:EU:C:2015:650.

purpose of the examination of that decision's validity, as the Court alone has jurisdiction to declare an EU act invalid[17].

The Court of Justice held that the existence of a Commission decision finding an adequate level of protection of the personal data transferred, ensured by third countries, cannot eliminate or even reduce the powers available to the national supervisory authorities under the Charter of Fundamental Rights of the European Union and the Directive. The Court stressed in this regard the right, guaranteed by the Charter, to the protection of personal data and the task with which the national supervisory authorities are entrusted under the Charter.

In particular, the judgment regarded the compliance of the Safe Harbour Agreement with the level of adequacy required by the Data Protection Directive for data processing, which was the result of data transfers to third countries.

The Court observed that the Safe Harbour (now replaced by the Privacy Shield) applied solely to the United States undertakings which adhered to it, and United States public authorities were not themselves subject to it. Furthermore, the national security, public interest and law enforcement requirements of the United States prevailed over the Safe Harbour scheme, so that United States undertakings were obliged not to apply the protective rules laid down by that scheme wherever a conflict with such requirements arose. The United States Safe Harbour scheme thus enabled interference, by United States public authorities, with the fundamental rights of persons as enshrined in the Charter, and the Commission decision of adequacy did not refer either to the existence, in the United States, of rules intended to limit any such interference or to the existence of effective legal protection against the interference, but only to the formal adequacy of the Safe Harbour scheme.

As regards a level of protection essentially equivalent to the fundamental rights and freedoms guaranteed within the EU, the Court held that, under EU law, legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data transferred from the EU to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down for determining the limits of the access of the public authorities to the data and of its subsequent use. The Court added that legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life.

Likewise, the Court observed that 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 her, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection, the existence of such a possibility being inherent in the existence of the rule of law.

From this perspective, the enlargement of the territorial scope of the GDPR (Article 3), read in connection with the stricter requirements set up for data transfers to third countries (Articles 44-49), are significant efforts to enhance EU data protection law on a global basis, given the centrality of the Charter.

The Data Protection Reform of 2016: the GDPR and the Law Enforcement Directive

[17] CJEU, *Press Release n. 117/2015*, https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

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 (General Data Protection Regulation), became applicable in May 2018. The rules aim to protect all EU citizens from privacy and data breaches in an increasingly data-driven world, while creating a clearer and more consistent framework for businesses, even though the GDPR refers to all individuals as beneficiaries, regardless of their nationality or place of residence (Article 1). The new rights for citizens include a clear and affirmative consent for their data to be processed and the right to receive clear and understandable information about it. Other rights are the right to be forgotten, where a citizen can ask for his/her data to be deleted, the right to transfer data to another service provider (e.g. when switching from one social network to another), and the right to know when one's data has been hacked. The new rules apply to all companies operating in the EU, even if these companies are based outside of the EU. Furthermore, it will be possible to impose corrective measures, such as warnings and orders, or fines on firms that break the rules.

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, became applicable in early June 2018. The directive protects citizens' fundamental right to data protection whenever personal data is used by law enforcement authorities. It ensures that the personal data of victims, witnesses, and suspects of crime are duly protected and facilitates cross-border cooperation in the fight against crime and terrorism[18].

Main principles of data processing

The basics: what's personal data?

The definition of personal data provided by Article 2 of the Directive and Article 4 of the GDPR are fairly similar, except for the fact that the GDPR provides for an enlargement of the notion of identifier and adds genetic factors[19]. 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
As provided by recital 26 GDPR, to determine whether a person is identifiable, a controller or another person must take into account all reasonable means that are likely to be used to directly or indirectly identify the individual, such as, for example, singling out, which makes it possible to treat one person differently from another.

[18] Fact Sheets of the European Union, available at http://www.europarl.europa.eu/factsheets/en/sheet/157/personal-data-protection.
[19] For the purpose of Directive 46/95/EC 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity; whereas Art. 4 of the GDPR provides that 'personal data' means any information relating to an identified or identifiable natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Legal persons are excluded from the application of the GDPR, even though they should not be excluded from the application of Articles 7 and 8 of the Charter and Article 8 of the ECHR[20].

The GDPR applies to pseudonomysed data but not to anonymised data. According to Article 5(e) of the GDPR, data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Consequently, if they are no longer needed, they shall be anonymised by the controller or erased upon request of the data subject. The controller shall also take into account the risk of re-identification, according to '*time, resources and effort needed in light of the nature of the data*'.[21]

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person (Article 4(5)).

Lawfulness, Fairness and Transparency

According to the principle of lawfulness, data processing is legitimate only if it is justified by law and can take place if covered by legal permission or the data subject's consent[22].
Individuals should be enabled to *fairly* understand how their personal data are handled, as regards the identity of the controller, the purpose of the processing, as well as the risks, rules, safeguards and rights in relation to the processing activities and how they can exercise those rights.
Transparency is a principle related to the processing of personal data. It should be transparent to natural persons that their personal data are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The specific purposes for which personal data are processed should be explicit, legitimate and determined at the time of the collection of the personal data. It is additionally required that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, using a clear and plain language. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data, and of how to exercise their rights in relation to such processing. These are the obligations of the data controller.
Such information could be provided in electronic form, for example, when addressed to the public, through a website. Given that children merit specific protection, any information and communication regarding processing that is addressed to a child should be in a clear and plain language such that the child can easily understand[23].
In this respect, most attention should be paid to the principle of purpose limitation, according to which personal data shall be collected for specified, explicit and legitimate purposes and not be further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes, provided that Member States ensure appropriate safeguards.

---

[20] ECtHR, *Bernh Larsen Holding AS and Others* v *Norway*, No 24117/08, 14 March 2013. See also, however, ECtHR, *Liberty and Others* v *the United Kingdom*, No 58243/00, 1 July 2008.CJEU, Joined cases C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert* v *Land Hessen* [GC], 9 November 2010, par. 53.
[21] Council of Europe, Committee of Convention 108 (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23 January 2017, par. 6.2.
[22] xxx
[23] GDPR: Recitals 13, 39, 58, 60, 71, 78, 100, 121; Arts 5(1)(a), 12(1), 13(2), 14(2), 26(1), 40(2)(a), 41(2)(c), 42(3), 43(2)(d), 53(1), 88(2).

Accountability

The GDPR introduces the general principle of accountability in Article 5(2) GDPR, which imposes the responsibility for the compliance of data processing with the GDPR and the obligation to keep a record of data processing, as well as placing the burden of proof for such compliance with the controller. Thus, the principle of accountability consists of two factors: the responsibility of the controller to ensure compliance with the GDPR; and the controller's ability to prove compliance to the Supervisory Authorities.

Data minimisation

The processing of personal data shall be restricted to adequate, relevant and limited use to what is necessary in relation to the purposes for which they are processed (recital 39 GDPR), seeking the reduction of data collection to the lowest possible level for achieving the purposes of processing.

Accuracy

This principle means that every reasonable step must be taken to ensure that data are up to date, correct or erased or rectified[24].

Integrity and confidentiality

Integrity and confidentiality are principles relating to the processing of personal data that are often treated together. More specifically, it is expected that personal data is processed in a manner that ensures the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. This is ensured by using appropriate technical or organisational measures. Controller and processor ought to adopt and implement appropriate technical and organisational measures to that effect.
The confidentiality principle aims at the prevention of unauthorised access to or use of personal data and the equipment for the processing. It should be ensured by the Member States' laws that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. In addition, the data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law[25].

Purpose limitation principle

According to this principle, the processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall be subject to a compatibility test with the initial purposes, provided that Member States ensure the appropriate safeguards.

[24] GDPR: Recital 39; Arts 5(1)(d), 18(1)(a).
[25] GDPR: Recitals 39, 49, 75, 83, 85, 162-163; Arts 5(1)(f), 28(3)(b), 32(1)(b), 38(5), 76.

The main novelties of the GDPR

1. *The Scope of the GDPR*

The material scope

The GDPR applies to any processing of personal data regarding physical persons. The Regulation becomes relevant for companies as soon as any data processing takes place. The (material) scope is interpreted in a very broad manner in order to ensure a high level of protection for individuals in connection with the protection provided by Article 7 of the CFR.

'Processing' means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means (Article 4(2) GDPR). Basically, any treatment of data will be considered as processing. Examples include collecting, recording, organising, structuring, storing and erasing of data.

Article 2(2) GDPR provides for four exceptions as to the material scope of application, as it does not apply in the areas outside the scope of Union Law (a), of security policy (b), if connected to criminal persecution (d), and purely for personal or household activity (c)[26].

The territorial scope

Although the GDPR is a European Regulation, its territorial reach extends over European boundaries. From a territorial perspective, the GDPR does not differentiate between controller and processor and sets out the same territorial scope for both. The GDPR mainly applies in the following two situations: the processing of personal data takes place in the context of the activities of an establishment of the controller or processor within the EU; or the processing of the data of individuals within the EU is carried out by a controller or processor not established in the EU.[27]

Compared to Directive 95/46/EC, the GDPR seeks to extend the reach of EU data protection law under the material and territorial scope of application. In particular:

- An EU-based data controller or processor comes under its scope where personal data is processed 'in the context of its activities';
- Where no EU presence exists, the GDPR still applies whenever:

    1. An EU resident's personal data is processed in connection with goods and services; or
    2. The behaviour of individuals within the EU is 'monitored'.

If neither controller nor processor is established within the EU, the GDPR can apply nevertheless. According to this principle, the applicable law depends on where the relevant contractual performance is being offered. Even the nationality of the customers is not relevant as long as they are located in the EU.

---

[26] P. Vogt and A. von dem Bussche, *The EU General Data Protection Regulation. A practical guide*, Springer, 2017, at 9, 10, 11, 12, and 13.

[27] This section is also based on Professor Christopher Kuner's keynote speech delivered during the e-Nact Workshop on Data Protection held in Florence on 28-29 January 2019.

The GDPR sets up a cluster of core issues such as:

- **establishment**, as the effective and real exercise of activity through stable arrangements[28]; **establishment principle**, according to which the choice of law depends on where an entity is established;
- **stable arrangement**, which means that it does not matter whether the relevant body is a branch or a subsidiary company with legal personality;
- **stability**, which must be determined in connection with the specific nature of the activity.

The GDPR applies under Article 3 in three circumstances:

- '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' (Article 3(1)); or
- 'The processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union' where the processing is related to the offering of goods or services (regardless of payment) to data subjects in the Union or the monitoring of their behaviour as far as it takes place within the Union (Article 3(2)); or
- 'The processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law' (Article 3(3)).

The first scenario is the processing '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 locution '*in the context of the activities*' must be interpreted in the sense that there has to be a connection between the economic activity of the establishment and the data processing, but it is not necessary that the establishment carries out any data processing itself.
Moreover, it should be interpreted broadly (Case C-131/12, *Google Spain*, par. 53) and can apply if a non-EU controller/processor and an EU establishment are 'inextricably linked', such as if the EU establishment raises revenue that helps enable the processing (*Google Spain,* par. 56).

The locution 'Regardless of whether the processing takes place in the Union or not' can envisage different situations:

- A data processor with an EU establishment is subject to data processor obligations (Article 28) but not data controller obligations.
- When an EU controller uses a non-EU processor, the processor is not directly subject to the GDPR, but may be indirectly subject by contract under Article 28 (e.g., the EU controller has to enter into a data processing agreement with a non-EU processor).
- An establishment of an EU data processor is not normally considered to be an establishment of the controller: i.e., a non-EU controller will not become subject to the GDPR by choosing a processor in the Union. This last case can leave a gap in protection (e.g., if the EU processor has a data breach, neither the controller nor the processor will have to notify this to DPAs or individuals).

[28] Recital 22: '[E]stablishment implies the effective and real exercise of activities through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.'

Article 3 sets out the conditions under which the GDPR applies to data processing with connections beyond the EU.
It thus sets out the basis of the GDPR's relations to third countries and its place in the wider world. There is huge interest in third countries about the scope of Article 3 and the extent to which the GDPR can apply to them.

The predecessor to Article 3 was Article 4 of the EU Data Protection Directive 95/46/EC, which was both an applicable law and a jurisdictional provision (i.e., it determined both which Member State law applied and the territorial scope of the Directive).

The evolution of the territorial scope of EU data protection law can be drawn through the most relevant CJC case-law:

- *Bodil Lindqvist*, Case C-101/01 (2003): the Court found that the DPD should not be interpreted to apply to the entire Internet (note the long gap before the next ruling, which shows how little attention was paid to this topic until recently).
- *Digital Rights Ireland*, Joined Cases C-293/12 and C-594/12 (Grand Chamber) (2014): the case did not deal with territorial scope *per se*, but par. 68 indicates that Charter protections must apply when data are held outside the EU.
- *Google Spain*, Case 131-12 (Grand Chamber) (2014): application of the law to an EU establishment was based on being 'inextricably linked' with a non-EU establishment. As the activities of Google's European affiliates were deemed inextricably linked to the operation of the Google search engine by the Google parent company in the United States, the search engine was subject to EU data protection law.
- *Weltimmo,* Case C-230/14 (2015): the case dealt with applicable law and the allocation of jurisdiction between Member State data protection authorities (DPAs).
- *Schrems*, Case C-362/14 (Grand Chamber) (2015): affirmed that data transfer rules must comply with the Charter and fundamental rights standards. In particular, the Court invalidated the EU-US Safe Harbour scheme because it did not ensure effective adequate protection against data access by US public authorities with regard to personal data that had been transferred to the United States
- *EU-Canada PNR*, Opinion 1/15 (Grand Chamber) (2017): evaluated the application of EU standards to data processing in Canada.
- *Wirtschaftsakademie*, Case C-210/16 (Grand Chamber) (2018): the Court opined on applicable law and DPA competence in an intra-EU context.
- *Google* v *CNIL*, Case C-507/17, Grand Chamber (24 September 2019): under the DPD and the GDPR, the right to dereferencing of search engine results should only apply within the EU; the nature of the Internet means that the extraterritorial effects of EU law should not apply (note: the Court interprets the territorial scope of the right to erasure under Article 17 GDPR which refers only to Member States and distinguishes it from the territorial scope of application of the GDPR under Article 3).

The second scenario is the processing of personal data of data subjects in the Union by a controller or processor not established in the Union where the processing is related to the offering of goods or services to data subjects in the Union or the monitoring of their behaviour in as far as it takes place within the Union.

This situation requires the processing of the personal data of data subjects who are in the Union by a controller or processor not established in the Union and one of the two following factors:

- The processing is related to the offering of goods or services (regardless of payment) to data subjects in the Union, or

- The monitoring of their behaviour in as far as it takes place within the Union.

The processing of the personal data of data subjects who are in the Union:
- Applies only to individuals in the Union, regardless of nationality, residence, or legal status.
- Processing of EU individuals in a third country is not covered unless related to targeting of individuals in the Union or the monitoring of their behaviour.

The offering of goods or services (regardless of payment) to data subjects in the Union ('targeting'):

- CJEU judgments in other contexts are relevant (e.g., Joined Cases C-585/08 and C-144/09, *Pammer* and *Hotel Alpenhof)*.

- The EDPB has mentioned the following criteria that can indicate the offering of good or services in the Union (EDPB, Guidelines 3/2018, pp. 15-16).[29]

The Guidelines drafted by the EDPB in 2018 state that: '*The EDPB does not consider that any online collection or analysis of personal data of individuals in the EU would automatically count as 'monitoring'. It will be necessary to consider the controller's purpose for processing the data and, in particular, any subsequent behavioural analysis or profiling techniques involving that data*.'

Potential examples of monitoring activities could be '*behavioural advertisement; geo-localisation activities, in particular for marketing purposes; online tracking through the use of cookies or other tracking techniques such as fingerprinting; personalised diet and health analytics services online; CCTV; market surveys and other behavioural studies based on individual profiles; monitoring or regular reporting on an individual's health status.*'[30]

The third scenario envisaged by Article 3 is 'the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.'
Application of the GDPR to international organisations and the diplomatic missions of third countries is controversial. The EDPB gives examples of the GDPR applying in Member State embassies and on cruise ships.
However, Article 3(3) evidences the EU legislator's poor understanding of public international law, at least with regard to embassies. Member State law does not apply in an embassy or diplomatic representation 'by virtue of public international law'.
In fact, public international law provides the opposite: under Article 41(1) of the Vienna Convention on Diplomatic Relations, a diplomatic representation must respect the law of the receiving State (without prejudice to its privileges and immunities).

---

[29] (1) The EU or at least one Member State is designated by name with reference to the good or service offered; (2) the data controller or processor pays a search engine operator for an internet referencing service in order to facilitate access to its site by consumers in the Union; or the controller or processor has launched marketing and advertisement campaigns directed at an EU country audience; (3) the international nature of the activity at issue, such as certain tourist activities; (4) the mention of dedicated addresses or phone numbers to be reached from an EU country; (5) the use of a top-level domain name other than that of the third country in which the controller or processor is established, for example '.de', or the use of neutral top-level domain names such as '.eu'; (6) the description of travel instructions from one or more other EU Member States to the place where the service is provided; (7) the mention of an international clientele composed of customers domiciled in various EU Member States, in particular by presentation of accounts written by such customers; (8) the use of a language or a currency other than that generally used in the trader's country, especially a language or currency of one or more EU Member states; (9) the data controller offers the delivery of goods in EU Member States.
The monitoring of their behaviour as far as it takes place within the Union:
Recital 24: 'In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques which consist of profiling a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.'
[30] EDPB, Guidelines 3/2108, available at https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3_en, at 18.

Nothing prevents Member States from applying the GDPR in their embassies, but they have to reconcile it with application of the law of the receiving state; however, the receiving state law cannot be enforced against them because of their privileges and immunities.

Since *Digital Rights Ireland* in 2014, the CJEU has emphasised the need to interpret the territorial scope of data protection law expansively as a way to protect fundamental rights.
The case *Google* v *CNIL* (Case C-507/17), against the backdrop of EDPB Guidelines 3/2018, indicates that the CJEU is restricted in the extraterritorial scope of the GDPR.
The right to dereferencing of search engine results should only apply within the EU. As a data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller has the obligation to erase personal data without undue delay where one of the grounds listed in that provision applies, the fact that the search engine is operated by an undertaking that has its seat in a third State cannot result in the processing of personal data carried out for the purposes of the operation of that search engine in the context of the advertising and commercial activity of an establishment of the controller on the territory of a Member State escaping the obligations of EU law. The supervisory or judicial authorities of Member States are competent to weigh up 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. Nonetheless, numerous third States do not recognise the right to dereferencing. Therefore, while the EU legislature has, in Article 17(3) GDPR, struck a balance between that right and that freedom so far as the Union is concerned, it must be found that, by contrast, it has not struck such a balance as regards the scope of a dereferencing outside the Union. Article 17 GDPR should be interpreted in the sense that it does not confer a scope on the rights enshrined in it that would go beyond the territory of the Member States and it does not impose on an operator which, like Google, falls within the scope of that Directive or that regulation a dereferencing obligation which also concerns the national versions of its search engine that do not correspond to the Member States.

Another judgment released by the Court of Justice on 3 October 2019 in the case *Eva Glawischnig-Piesczek* v *Facebook Ireland Limited* (Case C-18/18) came to completely different conclusions, despite the fact that the relevant legal framework was not the GDPR but Directive 31/2000 on electronic commerce, which holds that EU law does not preclude a host provider such as Facebook from being ordered to remove identical and, in certain circumstances, equivalent comments previously declared to be illegal and, in particular, EU law does not preclude such an injunction from producing effects worldwide, within the framework of the relevant international law which it is for Member States to take into account[31].

The facts regarded the case of Mme Eva Glawischnig-Piesczek, a member of the Nationalrat (National Council, Austria), chair of the parliamentary party Die Grünen (Greens) and federal spokesperson for that party who sued Facebook Ireland in the Austrian courts. She sought an order to compel Facebook Ireland to remove a comment published by a user on that social network that was harmful to her reputation, and allegations which were identical and/or of an equivalent content.

Under EU law, it is possible to order a host provider to remove information which it stores, the content of which is identical to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information. In addition, to order a host provider to remove information which it stores, the content of which is

[31] See https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-10/cp190128en.pdf.

equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned in such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content. A host provider can also be ordered to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.

Development of the territorial scope of the GDPR by the courts and DPAs will continue to be marked by tension between the protection of fundamental rights and the need to limit the extraterritorial reach of EU law.

2. *Data transfers to third countries*

International trade and international co-operation are based on flows of personal data to and from the European Union. However, the transfer of such personal data from the EU to controllers and processors located outside the EU in third countries should not undermine the level of protection of the individuals concerned, a third country being any country outside the European Economic Area (the 'EEA')[32].

Cross-border data transfers must comply with safeguards provided by the GDPR, on the basis of a twofold approach: data transfers must be compliant not only with the lawfulness of processing but also with the specific provisions set in Articles 44-49. This also includes onward transfers.

In addition to consent, Article 6 of the General Data Protection Regulation (GDPR) sets forth further authorisation reasons, such as fulfilling a contract or protecting vital interests. For special personal data which requires a higher level of protection, Article 9 of the GDPR provides separate legal requirements.

Once it has been assessed that data transfers meet the general requirements, the second step is to determine whether transfers to the third country are permitted. Secure third countries are those for which the European Commission has confirmed a suitable level of data protection on the basis of an adequacy decision. Data transfer to these countries is expressly permitted.

In the lack of an adequacy decision for a country, the controller must ensure in another way that the personal data will be sufficiently protected by the recipient. This can be assured by using standard contractual clauses, for data transfers within a Group through so-called 'binding corporate rules,' through the commitment to comply with codes of conduct which have been declared by the European Commission as being generally applicable, or by certification of the data processing procedure. Furthermore, there are several exceptions which legitimise data transfers to a third country, even if the protection of personal data cannot be sufficiently assured. Most frequently, the consent of the data

[32] *EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22018-derogations-article-49-under-regulation_en

subject is relevant here. At the same time, one must particularly note the requirements for such consent to be freely given. Further exceptions, such as transmitting to fulfil contracts, important reasons of public interest and the assertion of legal rights are usually less relevant in practice.

Especially from an economic point of view, data transfers between the United States and the European Union are of utmost importance. Since the CJC in the *Schrems* case declared the Safe Harbour agreement invalid, it has been replaced by another unique framework, the Privacy Shield, which should provide a stricter set of ground rules for data transfer from the EU to the US. However, many points criticised by the Court during the *Schrems* ruling still persist in the new arrangement. Therefore, the Privacy Shield is currently under high scrutiny by the European Data Protection Authorities, as well a key issue of the referral to CJC of the case *Schrems II* (reference for a preliminary ruling from the High Court of Ireland made on 9 May 2018 in *Data Protection Commissioner* v *Facebook Ireland Limited, Maximillian Schrems* - Case C-311/18).

The first legal basis laid down by the GDPR is the adequacy decision adopted by the Commission, according to the requirements mentioned in Article 45.

In the absence of an adequacy decision, other legal bases are the following: the consent explicitly related to the proposed transfer (Article 49); appropriate safeguards such as the standard contractual clauses approved by the Commission or by the supervisory authorities (Article 46); binding corporate rules approved by the competent supervisory authority (Article 47).
If no appropriate safeguards or standard contractual clauses are applicable, the GDPR – besides the case of explicit consent – provides derogations for specific situations such as:

- the performance of a contract;
- reasons of public interest;
- processing that is necessary for the exercise of legal claims (Article 49).

The most important new element of the GDPR is that the lack of compliance with the standards provided by Articles 44-49 determines the imposition of fines which amount up to 20,000,000.00 Euro or up to 4% of the total worldwide annual turnover (Article 83 GDPR).

2.1. Transfers on the basis of an adequacy decision

An adequacy decision implies that the European Commission has decided that a third country or an international organisation ensures an adequate level of data protection.

When assessing the adequacy of the level of protection, the European Commission takes into account elements such as the laws, respect for human rights and freedoms, national security, data protection rules, the existence or the effective functioning of data protection authorities and binding commitments entered into by the country in respect of data protection.

The adoption of an adequacy decision involves:

- a proposal from the European Commission
- an opinion of the European Data Protection Board ('EDPB')
- an approval from representatives of EU countries
- the adoption of the decision by the European Commissioners

The effect of such a decision is that personal data can flow from the EEA to that third country without any further safeguard being necessary. In other words, the transfer is the same as if it was carried out within the EU.

2.2. Transfers subject to appropriate safeguards

In the absence of an adequacy decision, the GDPR does allow a transfer if the controller or processor has provided 'appropriate safeguards'. These safeguards may include:

- **Standard data protection clauses**: For the majority of organisations, the most relevant alternative legal basis to an adequacy decision are standard contractual clauses. These are model data protection clauses that have been approved by the European Commission and which enable the free flow of personal data when embedded in a contract. The clauses contain contractual obligations on the Data Exporter and the recipient, and rights for the individuals whose personal data is transferred.

- **Binding corporate rules 'BCRs':** BCRs form a legally binding internal code of conduct operating within a multinational group, which applies to transfers of personal data from the group's EEA entities to the group's non-EEA entities. This group may be a corporate group or a group of undertakings engaged in a joint economic activity, such as franchises or joint ventures. BCRs are legally binding data protection rules with enforceable data subject rights contained in them, which are approved by the competent Data Protection Authority. There are two types of BCRs which can be approved: BCRs for Controllers, which are used by the group entity to transfer data that they have responsibility for, such as employee or supplier data; and BCRs for Processors, which are used by entities acting as processors for other controllers.

- **Approved Codes of Conduct:** The use of Codes of Conduct as a transfer tool, under specific circumstances, has been introduced by the GDPR in Article 40 (3). Codes are voluntary and set out specific data protection rules for categories of controllers and processors. They can be a useful and effective accountability tool, providing a detailed description of what is the most appropriate, legal and ethical behaviour within a sector. From a data protection viewpoint, codes can therefore operate as a rulebook for controllers and processors who design and implement GDPR-compliant data processing activities that give operational meaning to the principles of data protection set out in European and national law. Codes of Conduct that relate to personal data processing activities by controllers and processors in more than one EU Member State, and for which the EU Commission has adopted an implementing act, together with binding and enforceable commitments of the controller or processor in the third country, could be used as a transfer tool in the future.

- **Approved certification mechanisms:** these instruments have been introduced in the GDPR in Article 42 (2), with the aim to develop certification mechanisms able to demonstrate the existence of appropriate safeguards provided by controllers and processors in third countries. These controllers and processors would also make binding and enforceable commitments to apply the safeguards including provisions for data subject rights.

- **A legally binding and enforceable instrument between public authorities or bodies**: An organisation can make a restricted transfer if it is a public authority or body and is transferring to another public authority or body, and with both public authorities having signed a contract or another instrument that is legally binding and enforceable (Article 46 (2)(a) GDPR). This contract or instrument must include enforceable rights and effective remedies for individuals

whose personal data is transferred. This is not an appropriate safeguard if either the transferring organisation or the receiver is a private body or an individual. If a public authority or body does not have the power to enter into legally binding and enforceable arrangements, it may consider an **administrative arrangement** that includes enforceable and effective individual rights instead (Article 46 (3)(b) GDPR).

2.3. Derogations for specific situations

Finally, Article 49 provides specific exemptions from the general principle that personal data may only be transferred to a third country if an adequate level of protection is provided for in that third country. These derogations occur in specific situations, such as those based on consent, for the performance or conclusion of a contract, for the exercise of legal claims, to protect the vital interests of the data subject where they cannot give consent or for important reasons of public interest.

3. *Special categories of data*

The EU legislator prohibits data processing for special categories of data (Article 9 GDPR). The special categories of data that shall be prohibited are: 1) data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; 2) genetic data; 3) biometric data for the purpose of uniquely identifying a natural person; 4) data concerning health; and 5) data concerning a natural person's sex life or sexual orientation.

Data processing is allowed for such data when the processing is carried out: in the field of employment or social security; when processing is necessary to protect vital interests; processing is manifestly made public by the data subject; processing is necessary for reasons of substantial public interest; processing is necessary for reasons of public interest in the area of public health or for predictive medicine or occupational; and, when processing is necessary for reasons of achieving public interest.

As regards genetic data, biometric data and data concerning health, Member States may provide for further limitations.

The GDPR for the first time introduces the concept of:

Biometric data
Biometric data are a special category of personal data resulting from technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person.
Biometric data constitute one of the categories of *special data*. They are by their nature particularly sensitive in relation to fundamental rights and freedoms and merit specific protection as the context of their processing could create significant risks. Processing is initially forbidden unless specifically allowed by the Regulation or Directive or stricter law of the Member State. It is also vital that processing is strictly necessary and appropriate safeguards are applied for the rights and freedoms of the data subject.

Genetic data
They fall into the special categories of personal data for which the GDPR (Article 9) as well as the Law Enforcement Directive (Article 10) provide for with a special processing provision. More specifically, genetic data as well as other special categories of personal data, should be processed for

health-related purposes only to the benefit of natural persons and society as a whole, or to serve the public interest, for scientific, historical research or statistical purposes[33].

4. *Automated decision-making*

With regards to 'profiling' techniques – which include any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements – the GDPR has provided for a particular protection of the data subject in case of an automated process[34]. In fact, according to Article 22 GDPR, the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Exceptions are foreseen in the case that an automated decision is necessary for entering into, or performance of, a contract between the data subject and a data controller; it is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or it is based on the data subject's explicit consent. In any case, such exceptions do not apply to the special categories of data provided by Article 9.

5. *The right in the scope of consent (in case it is the legal ground for data processing)*

Consent is defined by Article 4 of the GDPR as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Consent has no longer the same relevance which it had under the Directive 46/95/EC, but it is only one of the legal bases of data processing. Despite its relevance, it has been included among other legal justifications of data processing. This is in particular due to the fact that consent has to be freely given in cases of a clear imbalance between the data subject and the controller. For example, the GDPR prohibits consent as a condition for the performance of a contract. The data subject can withdraw his or her consent at any time (Article 7(3)).
As for children's consent, the GDPR provides a novelty by setting the minimum age of 16 years for valid consent and allowing that consent be given for younger children by the holders of parental responsibility.

Among the other legal bases of lawful processing, legal permission could rely on data processing which is (Article 6, b) necessary for the performance of a contract of which the data subject is party; (Article 6, c) necessary for the compliance with legal obligations of which the controller is subject; (Article 6, d) necessary to protect the vital interest of the data subject; (Article 6, e) necessary for the performance of a task carried out in the public interest; (Article 6, f) necessary for the legitimate interests pursued by the controller or third party.

5.1. Conditions of consent

If the consent is given in the context of a written declaration that also concerns other matters, the

[33] Inform Project, *Data Protection Glossary*, 2018, at 26.
[34] Fundamental Rights Agency, *Handbook on European Data Protection law*, Publications Office of the European Union, 2018, at 99.

request for consent shall be presented in a manner that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language (Article 7 (2) GDPR).
Despite the fact that the GDPR does not provide for formal requirements as to the consent, in comparison with the Directive, it requires stricter conditions for obtaining the data subject's consent. Written form is desirable, although not mandatory. In particular, if the consent is given in the context of a written declaration that also concerns other matters, the request for consent shall be delivered in a manner that is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

As an alternative to 're-consent', Article 6 (4) entitles data controllers to perform a compatibility test to ascertain whether processing for another purpose is compatible with the previous purpose for which personal data has been collected. Where the further processing purposes are compatible, then no additional consent (or any other separate legal basis) shall be required. More precisely, in order to lawfully undertake 're-processing' without 're-consenting' both the following conditions should be met: (a) the original processing complied with all requirements for its lawfulness; and (b) the compatibility test confirms that the purposes of original processing and those of secondary processing are compatible.

6. *One-stop-shop mechanism*

The one-stop-shop mechanism provided by Article 56 GDPR means that, as a main rule, organisations carrying out cross-border personal data processing activities will only have to deal with one supervisory authority in the future.
We will deepen the discussion on this novelty in the section on National Supervisory Authorities.

7. *Data portability*

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided originally. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract, in case the processing is carried out by automated means. It also includes the right of the data subject to have the personal data transmitted directly from one controller to another, where technically feasible. However, it shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller.
Rights and freedoms of others as well as the right to erasure of the data subject shall not be compromised by the exercise of data portability.
The intrinsic limit of this right – aimed at ensuring fair competition between service providers – is that it applies only when the processing is based on the data subject's consent. Nonetheless, Article 23 GDPR grants EU Member States a broad competence to limit data subject's rights.

8. *Organisational measures*

The GDPR introduces specific organisational measures for controllers and processors, from which a legal responsibility for the compliance with the respective obligations under the GDPR arises. This aspect will be discussed in the section on controllers' and processors' obligations.

9. *European Data Protection Board*

Article 68 GDPR establishes a European Data Protection Board, which replaces the Article 29 Working Party established under the Data Protection Directive.

10. *Sanctions*

Remedies and sanctions have been strengthened by the GDPR for the violation of the right to personal data. In particular, administrative fines have been designed by the EU in order to discourage violation by data controllers as they may substantially affect the business assets of undertakings.

The rights of data subjects

By and large, the data subject has the right to receive transparent information and communication on the modalities for the exercise of his or her rights.

Conversely, this broad right corresponds to the obligation of controllers to take appropriate measures to provide any information referred to in those cases where personal data are or not collected from the data subject and any communication on the exercise of the right of access, rectification, erasure, restriction of processing, data portability or right to object relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

The communication must be made available in an easily accessible form.[35]

The right of access (Article 15 GDPR)

A data subject should have the right of access to the following information: the categories of personal data collected; the recipients; the purposes of data processing; and when it is possible, the estimated period for which the personal data will be stored, or, if not possible, the criteria used to determine that period. The data subject should be able to exercise that right easily and whenever he or she wishes, in order to check the lawfulness of the processing.
Additionally, access should be provided to information regarding: the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing and the right to an effective judicial/administrative remedy[36].
The right to access should not adversely affect the rights or freedoms of others, including trade secrets

[35] P. Vogt and A. von dem Bussche, *The EU General Data Protection Regulation. A practical guide*, Springer, 2017, at 143.
[36] See *Data protection glossary*, available at http://informproject.eu/wp-content/uploads/2018/04/D2.11-Data-Protection-Glossary.pdf.

or intellectual property and, in particular, copyright protecting software[37].

Member States should be able to adopt legislative measures delaying, restricting or omitting the information to data subjects or restricting, wholly or partly, the access to their personal data under certain circumstances, provided that such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned.

The right to rectification and erasure (Articles 16 & 17 GDPR)

The data subject has the right to obtain from the controller the rectification of inaccurate personal data or erasure of personal data concerning him or her also: by having incomplete personal data completed, and the erasure to be done without undue delay in cases where the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; the data subject withdraws the consent on which the processing is based and, where there is no other legal ground for the processing, the data subject objects to the processing and there are no overriding legitimate grounds for the processing; the personal data have been unlawfully processed; the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; or the personal data have been collected in relation to the offer of information society services directly to a child.

In case data are no longer necessary in relation to the purpose for which they were processed, the data subject can request the erasure. The burden of proof is up to the data subject.

The exercise of such a right implies that data become unusable in a way that prevents the controller, the processor or any third party from accessing and processing the data – irrespective of any physical destruction or deletion.

Consequent to the right of erasure, Article17(1) GDPR provides also for the right to be forgotten, which entails the obligation of the controller to take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

This right is relevant also in light of consent's withdrawal, as in such case there are no other legal grounds for processing. Consequently, a right to erasure could arise.

The right to erasure is not an absolute right, as it shall be balanced with other rights. In fact, it does not apply to the extent that processing is necessary for exercising the right of freedom of expression and information; or compliance with a legal obligation; or reasons of public interest in the area of public health; or archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; or for the establishment, exercise or defence of legal claims.

The right to restriction of processing (Article18 GDPR)

Where there is an issue on the lawfulness of data processing, a contestation of the accuracy, an objection by the data subject or the personal data are no longer necessary for the purposes of the processing, the data subject shall have the right to obtain from the controller restriction of processing.

[37] P. Vogt and A. von dem Bussche, at 153.

The right to object (Article 21 GDPR)

When the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or the processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, the data subject has the right to object. Such right is not subject to any time restrictions. As a consequence to the exercise of this right, the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. It applies to profiling activities and can be exercised by automated means. The data subject has also the right to object to the use of his or her personal data for direct marketing purposes at any time and free of charge. Data subjects must be informed of this right in a clear manner, separate from any other information. A logical consequence of the right to object could be the right to erasure, as clarified also by the explanatory report of Convention 108 (par. 79, explanatory report).

Controllers and processors

A 'controller' is a natural or legal person, public authority, agency or other body that, alone or jointly with others, determines the purposes and means of the processing of personal data, Article 4(7) GDPR[38]. The definition is identical with the one in the Data Protection Directive. Thus, the legal definition consists of three main components:
(1) a natural or legal person, public authority, agency or other body;
(2) that alone or jointly with others;
(3) determines the purposes and means of data processing.

The concept of 'processor' is defined by Article 4(8) as 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.

As expressly provided also in Article 2(d) of Directive 95/46, the concept of 'controller' refers to the natural or legal person who 'alone or jointly with others determines the purposes and means of the processing of personal data'. Therefore, that concept does not necessarily refer to a single natural or legal person and may concern several actors taking part in that processing, with each of them then being subject to the applicable data protection provisions (see, to that effect, judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, par. 29).

The objective of that provision being to ensure, through a broad definition of the concept of 'controller', effective and complete protection of the persons concerned, the existence of joint responsibility does not necessarily imply equal responsibility of the various operators engaged in the processing of personal data. On the contrary, those operators may be involved at different stages of that processing of personal data and to different degrees, so that the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case (see, to that effect, judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, par. 28, 43 and 44).

[38] P. Vogt and A. von dem Bussche, *The EU General Data Protection Regulation. A practical guide*, Springer, 2017, at 17.

However, a natural or legal person who exerts influence over the processing of personal data, for his or her own purposes, and who participates, as a result, in the determination of the purposes and means of that processing, may be regarded as a controller within the meaning of Article 2(d) of Directive 95/46.

Furthermore, the joint responsibility of several actors for the same processing, under that provision, does not require each of them to have access to the personal data concerned (see, to that effect, the judgment of 5 June 2018, *Wirtschaftsakademie Schleswig-Holstein*, C-210/16, EU:C:2018:388, paragraph 38). Article 26 GDPR provides for legal discipline of joint controllers[39].

Main obligations of controllers and processors

Responsibility, liability, accountability

Article 24 GDPR establishes, as a general rule, the responsibility and liability of the controller for any processing of personal data carried out by itself or on its behalf. As a consequence, it is obliged to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the Regulation.
The controller is also obliged to record processing activities (Article 30 GDPR) regarding the name, the contact details of the controller, the categories of data subjects, personal data and data recipients, and a description of the security measures. It provides also for an exemption for any enterprise or organisation employing less than 250 persons.

Data security

Several obligations are introduced by the GDPR in light of ensuring data security.
Article 32 GDPR obliges the controller and processor to undertake organisational and technical measures. This is one of the most fundamental obligations under the GDPR. Its breach can result in fines of up to EUR 10,000,000.00 or 2% of the total worldwide annual turnover (Article 83(4)).
Controllers must undertake a risk-based approach towards data security through an objective risk assessment. For example, risk factors to be taken into account are discrimination or the presence of special categories of data.

Among other measures we remember:

- pseudonomysation and encryption;
- ability to ensure ongoing confidentiality, integrity, availability and resilience of processing: confidentiality, integrity, availability and resilience
- ability to restore availability and access to personal data in a timely manner in case of a physical/technical incident
- process for regularly testing, assessing and evaluating effectiveness of technical and organisational measures.

[39] See Fundamental Rights Agency, *Handbook on European Data Protection law*, Publications Office of the European Union, 2018, at 107-109.

Privacy by design and privacy by default

Among the specific measures imposed on controllers for not complying with the legal obligations prescribed by the GDPR, Article 25 provides for a prospective obligation to implement compliance measures both at the time of processing and when determining the means of processing.

This obligation is prospective and is divided into two parts: by design, the controller shall implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects. By default, the controller shall ensure that personal data are not made accessible without the individual's intervention to an indefinite number of natural persons and that only personal data which are necessary for each specific purpose of the processing are processed. Concrete examples of privacy by design may be including IT systems directed towards data minimisation or pseudonymisation, whereas privacy by default involves, for example, the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility.

Cooperation with Supervisory Authorities

The specific obligation to cooperate shall take place upon request by supervisory authorities.

In order to avoid simultaneous processing and given the principle of the competence of national authorities, Article 56 provides the mechanism of the 'one-stop-shop', by which one Lead Supervisory Authority shall act as sole contact point for the controller/processor whose processing activities affect multiple EU Member States. 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.

Personal Data Breach

The GDPR introduces a general obligation of the controller towards the Supervisory Authorities in case of a personal data breach. Such a breach may occur by way of a technical or physical incident. The notification must take place within a 72-hour time frame of the controller becoming aware of the breach. In case of an incident with a high risk for the rights and freedoms of the data subjects concerned, the controller will have to communicate the breach also to them. In such a case, assistance from the Supervisory Authority will be available to the controller.
The EU legislator has also introduced an important novelty as regards the cooperation between controllers (joint controllers), according to which they shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referring to the exercise of the right of information and access (Article 26 GDPR).

In order to qualify as joint controllers under Article 26 GDPR, (1) two or more controllers must (2) jointly determine the purposes and means of processing.
Article 31 GDPR stipulates the general obligation to cooperate with Supervisory Authorities. This obligation applies to the controller, processor and, if applicable, their respective representatives.

Data protection impact assessment

The assessment shall contain at least a general description of the envisaged processing operations and the purposes of the processing, the legitimate interest pursued by the controller, an assessment of the necessity and proportionality of the processing operations in relation to the purposes, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address those risks including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the relevant legislation, taking into account the rights and legitimate interests of the data subjects and other persons concerned.
The controller shall carry out this assessment before the processing, in cases where processing operations are likely to result in a high risk to the rights and freedoms of data subjects, taking into account the nature, scope, context and purposes of the processing. The scope should be the evaluation of the origin, nature, particularity and severity of that risk while the outcome of the evaluation is of specific importance in determining the appropriate measures to be taken in order for the processing to comply with the Regulation and Directive.
The minimum requirements set up by Article 35 GDPR are a systematic description of the purposes and envisaged processing operations and, where applicable, the legitimate interest pursued by the controller, an assessment of the necessity and proportionality of the processing in relation to its purpose, an assessment of the risks to the rights and freedoms of the data subjects, and the measures envisaged to address the risks.

Designation obligation

According to Article 37 GDPR, private entities are obliged to designate a DPO when they perform regular and systematic monitoring and the core activities consist of the regular and systematic monitoring of data subjects on a large scale, or when they process special categories of personal data, and their core activities consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences.

Obligations of processors

Article 28 provides that the controller can commit the processor to specific obligations in the data processing agreements. In any event, processors are obliged to implement technical and organisational measures, to designate a Data Protection Officer (DPO) and to cooperate with the supervisory authorities.

Supervisory Authorities

As a general principle, supervisory authorities are given competence *'for the performance of the tasks assigned to and the exercise of the powers conferred'* on them on their national territory, as described in the GDPR. Recital 122 tells us that this competence includes *'processing affecting data subjects on its territory or processing carried out by a controller or processor not established in the Union when targeting data subjects residing in its territory'*.

According to Article 55 each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.

The practical cases to determine the competence of Supervisory Authorities may be the following: the controller/processor being established on the territory of the EU Member State of that Supervisory Authority; data subjects residing in the EU Member State of that Supervisory Authority being substantially affected/likely to be substantially affected by processing; or a complaint having been lodged with that Supervisory Authority.

In cases of cross-border data processing, a lead authority system is set up.

The GDPR identifies two situations of cross border processing. The first is data processing in the context of the activities of establishments in more than one Member State of a controller, where the controller is established in more than one Member State. The second situation occurs when the processing intervenes in the context of the activities of the single establishment of a controller, but which substantially affects - or is likely to substantially affect - data subjects in more than one Member State. This criterion must be interpreted on a case-by-case basis.

The identification of the lead supervisory authority is based on the main establishment of the data controller. The notion of the main establishment is defined in the GDPR as '*a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment*'.

However, the notion of a central administration is not always applicable. In order to identify which is the lead supervisory authority the following elements should be taken into consideration: where the decisions concerning the purposes and means of processing are given the final 'sign off'; where the decisions on business activities involving data processing are taken; where the effective implementation power of the decision regarding the processing lies; the location of the directors with overall management responsibilities; and where the company is registered.

For controllers, the main establishment will be either the place of central administration in the EU or, if decisions on the purposes and means of the processing do not take place there, the place where such decisions are made. Note that with regard to the latter the Guidelines provide a list of factors that will be relevant when identifying the main establishment. The physical location of the data processing equipment (e.g. servers) does not influence the identification of the main establishment.

For processors, the main establishment is either their place of central administration in the EU or the place of the establishment in the EU where the main processing activities take place. Further guidance is not provided as to how to interpret 'main processing activities'.

In cases involving a controller and a processor, the lead authority will be the lead authority of the controller. In this instance, the lead authority of the processor will take the role of a concerned authority.

Cases may comprise: (i) processing of personal data by the *same* controller or processor through local operations across more than one Member State (e.g. local branch offices); or (ii) the processing of personal data by a controller or a processor established in a single Member State that *'substantially affects or is likely to substantially affect'* data subjects in more than one Member State.

Supervisory authorities have an independent status.

In compliance with the duty of cooperation, supervisory authorities are required to provide assistance to each other in the form of information or carrying out *'prior authorisations and consultations, inspections and investigations'*. The European Commission can specify forms and procedures for mutual assistance.

Supervisory authorities can conduct joint investigation and enforcement operations. A supervisory authority has a right to be included in such operations if a controller has an establishment on its territory or a significant number of its data subjects are likely to be substantially affected.

Among the main tasks of supervisory authorities, we note: the duty to enforce the application of the GDPR; upon request, to provide information to any data subject concerning the exercise of their rights under this Regulation; to handle complaints lodged by data subjects; to conclude investigations; and to adopt standard contractual clauses and binding corporate rules for data transfers to third parties (Article 46 GDPR).

Even the lead authority must co-operate with other 'concerned' supervisory authorities. They are obliged to exchange information and try to reach consensus.

The lead authority must provide information to the other supervisory authorities and it can seek mutual assistance from them and conduct joint investigations with them on their territories.

Among its powers, we recall the power to: order controllers to provide any information, including all personal data, necessary for the performances of its tasks; to exercise investigatory powers; to obtain access to any premises of the controller and the processor; to exercise corrective powers, including warnings, reprimands and bans on processing; and to authorise processing when the controller faces a high risk (prior authorisation) (Article 47 GDPR).

Supervisory authorities shall impose administrative fines for infringements of the GDPR. They are basically of two kinds, depending on the gravity of the infringement: fines up to EUR 10 000 000, or in the case of an undertaking, up to two of the total worldwide annual turnovers of the preceding financial year in specific cases, and fines up to EUR 20 000 000, or in the case of an undertaking, up to 4% of the total worldwide annual turnover of the preceding financial year (for example, in the case of the violation of basic principles of processing or data subjects' rights).

While businesses may end up focusing too much on the financial penalties, it is also important to note that Article 53 of the GDPR provides DPAs with the power to order a data controller to:
• impose a temporary or indefinite ban on processing;
• suspend data flows to a recipient in a third party;
• comply with the data subject's requests;
• provide any information;
• ensure compliance with prior authorisations and prior consultations;
• warn or admonish;
• and/or order rectification, erasure or destructions.

Legal remedies under the GDPR

In light of the protection of the fundamental right to an effective remedy enshrined in Article 47 of the Charter, the GDPR envisages both administrative sanctions and judicial remedies which can be brought side-by-side. This situation may occur if the data subject considers that his or her rights under this Regulation are infringed or where the supervisory authority does not act on a complaint, partially or wholly rejects or dismisses a complaint or does not act where such action is necessary to protect the rights of the data subject.

Where a data subject alleges that there has been a breach of the GDPR which has caused the data subject damage, either material or non-material, he or she can lodge a complaint with the relevant supervisory authority within a member state and there is also a right to seek compensation from the data controller or data processor for the damage suffered.

The GDPR at Articles 77 and 78 offers two alternatives for lodging a complaint with a supervisory authority if data processing infringes the Regulation: an administrative remedy and a judicial remedy.

Article 78 distinguishes between the case of the right to an effective judicial remedy for each natural or legal person (not necessarily a data subject) against a legally-binding decision of a supervisory authority and the right to an effective judicial remedy for only data subjects who have not been informed within three months of the progress or outcome of an administrative complaint lodged pursuant to Article 77.

Every data subject should have the right to lodge a complaint with a single supervisory authority, in particular in the Member State of his or her habitual residence. The investigation following a complaint should be carried out, subject to judicial review, to the extent that is appropriate in the specific case. The supervisory authority should inform the data subject of the progress and the outcome of the complaint within a reasonable period.
Supervisory authorities should undertake relevant measures in order to foster the safeguard of Article 47 CFR.
If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

Furthermore, the GDPR ensures the effective judicial remedy against data processing which is non-compliant with the GDPR. Effective judicial remedy may be accomplished against supervisory authorities as well as controllers or processors.

As already provided also by the Data Protection Directive, under the GDPR the data subject has the right to lodge a complaint with a supervisory authority.

The data subject shall have the right to lodge a complaint with a supervisory authority in particular in the Member State of his or her habitual residence, place of work or place of the alleged infringement.

The right to an effective judicial remedy encompasses also the possibility to challenge any legally-binding decision of a supervisory authority.

For proceedings against a controller or processor in the case of unlawful processing, Article 79 GDPR enables the data subject - instead of lodging a complaint with a supervisory authority - to sue controllers or processors directly before the courts of Member States where they have an establishment or where data subjects have their habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Individual and collective action

Effective protection of fundamental rights in the field of data processing requires a convergence between individual and collective remedies as well as public oversight.
One of the most important provisions of the GDPR in this field is Article 80, which concerns both the representation of data subjects and collective action for the protection of personal data.
This provision includes two sections: the first section enables the data subject to give a mandate to non-profit organisations for exercising the remedies provided against the infringement of the GDPR; the second gives Member States the option to introduce a form of collective action based on the 'opt-out' mechanism (exercise of the right independently of the data subject's mandate).
In fact, Member States may provide for a body, organisation or association to have the right to lodge a complaint in the Member States, independently of a data subject's mandate, and the right to an effective judicial remedy where it has reasons to consider that the rights of a data subject have been infringed as a result of the processing of personal data in violation of the Regulation. That body, organisation or association may not be allowed to claim compensation on a data subject's on behalf or independently of the data subject's mandate.

An important measure has been established to avoid the same proceedings from being treated by different national authorities. Where proceedings concerning the same subject matter as regards processing by the same controller or processor are pending in the court of another Member State, any competent court other than the court first seized may suspend its proceedings.

Civil liability

Recalling Article 23, 95/46/EC Directive, Article 82 of the GDPR provides that any person who has suffered material or non-material damage as a result of an infringement of the Data Protection Regulation shall have the right to receive compensation from the controller or processor for the damages suffered arising from any infringement of the GDPR. This includes the right to receive compensation where provided by Member States. Controllers or processors have the burden of proof that they were not in any way responsible for the event giving rise to the damage.
It is highly controversial whether this provision envisages a mechanism of strict liability or is still based on the fault principle.
Article 82 GDPR also provides that joint controllers or processors are together considered jointly and severally liable for part of the compensation in case of damages. In this case, the claimant can recover the entire compensation awarded from any one of the liable parties regardless of the parties' individual shares of the liability. The party who pays the entire compensation can separately seek to recover from the other parties who are liable.

Penalties and fines

The GDPR requires Member States to provide for penalties in cases of infringements not covered by administrative fines under Article 83. Penalties should be proportionate, dissuasive and effective.
The adoption of such penalties and their amendments shall be notified by Member States to the Commission.
In any case, the imposition of criminal penalties for infringements of such national rules and of administrative penalties should not lead to a breach of the principle of *ne bis in idem*, as interpreted by the Court of Justice.

Where administrative fines are imposed on persons that are not an undertaking, the supervisory authority should take account of the general level of income in the Member State as well as the economic situation of the person in considering the appropriate amount of the fine. The consistency mechanism may also be used to promote a consistent application of administrative fines. It should be for the Member States to determine whether and to what extent public authorities should be subject to administrative fines. Imposing an administrative fine or giving a warning does not affect the application of other powers of the supervisory authorities or of other penalties under this Regulation.

Balancing data protection and other fundamental rights and interests

The right to data protection and the right to privacy are not absolute rights, as they shall be balanced with other fundamental rights and collective interests.
According to Article 52 CFR, any limitation on the exercise of the rights and freedoms enshrined in the Charter is subject to the principle of proportionality and may be made only if it is necessary and meets a general interest recognised by the Union or the need to protect the rights and freedoms of others.
For instance, the GDPR requires Member States to implement areas of derogation to the protection of personal data, in a proportionate way.

The most relevant legal areas in which the balance of interests should be carried out by taking into account conflicting interests are law enforcement, property and freedom of research.

Law enforcement vs data protection

The rules concerning law enforcement and data protection are to be sought in Law Enforcement Directive 680/2016, which applies 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, including the safeguarding against and the prevention of threats to public security (Article 1). In fact, the material scope of the GDPR under Article 2 does not include data processing for law enforcement purposes. Furthermore, matters related to national security are not addressed by the reach of the GDPR. According to recital 16, the GDPR does not apply to issues of the protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.

The constitutional balance between data protection and law enforcement may be envisaged via the judicial interaction technique with the Charter, which relies on the right to personal data regardless of the material scope of the GDPR and Law Enforcement Directive.

For further details we will refer to Casesheet No 8 of the Handbook.

Property vs data protection

Intellectual property may clash from different standpoints with the protection of personal data.

For instance, according to recital 63 GDPR, the right to access of data subjects can be limited for the protection of the rights of others, including intellectual property, trade secrets, and in particular the copyright protecting the software. Nonetheless, the most important example of conflict is represented by the contrast between Article 17 and Article 8 of the Charter, as ruled in several cases by the Court of Justice. Most of these cases dealt with the 'peer-to-peer' systems, according to which, copyright holders intended to obtain from controllers (communication providers) access to the IP number or personal data of the users suspected of unlawful downloading.

For example, in the very well-known *Promusicae* case[40] - concerning the case of a service provider that refuses to deliver personal data to the copyright holder claiming the infringement of its property rights by a huge number of users - the Court concluded that '*the Member States must, when transposing the directives mentioned above, take care to rely on an interpretation of those directives 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*' (par. 65 and 68).

Scientific research vs Data protection

The importance of collective interests involved in the exercise of the scientific research justifies in some cases the limitation of data protection rights.

Indeed, on the one hand, par. 1 of Article 89 provides for appropriate safeguards to be adopted for the rights and freedoms of the data subject when the processing is carried out for archiving purposes in the public interest, scientific or historical research purposes

On the other hand, several passages of the GDPR envisage possible derogations to data protection rules. For instance, par. 2 of Article 89 expressly lays down specific derogations that may be enacted by Member States or EU law from the rights referred to in Articles 15, 16, 18 and 21 (access, rectification, restriction and right to object) to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.

[40] CJEU, C-275/06, *Productores de Música de España (Promusicae)* v *Telefónica de España SAU* [GC], 29 January 2008.

Furthermore, Article 17 GDPR provides that the right to erasure does not apply in the case that processing is necessary for achieving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing.

In the field of specific categories of data, Article 9(g) introduces a specific derogation to the general prohibition if the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1).

Finally, Article 5(1)(b) mitigates the purpose limitation principle providing that further processing of personal data for public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’).

Part II - Selected cases

Methodological remarks

The casesheets that follow are based on the cases that have been provided by the national experts that participated in the e-NACT working group on data protection.

The selection has been made in line with the following criteria:

1. **Problem-based**: the national jurisprudence reflects in so far as possible the problems, questions, and ambiguities that national judiciary face in relation to the use of the Charter in the field of data protection.
2. **EU relevance**: the national jurisprudence identifies in so far as possible issues of EU-wide relevance, which touch upon the application (or omission of application) of the Charter in connection with the application of EU primary and secondary sources in the application of data protection.
3. **EU Charter of Fundamental Rights**: Priority is given to cases that cite the Charter of EU Fundamental rights. Additionally, cases that may have cited the Charter but omitted to do so (i.e. where the Charter was applicable) as well as the possible motives for doing or not doing so may be highlighted.
4. **EU Charter of Fundamental Rights level of protection:** particular attention is paid to national jurisprudence where the EU Charter was used to ensure a higher standard of protection of personal data compared to the protection ensured by the EU secondary legislation.
5. **Relationship between the EU Charter of Fundamental rights and the ECHR:** Has the EU Charter been used to confer more extensive protection of fundamental rights than that offered under the ECHR, or vice versa?
6. **Judicial Dialogue**: a special emphasis is placed on national jurisprudence that used one or more of the following judicial interaction techniques: preliminary reference procedure under Article 267 TFEU; direct reference to the case law of the CJEU or ECtHR; references to the jurisprudence of foreign national courts; and disapplication of national legislation implementing EU secondary legislation.
7. **Divergent positions of national judiciary**: national jurisprudence highlighting divergent positions of national courts is considered: lower level courts vs high courts/constitutional courts/other specialised national courts.
8. **CJEU case law connection**: national jurisprudence highlighting the difference or common approach to legal issues also faced by the CJEU.

Brief glossary of judicial interaction techniques

Most of the following judicial interaction techniques have been described in the context of the ACTIONES (Active Charter Training through Interaction of National Experiences) project, an EU-funded project coordinated by the EUI Centre for Judicial Cooperation, which ended on 31 October 2017[41].
Hereinafter, we will provide an overview of the most common judicial interaction techniques, which will be useful for the analysis of the case sheets dealing with data protection.
As we can see, the commonly used technique is the technique of consistent interpretation, which enhances the judicial dialogue between national courts and EU courts in a constructive way and in light of the protection of fundamental rights.
However, we also encountered cases in which dissenting opinion and vertical interaction (this only at national level) have been used.

INTERPRETATIVE TECHNIQUES

Consistent interpretation

Typically, national judges must interpret national law in compliance with their constitution. Furthermore, they are obliged to interpret domestic laws in such a manner so as not to infringe upon EU and ECHR law. This duty is the result of the principle of the primacy of EU law over national law, and of the obligation of the High Contracting Parties to ensure that the ECHR is implemented within the domestic legal order. According to the doctrine of consistent interpretation, a national judge must choose among different possible interpretations of a domestic provision that which does not lead to a conflict with EU law or the ECHR. In particular, as far as EU law is concerned, consistent interpretation is a technique through which national judges can sometimes overcome the lack of implementation of EU legislation through the domestic legislator's activism, eventually limiting the implications of the lack of horizontal effect of EU secondary law (notably, directives). In order to provide a compliant interpretation with EU law, national judges must use the instruments allowed by national law in order to achieve the purpose of an EU act.

Comparative reasoning

It can be useful to look at the approach endorsed by legislators in other States or by foreign courts in similar legal cases. This technique can offer a solution adopted by another national judge when confronted with the application of the same EU or ECHR legal provision, or when the State acts within the margin of appreciation. The national judge who wishes to engage in comparative reasoning should: 1) choose a foreign decision that may have similar facts; and 2) adapt the solution chosen in another legal context to his or her own legal order.

INTERACTION BETWEEN LEGAL PROVISIONS

[41] See the database available at http://judcoop.eui.eu/data/?p=data.

Disapplication

This technique is probably the one that implies the highest degree of interference of supranational/international law in the domestic legal orders of the Member States, as it requires national judges to set aside domestic law that conflicts with EU law, the ECHR or international law. Thus, it presupposes an assessment of incompatibility between the incompatible national provision and the relevant supranational/international law. The determined incompatibility of national law with EU-level law that could lead to disapplication of national law does not render the latter void – it merely precludes its application in that specific case.

INTERACTION BETWEEN RIGHTS (NATIONAL/EU)

Proportionality test

This technique requires national judges to appreciate whether the domestic measure interfering with supranational/international law pursues a legitimate aim, actually contributes to that aim and is the least restrictive measure that can achieve it. This technique is feasible only in relation to fundamental rights which can be balanced with other fundamental rights, and for the purpose of balancing fundamental rights guarantees against national public policies or among different fundamental rights guarantees.

INTERACTION BETWEEN COURTS

Preliminary ruling

Article 267 TFEU provides a mechanism of direct cooperation between national judges and the CJEU. It allows any national court to refer questions directly to the CJEU on the interpretation or validity of EU law. In principle, courts against whose decisions there is no domestic judicial remedy are under an obligation to refer a preliminary question whenever they have doubt on the interpretation or the validity of EU provisions, whereas other courts are under an obligation to refer only if they consider that the provision of EU law applicable to their case is not valid.

DEFERENTIAL APPROACH

Margin of appreciation

In order to preserve Member States' regulatory autonomy and constitutional identity, the ECtHR is keen to afford them some margin of discretion when implementing Convention obligations. This is particularly true with respect to fundamental rights in two hypotheses. First, when there is no European consensus as to the interpretation and application of a certain right. Second, when rights must be balanced with one another, in which case the choice of the correct balance is entrusted to the State. The doctrine of margin of appreciation implies that the application of the ECHR is not necessarily uniform across all Member States, whereas at least in principle, the application of the EU Charter of Fundamental Rights is less concerned with local peculiarities and advocates an unconditional compliance with the uniform standards of protection set therein (the CJEU in Melloni expressly states that 'the primacy, unity and effectiveness of EU law' should not be compromised by the adoption of domestic standards).

Judicial self-restraint

This is a procedural or substantive approach to the exercise of judicial review. As a procedural doctrine, the principle of restraint urges judges to refrain from ruling on specific legal issues, and especially on constitutional ones, unless the decision is necessary for the resolution of a concrete controversy. As a substantive one, it compels judges to consider constitutional questions to grant substantial deference to the views of the governed branches and invalidate their actions only when constitutional limits have clearly been violated[42].

Equivalent protection

This doctrine has been developed for ruling on the relationships between the Court of Justice of the European Union and the European Court of Human Rights. It is a horizontal interaction technique, which aims to ensure that the protection of fundamental rights by the EU law can be considered equivalent to that of the Convention system, the only exception being that this doctrine can be rebutted if the protection under the Convention is manifestly deficient (Bosphorus case).

Specifically, par. 3 of Article 52 is intended to ensure the necessary consistency between the Charter and the ECHR by establishing the rule that, in so far as the rights in the present Charter also correspond to rights guaranteed by the ECHR, the meaning and scope of those rights, including authorised limitations, are the same as those laid down by the ECHR. This means in particular that the legislator, in laying down limitations to those rights, must comply with the same standards as are fixed by the detailed limitation arrangements laid down in the ECHR, which are thus made applicable for the rights covered by this paragraph, without thereby adversely affecting the autonomy of Union law and of that of the Court of Justice of the European Union[43].

DISSENTING OPINION[44]

The progressive integration of the domestic judicial authorities within the multi-level European systems calls upon national judges to acquire the capability to manage the logic inherent to judge-made law systems, such as the EU and ECHR systems are. Civil law legal systems, particularly those more strongly inspired by the French model[45], are traditionally grounded on the cornerstone of the primacy of statutory law, according to which the *ratio legis* is the direct and binding reference of the judicial interpretation and application of the law. The *ratio legis* is by its nature logically and chronologically placed *before* the case to adjudicate. It is the reason for the norm, enshrined in the formal structure of the legal provision, and as such reflects its general and abstract nature. The thinking of the continental judge is influenced by the logical structure of the normative system he or she is called upon to interpret and apply. Consequently, the judicial reasoning traditionally presents a deductive syllogistic structure.

In contrast, the ECHR legal order is grounded on the cornerstone of the European Convention of Human Rights (along with its Protocols), which is a very short charter, and above all on the case-law elaborated by the ECtHR. The compelling force stemming from the ECHR legal system is rooted

---

[42] *See* https://www.britannica.com/topic/judicial-restraint.

[43] See Explanations relating to the Charter of Fundamental Rights, Art. 52-Scope and interpretation, Official Journal of the European Union C 303/17 - 14.12.2007, available at https://fra.europa.eu/en/charterpedia/article/52-scope-and-interpretation-rights-and-principles.

[44] This paragraph has been drafted on the basis of Mr Francesco Perrone's contribution.

[45] H. de Charles Montesquieu, *L'Esprit des Lois* (1748); English trans., The Spirit of Laws (translated by T. Nugent) (Nourse & Vaillant, 1752).

in the logic of the *ratio decidendi*, that is to say the concrete reason on which the assessment performed by the Court is grounded. The *ratio decidendi* logically and chronologically comes *after* the case to adjudicate, so that its material characteristics have a decisive weight on the reasoning of the judicial assessment. Therefore, the national judge, where called upon to decide cases falling within the scope of the ECHR, must face the need to change the usual structure of his or her reasoning: from the abstract, deductive, syllogistic approach assumed by the logic of the primacy of the statutory law, to the inductive and concrete logic of the *ratio decidendi*-oriented system. This syllogistic reasoning gives way to the distinguishing technique, which relates to two entities, both concrete: the case pending before the domestic jurisdiction and the *ratio decidendi* of a relevant precedent of the ECtHR. The *ratio decidendi* is to be searched by the interpreter not only in the reasoning of the judgment, which is the privileged structure expressing the logic of the decision but also in the concurring and dissenting opinions, which are inasmuch able to shed light on the logical thread followed by the majority.

Implementation of the GDPR at national level

As regards the implementation of the GDPR at national level, see https://iapp.org/resources/article/eu-member-state-gdpr-implementation-laws-and-drafts/.

Italy on 10 August 2018 passed the D.lgs. 101/2018, which includes provisions for the adaptation of national legislation to the GDPR[46], harmonising the Italian Privacy Code (D.Lgs. n. 196/2003) and other national laws with the European General Data Protection Regulation. The decree entered into force on 19 September 2018.
As the GDPR does not need to be implemented at national level and given the existence in Italy of legislation on data protection (Legislative Decree 196/2003, 'Privacy Code'), the Italian Parliament approved an enabling act which harmonised both legislative measures, abrogating specific legal provisions of the Legislative Decree 196/2003. Among the most relevant measures, the lowering of the age of consent to 14 years is noteworthy. As regards the processing of particular categories of data, with reference to genetic, biometric and health data, the Garante will issue, every two years, provisions on safeguard measures, aimed at identifying 'the security measures, such as cryptography and pseudonymisation procedures, minimisation measures, specific methods of selective data access and to provide information to data subjects, as well as other necessary measures to guarantee the data subjects' rights.' In some cases (see Article 5), the principle of equal rank is maintained to justify the processing of particular categories of personal data, such as sexual life, sexual orientation and health. The general authorisations for the processing of sensitive data according to the Privacy Code, in line with Article 21 of the decree, will be updated by the Garante with a provision only after a public consultation is held.
According to Articles 15-22 of the GDPR, data subjects' rights will be limited or excluded in specific cases when they conflict with other requirements imposed by national law, as in the case of the application of anti-money laundering measures, the prerogatives of the parliamentary commissions of inquiry, the processing carried out in order to defend investigation activities, or the exercise of a right in court, even in the case of whistleblowing. The same rights, if related to deceased persons and with certain limitations, may be exercised by those who have an interest of their own, or act to protect the person concerned, as a proxy, or 'for family reasons deserving protection.'
It is left to the Garante, together with Italy's communications regulator, the AGCOM, to define the rules for the inclusion of contracting parties' personal data — and the following use — in telephone directories. Regarding this, the legislator will undertake a courageous attempt to rewrite articles

[46] See the Italian text of the Legislative Decree at http://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=true;

related to Title X of the Privacy Code, including references to telemarketing, despite the pending approval of the ePrivacy Regulations, which will replace the ePrivacy Directive.
With regard to the effective judicial remedies, and in addition to lodging a complaint with the Garante, data subjects may appeal to the ordinary judicial authority. The complaint is processed within a maximum time of nine months from its submission. However, the data subject is given the opportunity to submit reports to the Garante.
Novelties have also been introduced to the internal structure of the Garante.
Criminal sanctions already introduced by the Privacy Code have been reorganised and reformulated. The new penalties will regard: unlawful data processing; illegal communication and disclosure of data processed on a large scale; untruths in the communication to the Garante and the interruption of the activities of the Italian DPA; noncompliance with the provisions of the Garante; violations of the provisions on remote controls; and surveys of workers' opinions.
Facilitated methods will be defined in relation to previous violations as well as previous pending proceedings in front of the Garante. Finally, the provisions of the Garante continue to be applied, as long as they are compatible with the GDPR and with other dispositions of the decree. Finally, as regards the administrative measures, it is important to underline that in the first eight months from the date of entry into force of the decree, the Garante will carefully pursue their application.

Ireland passed the Data Protection Act on 24 May 2018[47].

The Bill implements Ireland's national legislation in areas where the EU General Data Protection Regulation ('GDPR') provides a margin of manoeuvre to Member States, and specifies the investigative and enforcement powers of the Irish Data Protection Commission. The Bill also implements Directive 2016/680 (Law Enforcement Directive) into Irish law.

The key points of the Bill include:

- Data Protection Commission: The Bill establishes the Data Protection Commission, which replaces the current Office of the Data Protection Commissioner. The Bill permits the appointment of three Commissioners, one of which will act as Chair and have voting rights in cases of decisions to be taken by the Commission where the vote is tied.
- Children's Data: The Bill notes that for the purposes of Data Protection Regulation in Ireland, a child is a person under 18 years of age. The initial draft of the Bill specified 13 years as its implementing age of digital consent in the context of Article 8 of the GDPR. However, in the previous committee stage, the age was amended to 16 years. A review of the provision is to take place three years after it comes into operation. Furthermore, the Bill specifies that processing children's data for the purposes of direct marketing, profiling or micro-targeting is an offense punishable by administrative fines.
- Common Travel Area: The Bill provides that processing of personal data and disclosure of data for the purposes of preserving the Common Travel Area (between Ireland, the United Kingdom of Great Britain and Northern Ireland, the Channel Islands and the Isle of Man) is lawful where the controller is an airline or ship.
- Further Processing: The Bill states that processing of personal data or sensitive data for a purpose other than that for which the data was originally collected is lawful where the processing is necessary to: (1) prevent a threat to national security, defence or public security; (2) prevent, detect, investigate or prosecute criminal offenses; (3) provide or obtain legal advice or for legal claims and proceedings; or (4) establish, exercise or defend legal rights.

[47] See the text of the Data Protection Act at https://data.oireachtas.ie/ie/oireachtas/act/2018/7/eng/enacted/a0718.pdf; for the summary, see https://www.huntonprivacyblog.com/2018/05/22/irish-data-protection-bill-final-committee-stage-irish-legislature/.

- Sensitive Data: The Bill outlines circumstances additional to those of Article 9 of the GDPR where the processing of special categories of data is permitted. These include the processing of: (1) special categories of data for the purposes of providing or obtaining legal advice, for legal claims and proceedings or to establish, exercise or defend legal rights; (2) political opinion data carried out in the course of electoral activities for compiling data on peoples' political opinions by a political party or a candidate for election, or a holder of elective political office in Ireland and by the Referendum Commission in the performance of its functions; (3) special categories of data where necessary and proportionate for the administration of justice or the performance of a function conferred on a person by or under an enactment or by the Constitution; and (4) health data where necessary and proportionate for insurance, pension or property mortgaging purposes.
- Right to Access Results of Examinations and Appeals: The Bill specifically provides for a right of access to examination results, examination scripts and the results of an examination appeal.
- Enforced Access Requests: The Bill notes that a person who requests that an individual make an access request in connection with the recruitment of that individual as an employee, the continued employment of that individual or for purposes of a contract for the provision of services to the person by the individual will be guilty of an offense and subject to a fine or imprisonment.
- Right to Object to Direct Marketing: The Bill protects direct mailing carried out in the course of electoral activities, subject to certain conditions, from the right to object to direct marketing.
- Administrative Fines: The Bill specifies that where the Commission decides to impose an administrative fine on a controller or processor that is a public authority or public body, but is not a public authority or public body that acts as an undertaking within the meaning of the Competition Act 2002, the amount of the administrative fine concerned shall not exceed €1,000,000. Previous editions of the Bill exempted such public authorities and public bodies from administrative fines.
- Representative Actions: The Bill permits a data protection action to be brought on behalf of a data subject by a non-profit body, organisation or association, and the court hearing the action shall have the power to grant the data subject relief by way of injunction, declaration or compensation for the damage suffered by the plaintiff as a result of the infringement. Previous editions of the Bill did not permit recovery in the form of damages.

Portugal passed Draft Law No 120/XIII/3.ª (GOV), implementing (EU) Regulation 2016/679 (General Data Protection Regulation or GDPR) in Portugal on 14 June 2019. Law No 58/2019 of 8 August 2019, which adapts Portuguese law to the GDPR ('Portuguese Data Protection Law'), subsequently entered into force. The Portuguese Data Protection Law revoked the previous data protection law, Law No 67/98, of 26 October 1998.

Following the publication of the Portuguese Data Protection Law, the Competent National Data Protection Commission issued Resolution No 2019/494 in September 2019 ('CNPD Resolution No 2019/494') on specific parts of the Portuguese Data Protection Law because they do not comply with the GDPR: (i) aspects of the territorial scope of the Portuguese Data Protection Law; (ii) exemptions from data subjects' rights where a duty of confidence arises; (iii) processing of personal data by public entities for purposes other than those which justified the data collection; (iv) restrictions on the validity of consent provided by employees; (v) general conditions for imposing administrative fines; (vi) tying of consent to contract performance; and (vii) the annulling of existing authorisations.

Among the most relevant novelties are: the duty of secrecy for medical professionals means that the processing of health and genetic data must be conducted in secrecy; the data collected from CCTV surveillance, such as images and videos, can only be used for the security of people and goods and not for other purposes; and the CNPD stated that the processing of biometric data can only be

conducted to control the access and attendance of employees. Consent to the processing of personal data will not be lawful if the processing results in a legal or economic advantage for the employee.

In addition, Law No 59/2019 ('Law 59/2019') of 8 August 2019 on the protection of natural persons regarding the processing of personal data connected with criminal offences or the execution of criminal penalties, and on the free movement of such data, implemented the Law Enforcement Directive.

Spain passed on 5 December 2018 the Organic Law 3/2018, which repealed the Organic Law 15/1999, except for several articles relating to the processing of personal data by the police and judiciary until a law adopts 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 offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. This Law adapts the Spanish legal system to the General Data Protection Regulation and further provides specifications for or restrictions of its rules, as explained in the GDPR. In this sense, the law states that the fundamental right to data protection of natural persons, under Article 18.4 of the Spanish Constitution, shall be exercised under the GDPR and this law. Second, the law guarantees the digital rights of citizens and employees, beyond the GDPR. For example, the law includes provisions on the right to internet access, the right to digital education, the right to correction and the right to digital disconnection in the workplace.
As regards data subjects' rights, Article 12.1 of the law states that a data subject's rights may be exercised personally or through a legal or voluntary representative. Furthermore, Article 12.3 of the law provides that the processor may attend, on behalf of the controller, any request for the exercise of a data subject's rights when provided in the contract or other legal instrument that binds them.

With regard to the right of access and taking into consideration Article 12(5) of the GDPR, the law specifies that requests from a data subject are excessive because of their repetitive character when submitted 'more than once during a period of six months, unless there is a legitimate reason.'

Article 15.2 of the law also specifies that: 'When the suppression derives from the exercise of the right of opposition in accordance with Article 21(2) GDPR, the controller may keep the necessary identification data of the affected person in order to prevent future processing for direct marketing purposes.'

As regards children's rights to personal data, Article 12.6 of the law extends to 'any other rights' including digital rights guaranteed in the law, even beyond data protection, the rights provided by Article 8 GDPR.

Finally, in the field of labour law, the new Organic Law places much emphasis on the protection of privacy and digital rights in the workplace[48].

Romania has passed Law 190/2018 on measures to implement the regulations of the European Parliament and Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, repealing EU Directive 95/46, but the text is available only in Romanian and no official English translation is provided.

[48] See https://iapp.org/news/a/spains-new-data-protection-law-more-than-just-gdpr-implementation/.

Casesheets

Right to be forgotten
Casesheet no 1 – Spain, Audiencia Nacional (National High Court), ROJ 2433/2017, ordinary, 11 May 2017
Casesheet no 2 – Spain, Tribunal Supremo (Supreme Court), Contentious-Administrative Chamber, ROJ 2836/2016, 20 June 2016
Casesheet no 3 – Spain, Tribunal Constitucional, Constitutional Court, no 58/2018, constitutional, 4 June 2018
Casesheet 4 – Italy, Court of Cassation (Terza Sezione Civile, Ordinanza 26 June – 5 November 2018 no 28084)

Casesheet no 1[49] – Spain, Audiencia Nacional (National High Court), ROJ 2433/2017, ordinary, 11 May 2017

Link to the full text:
http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=8095052&links=&optimize=20170713&publicinterface=true

ECLI: ES:AN:2017:2433

Core issues
What is the definition of the 'right to be forgotten' adopted at EU level? According to which criteria could the elimination of data be justified?

[49] This casesheet has been drafted on the basis of the template provided by Joan Solanes Mullor.

At a glance

Country	Area	Reference to EU law	Legal and/or judicial body	Judicial InteractionTechnique
•Spain	•. Right to be forgotten	Directive 95/46/EC Arts. 7 and 8 CFR	National High Court	Preliminary ruling Consistent interpretation

Case(s) description

a. Facts

In 1998, *La Vanguardia* newspaper of Spain published two articles concerning an attachment and garnishment action against Costeja González. In 2009, González contacted the newspaper, asserting that when his name was entered in a search on google.com, there was still a reference to the pages of the newspaper concerning the legal action. González argued that the information should be removed because the proceedings were concluded years earlier and there was no outstanding claim against him. The newspaper, however, denied his demand, claiming that the legal action was published pursuant to an order by Spain's Ministry of Labour and Social Affairs. Then, in 2010, he contacted Google Spain, arguing that the online search results of his name should not make reference to the newspaper's publication of his legal proceedings. Upon Google's failure to comply, González brought a complaint before Spain's Data Protection Agency against the newspaper, Google Spain, and Google Inc. The Agency dismissed the action against the newspaper, reasoning that the publication was made pursuant to a government order. But it upheld the complaint against Google and its subsidiary, Google Spain. The AEPD 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. Google Spain and Google Inc. brought two actions before the Audiencia Nacional (National High Court, Spain), claiming that the AEPD's decision should be annulled. It is in this context that the Spanish court referred a series of questions to the Court of Justice.

The National High Court of Spain presented the following questions to the European Court of Justice for a preliminary ruling: (1) whether the EU Directive 95/46 as implemented through the national legislation of a Member State can be applied to a foreign Internet search engine company that has a branch or subsidiary with the intent to promote and sell advertising space geared towards the inhabitants of that Member State; (2) whether the Internet search engines' act of locating information published by third parties, and later indexing and making the information available to Internet users can be considered as 'processing of personal data' within the meaning of the Directive; (3) whether the operator of a search engine must be regarded as a 'controller' with respect to the processing of personal data under Article 2(d) of the Directive; (4) whether on the basis of legitimate grounds to protect the right to privacy and other fundamental rights envisioned by the Directive, operators of Internet search engines are obligated to remove or erase personal information published by third party websites, even when the initial dissemination of such information was lawful. Article 1 of Directive 95/46 obligated EU States to protect 'the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.' At the same time, it prohibits restrictions on the free flow of personal data between the EU members. The Directive defined personal data as 'any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.' The act of processing such information includes 'any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.' Under Article 2(d), a 'controller' of personal data is any 'natural or legal person, public authority, agency or any other body, which alone or jointly with others determines the purposes and means of the processing of personal data.'

b. Reasoning of the Court

The National High Court had to decide on 230 cases regarding claims by individuals against Google Inc. and Google Spain SL for not erasing personal data which was accessible to the public through its search engine. The National High Court selected one of those cases and asked the CJEU about the interpretation of 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 and Articles 7 and 8 of the Charter.

The case selected by the National High Court involved the request of an individual to delete the information published in 1998 in the newspaper La Vanguardia in which his name appeared for a real estate auction connected with proceedings for the recovery of social security debts. At the same time, this information from the newspaper was available to the public on the internet through the search engine of Google Inc. and Google Spain SL. The Spanish National Agency for Data Protection issued an administrative resolution ordering Google Inc. and Google Spain SL to eliminate the personal data requested and excluding the newspaper's liability.

The decision of the CJEU in *Google Spain* has attracted wide attention. Three findings of the decision of the CJEU should be highlighted. First, the CJEU interpreted Articles 2(b) and 2(d) of Directive 95/46/EC and concluded 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' within the meaning of Article 2(b) when that information contains personal data and, second, the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of Article 2(d). Second, the activity of 'processing of personal data' should be considered as being carried out in the territory of a Member State, in this case, in Spain. Third, a case-by-case analysis of the rights and interests in conflict is warranted: on the one hand, the rights of Articles 7 and 8 of the Charter and, on the other the right of the public to access information. This analysis should be performed case-by-case, taking into account the nature of the personal data in question and the interests of the public in having access to this information.

The National High Court, following the decision of the CJEU in *Google Spain*, first established a general approach to all cases and, after that, resolved the particular case at bar. In relation to the general approach, the National High Court stated: (1) the individual (data subject) seeking to eliminate personal data must file a complaint before the 'controller' of the information or the Spanish National Agency for Data Protection, showing the links and results connected to this personal data, as well as the nature and content of this personal data; (2) in the context of this complaint, the 'controller' or the Spanish National Agency for Data Protection must balance the rights in conflict - the right to personal data and right to access to information - taking into account the specific situation of the individual (case-by-case analysis of the rights in conflict); (3) the elimination of the data will be justified, *inter alia*, in light of the nature of the information, the sensitivity to the private life of the individual, the irrelevance of the data for the aims alleged for the processing, or the time elapsed.

The National High Court applied this general approach to the case at bar and annulled the decision of the Spanish National Agency for Data Protection. This Court understood that the right to access to information prevails over the right to personal data. The applicant was a surgeon widely known in the scientific arena. He had a public profile and his services were advertised on the website. The opinions published on the internet forum in 2008 were related to his professional background and performance and not to his personal life. Finally, the opinions were expressed in a critical way, but

not through insults or degrading terms. For all these reasons, the information was sensitive and of public interest and should remain accessible to the public.

c. Impact on national cases

After the decision of the CJEU in *Google Spain* and its implementation by the National High Court in the first 18 cases, Google Spain SL and Google Inc. decided to withdraw from 130 judicial cases. Google Spain SL and Google Inc. decided instead to maintain active in approximately 80 cases. The alliance of the CJEU and the National High Court has resulted in the voluntary reduction of cases: it has had a clear deterrence effect, reinforcing the National High Court position. The decisions of the National High Court in the other pending cases vary in light of the result of the balancing test. In some of them the result is in favour of the right to personal data, in others the right to access to information is predominant. There are also cases in which the National High Court declares that the applicant has not identified accurately the information qualified as personal data and, therefore, the balancing test cannot be performed. However, all the decisions consistently apply the general approach established by the National High Court following the decision of the CJEU.

Analysis

a. Role of the Charter

The debate, both at the national level and before the CJEU, was whether the case fell within the scope of application of 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. The territorial application of the Directive and the concept of 'processing personal data' were the key for the application of Directive 95/46/EC. The National High Court, through the preliminary reference, helped the CJEU in order to clarify these two relevant issues. After the CJEU declared that Directive 95/46/EC was applicable, the Charter also became relevant for solving the issue. The Directive was interpreted by the CJEU in light of Articles 7 and 8 of the Charter, being the Charter determinant for the final outcome of the CJEU decision and, at the end, for the National High Court.

b. Judicial dialogue

b.1. Vertical interaction

The National High Court solved the case by applying the technique of consistent interpretation. Previously, the National High Court had sent a preliminary reference to the CJEU in the first group of cases in which the applicants pursued the elimination of personal data from Google's search engine. After the decision of the CJEU in *Google Spain*, the National High Court regularly decides on all the issues applying the CJEU's framework. Therefore, the National High Court is not sending more preliminary references because the CJEU's framework adopted after the *Google Spain* case clarified the scope of application and the meaning of the Directive 95/46/EC in light of the Charter. The National High Court automatically applies the CJEU's framework, designed in the case *Google Spain*[50].

[50] Hereinafter we recall the facts of another case from the 230 cases. This case deals with the request of an individual to delete the information published in 2008 in an internet forum. The applicant at that time was a surgeon specialised in the spinal column. In the internet forum, a former patient explained their experience with the applicant. The opinions of the former patient explained, in critical terms, a bad experience with the applicant. The opinions were related to the treatment and the professional experience of the applicant, without tackling aspects of the personal aspects of the applicant and without using insults or other degrading terms. The applicant requested from Google Inc. and Google Spain SL the removal of this information in 2014. Google Inc. and Google Spain SL denied

FOCUS

Judgment of the Court (Grand Chamber), 13 May 2014, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, C-131/12 (Google Spain)

Link to the full text:
http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6550595
ECLI:EU:C: 2014: 317

Although not expressly referring to Article 47 of the Charter, the Court relies on the principle of effectiveness to underline that given the objective of ensuring an effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, the words carried out in the context of the activities' of an establishment cannot be interpreted restrictively. The Court states that it is clear from the EU legislation on data protection that the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented by prescribing a particularly broad territorial scope.

As regards the Directive's territorial scope, the Court observes that Google Spain is a subsidiary of Google Inc. on Spanish territory and, therefore, an 'establishment' within the meaning of the directive. The Court rejects the argument that the processing of personal data by Google Search is not carried out in the context of the activities of that establishment in Spain. The Court holds, in this regard, that where such data are processed for the purposes of a search engine operated by an undertaking which, although it has its seat in a non-Member State, has an establishment in a Member State, the processing is carried out 'in the context of the activities' of that establishment, within the meaning of the directive, if the establishment is intended to promote and sell, in the Member State in question, advertising space offered by the search engine in order to make the service offered by the search engine profitable.

So far as concerns, next, the extent of the responsibility of the operator of the search engine, the Court holds that the operator is, in certain circumstances, obliged to remove links to web pages that are published by third parties and contain information relating to a person from the list of results displayed following a search made on the basis of that person's name. The Court makes it clear that such an obligation may also exist in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful.

Consequently, the Court decides that the processing of data is carried out 'in the context of the activities' of an establishment in a Member State even if it is 'only' intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable, given that 'the activities of the operator of the search engine and those of its establishment situated in the Member State concerned 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'. The fact that the display of results is accompanied, on the same page, by the display of

the request. The Spanish National Agency for Data Protection issued an administrative resolution ordering Google Inc. and Google Spain SL to eliminate the personal data requested.

advertising linked to the search terms, proves that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory.

The Court concludes that in such circumstances, it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the Directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the Directive seeks to ensure, in particular their right to privacy, with respect to the processing of personal data, a right to which the Directive accords special importance. On the question related to the localisation of the 'use of equipment, automated or otherwise', the Court takes the view that since the protection is applicable as a result of the answer given to Question 1(a), there is no need to answer the question.

b.2. Horizontal dialogue (European) – Consistent interpretation

There was a potential link between Articles 7 and 8 of the Charter and Article 8 of the ECHR and the ECrtHR case law developing it. However, neither the National High Court nor the CJEU in *Google Spain* refers to the ECHR and the case law of the ECtHR.

Casesheet no 2[51] – Spain, Tribunal Supremo (Supreme Court), Contentious-Administrative Chamber, ROJ 2836/2016, 20 June 2016

Link to the full text:
http://www.poderjudicial.es/search/contenidos.action?action=contentpdf&databasematch=TS&reference=7719109&links=&optimize=20160624&publicinterface=true

ECLI:ES:TS:2016:2836

Core issues
What should the recipient do to have his or her data cancelled? According to which criteria could the elimination of data be justified?

At a glance

Country	Area	Reference to EU law	Legal and/or judicial body	Judicial InteractionTechnique
•Spain	•. Right to be forgotten	Directive 95/46/EC Arts. 7 and 8 CFR	Supreme court	Consistent interpretation

Case(s) description

a. The facts

The case involved the request of an individual to delete the information published in 2010 in the Spanish Official Gazette (BOE), which was indexed in the Google search engine. This information declared the loss of the condition of civil servant because of a criminal conviction. The applicant requested of Google Spain SL the removal of this information. The Spanish National Agency for Data Protection issued an administrative resolution ordering Google Inc. and Google Spain SL to eliminate the personal data requested.

b. Reasoning of the Court

The Spanish Supreme Court declared in the case at bar that Google Spain SL is not responsible for the treatment of the data and, therefore, the requests to supress the data should be sent to Google Inc. (located in the US) and not Google Spain SL (which is only an intermediate without responsibility). The substantive outcomes of the CJEU decision and the follow-ups decisions of the National High Court remain untouched (the criteria to suppress the data and the proportionality test have not change). The only change is that the recipient against the individual has to send his/her request for suppression.

The Spanish Supreme Court argues that the CJEU in *Google Spain* only stated that Google Spain SL was a subsidiary of Google Inc. and this condition was enough for the territorial application of Directive 95/46/EC (having Google Inc. a permanent 'establishment' in the territory of the EU). Google Spain SL was necessary for the purposes of triggering the scope of application of the Directive. However, for the Spanish Supreme Court, the CJEU decision made clear that the only party

[51] This Casesheet has been drafted on the basis of the template provided by Joan Solanes Mullor.

responsible for the treatment of the personal data was Google Inc. Google Spain SL only was a commercial brand (or commercial establishment) of Google Inc. which was the only party responsible in determining the objectives and methods of processing the personal data. Thus, for the Spanish Supreme Court, Google Spain SL cannot be considered 'responsible' for the processing of personal data because it does not participate in the determination of the objectives, aims and methods for processing such data. This is only a responsibility of Google Inc.

c. Impact on national cases

Following the decision of the National High Court, however, the Spanish Supreme Court (Contentious-Administrative Chamber) declared that Google Spain SL is not responsible for the treatment of the data and, therefore, the requests to supress the data should be sent to Google Inc. (located in the US) and not Google Spain SL (which is only an intermediate without responsibility). See, for instance, the Spanish Supreme Court judgment (Contentious-Administrative Chamber) no 574/2016, of 14 March 2016, ECLI:ES:TS:2016:964. However, the substantive outcomes of the CJEU decision and the follow-up decisions of the National High Court remain untouched (the criteria to suppress the data and the proportionality test have not change). The only change is that the recipient against the individual must send his/her request for suppression. On the contrary, the Spanish Supreme Court (Civil Chamber) has also recently decided that, when action for damages is launched, Google Spain SL is responsible. See the Spanish Supreme Court judgment (Civil Chamber) nº 210/2016, 5 April 2016, ECLI:ES:TS:2016:1280. In short, depending on the course of action, the private individual will have to follow different paths: (1) in the case that the goal is to request the suppression of the data, the request must be sent to the Spanish National Agency for Data Protection or to Google Inc. (not Google Spain SL); and (2) in the case of a civil action for damages, the action can be pursued directly against Google Spain SL.

In this regard, another judicial line has been opened: claims for damages for the non-elimination of personal data by the search engines. For the first time, the Provincial Court of Barcelona has sanctioned Google Spain SL for damages (8,000 EUR in favour of the applicant) because the search engine did not eliminate personal data when a decision issued by the Spanish National Agency of Data Protection ordered to proceed with that elimination (Provincial Court of Barcelona, 364/2014, judgment of 17 July). As a consequence of the recognition of the search engines as 'controllers' and that they are in charge of balancing the rights in conflict case-by-case, the search engines are liable for damages in case they do not comply with their duties. Recently, the Spanish Supreme Court has ratified the compensation for damages in this case (see the Spanish Supreme Court judgment (Civil Chamber) nº 210/2016, 5 April 2016, ECLI:ES:TS:2016:1280).

Analysis

a. Role of the Charter

The debate, both at the national level and before the CJEU, was whether the case falls within the scope of application of 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. The territorial application of the Directive and the concept of 'processing personal data' were key to the application of Directive 95/46/EC. The National High Court, through the preliminary reference, helped the CJEU to clarify these two relevant issues. After the CJEU declared that Directive 95/46/EC was applicable, the Charter also became relevant for resolving the issue. The Directive was interpreted by the CJEU in light of Articles 7 and 8 of the Charter, being the Charter determinant for the final outcome of the CJEU decision and, at the end, for national courts.

b. Judicial dialogue

b.1. Vertical interaction

The Supreme Court solved the case by applying the technique of consistent interpretation. Previously, the National High Court had sent a preliminary reference to the CJEU in the first group of cases in which the applicants pursued the elimination of personal data from Google's search engine. After the decision of the CJEU in *Google Spain*, the National High Court decides regularly on all the issues that apply the CJEU's framework. Therefore, the National High Court no longer sends more preliminary references because the CJEU's framework adopted after the *Google Spain* case clarified the scope of application and the meaning of the Directive 95/46/EC in light of the Charter. The National High Court is automatically applying the CJEU's framework designed in the case *Google Spain*.

In the case of the Spanish Supreme Court, the Court dealt extensively with the findings of the CJEU in *Google Spain* and decided that there was no need to send a preliminary reference regarding the question whether Google Spain SL is 'responsible' for processing personal data in accordance with Directive 95/46/EC. The Supreme Court considers that the CJEU decision in *Google Spain* is clear regarding this point: the findings of the CJEU point out that only Google Inc. is responsible for processing the personal data. Google Inc. is in charge of the search engine and its operation, not Google Spain SL. Google Spain SL is only relevant for the territorial application of EU law, but any finding of the CJEU leads to the conclusion that it should be deemed as 'responsible' or 'co-responsible' for processing the personal data. Therefore, the CJEU decision being clear on that point, the Supreme Court interprets national law as in consistence with the findings of the CJEU decision in *Google Spain*.

b.2. Horizontal dialogue (European)

There was a potential link between Articles 7 and 8 of the Charter and Article 8 of the ECHR and the ECtHR case law developing it. However, neither the National High Court nor the CJEU in *Google Spain* refers to the ECHR and the case law of the ECtHR.

Casesheet no 3[52] – Spain, Tribunal Constitucional, Constitutional Court, no 58/2018, constitutional, 4 June 2018

Link to the full text:
http://hj.tribunalconstitucional.es/en/Resolucion/Show/25683

ECLI:ES:TC:2018:58

Core issues
Can the right to privacy encompass the right to informational self-determination?

At a glance

Case(s) description

1. *Facts*

In the 1980s, the print edition of the *El Pais* newspaper published the criminal proceedings against a drug-related criminal organisation. The newspaper story explained the composition of the criminal organisation, the police intervention and finally the criminal proceedings that followed and the relevant convictions. The story identified by their forenames and surnames the people involved in the criminal organisation.

In 2007, *El Pais* provided free online access to its digital archives. Consequently, the above-mentioned story was available online. Through a search on a general search engine (such as *Google*) and the internal search engine of *El Pais*, the story was easily accessible by using as a search criterion the forenames and surnames of the people mentioned in the story.
The applicants in 2011 decided to start judicial proceedings against *El Pais* alleging that the story being available online and easy to find with a search for their forenames and surnames was a violation of their right to privacy and personal data. They sought the de-indexation of the story in the digital archives of *El Pais* from all search engines and the suppression of their forenames and surnames from the story (anonymisation of the story of the newspaper). The First Instance Court (*Audiencia Provincial*) decided in favour of the applicants and obliged *El Pais* to, first, de-index the story from both general search engines and the internal search engine of the newspaper and, second, to anonymise the story. The second instance court (*Tribunal Supremo*) partially revoked the decision of the First Instance Court and decided that *El Pais* was only obliged to de-index the story from general search engines, but not from the internal search engine while anonymisation was not necessary. Finally, the applicants filed an individual constitutional complaint before the Spanish Constitutional Court.

2. *Reasoning of the Court*

[52] This Casesheet has been drafted on the basis of the template provided by Joan Solanes Mullor.

The Spanish Constitutional Court partially upheld the decisions of the inferior courts. It decided to de-index the story from the general search engines and from the internal search engine. It did not make anonymisation of the story obligatory.
The Spanish Constitutional Court expressly referred to the 'right to be forgotten' as a constitutional right. Article 18.4 of the Spanish Constitution establishes the right to personal data which includes the right to control your personal data, especially in the context of computing and the internet. This was the first time that the Constitutional Court referred to this specific right and, in doing so, recognised it at the constitutional level as a fundamental right enshrined in article 18.4.

Once the 'right to be forgotten' was recognised as a fundamental right, the Constitutional Court balanced the same with freedom of information (Article 20 of the Spanish Constitution). The story published by *El Pais* was only a description of facts and events, without expressing opinions, therefore freedom of expression was not applicable. Under the framework of freedom of information, the Constitutional Court applied the classic canon in the field. The story published must be verified and noticeable (of general interest). There was no debate about the trustworthiness of the story and the Constitutional Court focused on the noticeability of the story. There was no doubt for the Constitutional Court that in the 1980s the story published was of general interest for the public (drug trafficking and criminal proceedings), but the time that had elapsed (more than 20 years) eroded the noticeability of the story. The story seriously affected the reputation and privacy of the applicants – there were no public figures involved – by revealing their involvement in past crimes and their convictions. But the criminal record of the applicants was archived and the story did not show any new event connected to the past. The personal data available to the public was no longer relevant from the point of view of the interest of informing the public. However, the Constitutional Court recalled that the information could still be relevant from the point of view of scientific, historical or cultural research. In this context, the digital archives of newspapers are relevant in a democratic society and should be protected. By making past events available to the public, digital archives preserve knowledge and disseminate it to the public.

Considering all these criteria, in the case at bar the Constitutional Court analysed the measures taken by the ordinary courts. Regarding the de-indexation of general search engines, the Constitutional Court maintained the decisions of the first and second instances and did not address the issue by itself. Both *Audiencia Provincial* and *Tribunal Supremo* agreed on the de-indexation because it was very prejudicial for the applicants and, therefore, the balance between freedom of information and privacy was broken. Regarding the de-indexation from the internal search engine, the *Audiencia Provincial* ordered also the de-indexation, but not the *Tribunal Supremo*. The Constitutional Court agreed with *Audiencia Provincial* and quashed the decision of the *Tribunal Supremo*. For the Constitutional Court, digital archives should be protected, but the possibility was enough of searching for the story through thematic or other search criteria. For preserving the integrity of the digital archive, it was not necessary to maintain the indexation of the forenames and surnames of the applicants. Therefore, the Constitutional Court ordered the de-indexation of the forenames and surnames of the applicants and consequently the general public could not search in the digital archive by texting the forenames and surnames of the applicants. Finally, the Constitutional Court did not, following the lead of the *Tribunal Supremo*, make anonymisation of the story obligatory. For the Constitutional Court, anonymisation is a more intrusive measure against freedom of information. The de-indexation from the internal search engine already reduces the impact on the privacy of the applicants and it is enough to correctly balance between privacy and freedom of information

Impact on national cases
The Spanish Constitutional Court uses the ECJ and ECtHR case law for reinforcing its own argumentation under national constitutional law. The Constitutional Court develops a new constitutional right - the right to control personal data - by interpreting Article 18.4 of the Spanish

Constitution. In the development of this new constitutional right and, therefore, in reshaping the meaning of the constitution, the ECJ case law is crucial and is used by the Constitutional Court. The new development by the Constitutional Court is supported in the ECJ case law.
At the same time, the balance between freedom of information and privacy is reshaped thanks to ECJ and ECtHR case law. The time that has elapsed between the publication of the newspaper story and the time when an individual desires to terminate its impact on his or her private life now weighs in the balance (the time elapsed can reduce the relevance for the general interest). This development is taken into account directly from the *Google Spain* case. At the same time, the level of protection for newspaper digital archives is understood in accordance with the ECtHR case law (especially the *Times Newspaper* case).
The Spanish Constitutional Court wanted to be aligned with the case law of the ECJ and the ECtHR. The aim of the Spanish Constitutional Court was to reinforce its own case law on freedom of information and privacy and to support new case law developments.

Analysis

a. Role of the Charter

The ECJ judgment in the *Google Spain* case is determinant to the inclusion of the right to be forgotten (or the right to control your personal data) in Article 18.4 of the Spanish Constitution. The Spanish Constitutional Court refers explicitly to the case and directly quotes Articles 7 and 8 of the Charter. The Constitutional Court for the first time recognises the right to be forgotten as a constitutional right and this step is done through their own reasoning and the evolution of its own case law. However, the Constitutional Court refers to the *Google Spain* case and the Charter as a determinant factor to support its own argumentation under national constitutional law.

b. Judicial dialogue

b.1. Vertical interaction

The Spanish Constitutional Court extensively referred to and quoted the ECJ judgment on *Google Spain*. It aims for recognition at the constitutional level of the right to be forgotten and the reference to the ECJ case law is key here. The constitutional development is done through references to the ECJ judgment in *Google Spain*. It is an example of 'interiorising' EU law. At the end, the Constitutional Court interprets article 18.4 Spanish Constitution in light of the ECJ case law and this operation is done explicitly and adequately by quoting it.

Moreover, the Spanish Constitutional Court extensively referred to and quoted the ECtHR case law on freedom of information and privacy. The national balancing test incorporates the level of protection of the digital archives of newspapers as developed by the ECtHR. The Constitutional Court extensively refers to the *Times Newspaper* case and the national constitutional balance test is adapted to the insights of the ECtHR case law. Again, this case is a good example of a correct understanding of the ECtHR case law by the Spanish Constitutional Court. The national constitutional test is still a national test but includes the insights and the considerations of the Strasbourg court's case law.

b.2. Horizontal dialogue (European)

The ECHR and the Strasburg court's case law weigh the balance between freedom of information and the right to privacy. The balance is done by the Constitutional Court under national constitutional law, but Strasbourg case law is used to add new insights into the balancing. In short, Strasbourg case law is used to give an appropriate weight to the protection of newspaper digital archives. The *Times Newspapers* case becomes crucial (ECtHR judgment of 10 March 2009, *Times Newspaper Ltd* (no 1

and 2) v *United Kingdom*). In this case, the ECtHR recognises the value of newspaper digital archives but, at the same time, qualifies it as a secondary function of the press. The Constitutional Court introduces this level of protection of digital archives in the balancing and concludes that digital archives deserve protection but, in the end, this protection can be diminished in favour of the right to privacy because digital archives are secondary in press functions. Therefore, the balancing operation concluded that de-indexation of digital archives from general and internal search engines is a perfect measure for protecting privacy without compromising the integrity of the digital archives. However, anonymisation is a very intrusive tool and will compromise the integrity of digital archives, which deserves protection.

Casesheet no 4 – Italy, Court of Cassation (Terza Sezione Civile, Ordinanza 26 giugno – 5 novembre 2018 no 28084)

Link to the full text:

Core issues
Are the criteria mentioned by Article 17 GDPR that justify the right to erasure alternative or concurrent?

At a glance

Country	Area	Reference to EU law	Legal and/or judicial body	Judicial Interaction Techniques
•Italy	•Right to erasure	Art. 17 GDPR Arts. 7 and 8 CFR	• Supreme Court	•Consistent interpretation

Case(s) description

a. Facts

Twenty-seven years after the incident, the newspaper Unione Sarda in 2009 republished the details of a homicide case for which the convicted person had already served his sentence of 12 years imprisonment. This person thus complained to the Court of Cagliari for moral damages and damage to property, as well as to his image and reputation as a result of the new negative media coverage to which he had been exposed.

Cited jointly for compensation, the newspaper Unione Sarda and the journalist reacted and contested the claim by virtue of the fact that the article in question was part of a weekly column dedicated to the most important events that had occurred in Cagliari in the last 30-40 years and the republishing of the fact was of public interest. Both the Court of Cagliari and the Court of Appeals in the second instance rejected the applicant's request.

The person appealed to the Supreme Court against the sentence, denouncing the violation and misapplication of Article 2 of the Constitution, specifically for the part the Court of merit considered incompatible with Article 21 of the Constitution, which prevails always over individual rights - guaranteed by Article 2 - including the right to be forgotten. Furthermore, he maintained that the historical material fact of republication (accompanied by a photograph and a complete indication of its details) of an article that had already been published back in 1982 is profoundly detrimental to the rights, as guaranteed by the aforementioned article of the Italian constitutional charter.

b. Reasoning of the Court

The Court then proceeded with the analysis of the legal and jurisprudential framework of the internal and supranational order in the matter of balancing the right to inform individuals (placed at the service of the public interest in information) and the right to be forgotten (set forth to protect the privacy of the person).

The information right, according to the unanimous teaching of the jurisprudence of Cassazione, is a subjective public right, to be understood in the broader rights context concerning the free expression of thought and the press. However, it cannot be considered as without limits.

The Supreme Court resumed judgment no 5259 of 18/10/1984 of the First Section, in which it was affirmed that the right to news 'is legitimate when the following three conditions are involved:
a) the social utility of information;
b) the truth (objective or even just putative, provided it is the result of serious and diligent research work) of the facts presented;
c) the way of presenting facts and their assessment, not exceeding the information purpose to be achieved, is marked by objectivity at least in the sense of excluding prejudice and bias and, in any case, respectful of that minimum of dignity to which the most reprehensible of people are always entitled, so that the most human feelings can never be allowed to be trivial or derisory'.

Furthermore, as early as 1998, the Supreme Court explicitly recognised the right to be forgotten, describing it as '*... the right interest of every person not to remain undeterminably exposed to further damage that is caused by the repeated publication of his honour and reputation of a previously legitimately disclosed information*' (Section 3, Sentence No 3679 of 09/04/1998). In this ruling, the Court ruled that '*it has been specified that, for the legitimate exercise of the right of news, the existence of the requirement of the public interest regarding the fact narrated is not sufficient, but the news of the news is also necessary*'.

The Court then recalled the recent guidelines for the delicate balancing between the right to report and the right to be forgotten, expressed in March 2018 by the First Section of Cassation (see Ordinance No 6919 of 20/03/2018), which in order are:

a) the contribution made by republication to a debate in the public interest of the actual and current interest in the dissemination of the image or the news,

b) the high degree of notoriety of the subject represented, due to the particular position they hold in the public life of the country,

c) the methods used to obtain and give information (true, disseminated in a manner not exceeding the information purpose and free from insinuations or personal considerations),

d) the prior information about the publication in order to allow the interested party the right to reply.

This list, according to the Court, is not very clear and could lead to an excessive closure of cases in which the righ to be forgotten prevails, leading it to be effectively ineffective. In fact, the Court did not specify if these assumptions were requested by way of being concurrent or alternative: if one were to opt for cumulation, the right to be forgotten would rarely prevail over the right to report.

The presented regulatory framework has also been enriched by the new European regulation on personal data, which illustrates in which cases it is possible to request the exercise of the right to be forgotten.

The Court concludes by stating that the importance of balancing the relationship between the right to news, information or the manifestation of thought and the right to be forgotten makes the identification of unequivocal reference criteria 'indifferent', and therefore puts the issue back to the United Sections: 'We therefore refer the case to the First President of the Court for the possible assignment to the United Sections of the question of particular importance, concerning the balancing of the right of news - placed at the service of the public interest in information - and of the so-called

right to be forgotten - placed to protect personal privacy - in the light of the legal and jurisprudential framework in the internal and supranational legal systems'.[53]

Analysis

a. Role of the Charter

Even though the Charter has not been recalled directly by the Court in this judgment, it is striking how the right to be forgotten is considered a constitutional right to be balanced with other constitutional rights.
In the reasoning of the Court, the balance between the right to report and the right to be forgotten affects the way in which democracy is understood in our current civil society, which, on the one hand makes the pluralism of information and its critical knowledge a fundamental pillar, while, on the other it cannot ignore the protection of the personality of the individual human person in its various expressions. It seems to the Court, starting only from the concrete case, it is possible to define: when a public interest can actually be configured to the knowledge of facts (such as insinuations of doubts and uncontrolled voices); when, in spite of the time passed by the facts, this interest can be considered current; which terms, on the existence of said interest, can affect the gravity and the criminal relevance of the fact; the completeness (or incompleteness) of the news of the fact; the purpose of processing the data (if, for example, for research purposes scientific or historical, for statistical purposes, for information purposes or for other reasons, for example marketing purposes); the notoriety (or lack of notoriety) of the person concerned; and the clarity of the expository form used (also avoiding the unification and the combination of false news and true news).

b. Judicial interaction
b.1. Vertical dialogue – Consistent interpretation

The judgment expressly quotes Article 17 GDPR and the particular circumstances under which the right to be forgotten can be exercised. The referral to Sezioni Unite of the Court of Cassation aims to assess whether the criteria prescribed by Article 17 GDPR may occur jointly or separately.

FOCUS – Article 17 GDPR

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws the consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

[53] For the follow-up to the Google Spain case in Italy, see *Re-Jus Casebook. Effective Justice in Data Protection*, 2015, at 145.

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

1. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

2. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

    (a) for exercising the right of freedom of expression and information;
    (b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
    (c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
    (d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
    (e) for the establishment, exercise or defence of legal claims.

Data retention

Casesheet no 5 – Portugal, Tribunal Constitucional (Constitutional Court) - Case 333/2018, 27 June 2018

Casesheet no 6 – Portugal, Tribunal Constitucional (Constitutional Court) - Case 403/2015, 27 August 2015

Casesheet no 7 – Romania, Curtea Constituțională a României (Romanian Constitutional Court), 424 D/2014 & 478/D/2014, 8 July 2014

Casesheet no 8 – Ireland, *Graham Dwyer* v *Data Commissioner*, The High Court, No 351/2015, 6 December 2018

Casesheet no 5[54] – Portugal, Tribunal Constitucional (Constitutional Court) - Case 333/2018, 27 June 2018

Link to the full text:
http://www.tribunalconstitucional.pt/tc/acordaos/20180333.html

Core issues
Is the collection of data from a DNA database lawful processing?

At a glance

Case(s) description

a. *Facts*

The plaintiff has argued that the provision pursuant to Article 8 (3) of the Profile DNA Database Act violates the CPR.

The abovementioned provision determines that a DNA sample can be collected from a convicted criminal by police authorities, following a judicial decision. However, this can only happen if the following conditions occur: (*i*) commission of a criminal offense out of malice and not out of negligence and (*ii*) sentence of imprisonment for at least three years.

The court must decide if the sample collection under the abovementioned circumstances can be regarded as an adequate, necessary and proportionate measure.

b. *Reasoning of the Court*

The court starts by giving an account of the jurisprudential and normative framework.

As far as the normative framework is concerned, the court highlights the purpose pursued by the DNA Profile Database Act. It is mentioned that the creation of a DNA database has improved the chances of identifying the person responsible for the commission of a criminal offence. However, the efficacy of such a tool depends on the number of samples collected. Additionally, the court notes that the right

[54] This casesheet has been drafted on the basis of the template provided by Afonso Brás and Sara Azevedo

to information is guaranteed before the sample collection, according to Article 10(1) of the Personal Data Protection Act and Article 13 of the GDPR.
Regarding the jurisprudential framework, the court considers the case law produced by the European Court of Human Rights. Among other statements, the referred Court has consistently prohibited a general and indiscriminate power of DNA data retention. Moreover, according to the European Court of Human Rights, one must ensure a fair balance between the public interest in the retention of DNA data and the restricted fundamental rights.
Clearly influenced by the abovementioned case law, the Court concludes that the DNA Profile Database Act does not entail a general and indiscriminate power of DNA data retention.
Concerning the fair balance between the competing interests, the court concludes that the purposes pursued by this measure (achievement of justice and discovery of truth) have constitutional dignity. The court highlights that the creation of a DNA database reduces the number of unresolved criminal investigations, allowing the identification of both perpetrators and innocents.
Moreover, the court underscores that the DNA database has the sole purpose of identifying the author of future crimes. Therefore, the sample taken only collects the necessary data for identification, leaving aside health or hereditary information.
Finally, the court explains that Article 30(4) of the CPR does not forbid punishments that entail the loss of civil rights. The referred article only prohibits the loss of civil rights as an automatic result of a conviction, without a judge's intervention. Bearing in mind such a provision, the Court clarifies that the sample collection requires a judicial authorisation and that this measure was not created to function as an additional sanction.
In conclusion, from the Court's point of view, even though some fundamental rights were restricted, the creation of a DNA profile database was an adequate, necessary and proportionate measure.

c. Impact on national cases

As mentioned before, there was no interaction between the national court and the CJEU. However, the DNA Profile Database Act was amended during the trial [Law No 90/2017 of 22 August].
According to the first version of Article 8(2), the sample collection could only be authorised by the judge after the final judgment.
According to the current version, the authorisation ought to be given with the conviction.
However, as stated in the Court's decision, this amendment aimed to improve the database's efficacy, considering that the initial results fell short of expectations.
The Court offers a consistent interpretation between the DNA Profile Database Act and the case law produced by the European Court of Human Rights.
Bearing in mind that the creation of the DNA database entailed a restriction of some fundamental rights, the Court evaluates if that decision can be regarded as an adequate, necessary and proportionate measure. For this proportionality judgment, and using a comparative reasoning, the court pays special attention to the referred case law. The court performs a consistent interpretation of the Profile DNA Database Act with the case law produced by the European Court of Human Rights.
Bearing in mind that the creation of the DNA database entailed a restriction of some fundamental rights, the Court evaluates if that decision can be regarded as an adequate, necessary and proportionate measure. For this proportionality judgment, and using a comparative reasoning, the Court pays special attention to the referred case law.

Analysis

a. Role of the Charter

Even though the case bears a relationship with Article 8 of the Charter, this article is not mentioned in the Court's decision. Unfortunately, this is a quite common phenomenon: despite mentioning and applying EU sources such as Directive 95/46/EC and Article 10 of Regulation (EU) 2016/679, the

court completely overlooks he Charter. Nevertheless, the Court mentions Article 8 of the European Convention on Human Rights.

b. Judicial dialogue

b.1. Vertical interaction

As mentioned above, the Criminal Court of Sintra, the Central Court of Lisbon and the Supreme Court of Justice ruled against the plaintiff of this claim. The Constitutional Court also ruled against the plaintiff, considering the norm in analysis lawful. The Court cites the following judgments from the European Court of Human Rights:

- Judgment *Van der Velden* v *the Netherlands* (case no 29514/05), 7 December 2006;
- Judgment *S. and Marper* v *the United Kingdom* (case no 30562/04 and 30566/04), 4 December 2008;
- Judgment *Rotaru* v *Romania* (case no 28341/95), 4 May 2000;
- Judgment *Peruzzo and Martens* v *German* (case no 7841/08 and 57900/12), 4 June 2013.
- Judgment *Aycaguer* v *France* (case no 8806/12), 22 June 2017.

b.2. Horizontal interaction (among MS)

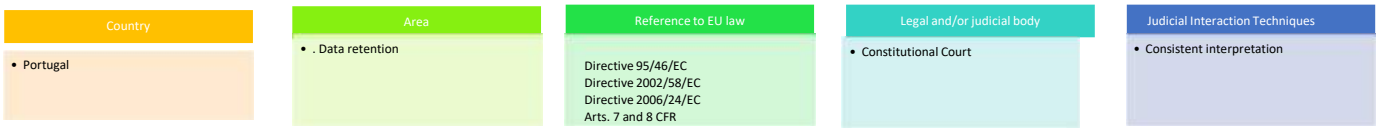
Even though the Court does not quote any other national judgments, it mentions that countries such as England, Scotland, Austria, France and Germany have already worked on a DNA profile database. The Court mentions previous decisions about the same subject: collecting a DNA sample from a convicted criminal to obtain a genetic profile [Constitutional Court, Judgments no 155/2007 (2 March 2007) and 228/2007 (28 March 2007)]. In those cases, the Court declared the relevant provisions unconstitutional. However, the provisions in question permitted the collection of a DNA sample without judicial authorisation and even if the convicted criminal had expressly refused to do so.
Additionally, the Court mentions the Council Resolution of June 2001 (2001/C 187/01) and the Council Resolution of 9 June 1997 (97/C 193/02), both on the exchange of DNA analysis results.

Casesheet no 6[55] – Portugal, Tribunal Constitucional (Constitutional Court) - Case 403/2015, 27 August 2015

Link to the full text:
http://www.tribunalconstitucional.pt/tc/acordaos/20150403.html

Core issues
Should the access to metadata be qualified as an interference in correspondence through telecommunications?

At a glance



Case(s) description

a. Facts

The Portuguese Parliament enacted the Intelligence System Act in August 2015. The decree was sent to the President of the Republic of Portugal on 6 August 2015, who asked for an anticipatory constitutional review. According to the CPR, the President of the Republic of Portugal has the right to ask for an anticipatory constitutional review. The President decided to exercise the mentioned right, expressing his doubts about the constitutionality of the decree. From the President's point of view, two questions ought to be answered: first, one needs to know if the access to metadata should be qualified as an interference in the correspondence through telecommunications; second, one needs to assess whether the authorisation of the Prior Control Commission is equivalent to a criminal procedure.

According to the aforementioned decree, following an authorisation of the Prior Control Commission, the Intelligence Services of the Portuguese Republic can have access to metadata such as traffic data and other data connected with communications.

b. Reasoning of the Court

The Court starts by presenting three categories of personal data: the basic data; the content data; and the traffic data. According to the Court, the decree analysis covers only the last category, which can be defined as any data processed for the purpose of using an electronic communications network, including data relating to the routing, duration or time of a communication.

Subsequently, the Court describes the applicable international legal framework. Considering the normative framework, the Court highlights Article 12 of the Universal Declaration of Human Rights, Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the EU Charter. Regarding the jurisprudential framework, the Court briefly quotes the abovementioned CJEU case law. Moreover, the Court also mentions the case *Malone* v *United Kingdom* (Judgment of the European Court of Human Rights, app. no 8691/79, 2 August 1984).

According to the Court, the processing of personal data related to communications defies the fundamental rights of the people involved. Even if there is no access to the content of that

[55] This Casesheet has been drafted on the basis of the template provided by Afonso Brás and Sara Azevedo

communication, processing traffic data is enough to gather personal information (with whom a person talks most, his or her favourite locations, his or her schedules, etc.).
Therefore, from the Court's perspective, the norm extracted from Article 34(4) of the CPR is a natural result of having the right to protection of private and family life and the right to protection of personal data, enshrined in Article 26 of the CPR.
Having said that, the Court concludes that electronic communications must have the same level of protection as that granted to communications in person.
The right to communicative self-determination, enshrined in Article 34(4) of the CPR, is also highlighted by the Court. This right comprehends both a negative and a positive dimension. The former means that the State must refrain from abuses; the latter entails positive actions such as an obligation to enact legislation to protect citizens as far as the protection of personal data in communications is concerned.
The Court recognises that, besides content data, traffic data are also included in the aforementioned right. Therefore, the Court must determine whether the right to communicative self-determination was violated by this decree.
Article 34(4) includes a prohibitive provision (*The interference of public authorities in the correspondence through telecommunications as well as other means of communication shall be forbidden*) and a permissive provision (*except when foreseen in the law and only in the criminal procedure domain*), the former being the ordinary rule and the latter being the exception.
The lawfulness of this measure depends on whether it falls under the ordinary rule or the exception. Were this measure to fall under the exception it would be seen as lawful. In contrast, falling under the rule entails a necessary unconstitutionality. Therefore, one needs to analyse if the procedure that results in the authorisation of the Prior Control Commission is equivalent to a criminal procedure.
The Court defines criminal procedure as an ordinated sequence of acts carried out by legitimate organs and aiming to provide a decision about a potential criminal offense and its legal consequences. The criminal procedure provides the minimum guarantees to criminal defendants and demands the intervention of a judge.
The Court concludes that it is not possible to endorse a broad interpretation of the aforementioned exception. Consequently, considering the following statements, it is clear that the procedure prescribed by the decree cannot be qualified as a criminal procedure:
First, the traffic data are not collected for the purposes of an ongoing criminal investigation. In fact, the information is given to the Intelligence Service of the Republic of Portugal and not to the Criminal Police Bodies. However, only the latter are responsible for gathering evidence.
Second, the authorisation enacted by the Prior Control Commission does not solve the problem. In fact, the Prior Control Commission is an administrative body and, according to the CPR, the criminal procedure belongs exclusively to the courts. Therefore, the CPR prohibits the existence of prior administrative procedures.
Third, the decree under analysis does not provide the necessary guarantees to the data subject. Indeed, the decree does not clarify in which circumstances the commission has the power to authorise access to personal data. Moreover, nothing is said about the duration of the authorisation or about the need to erase the data after a period of time.
Considering this topic, the Court mentions the case law of the European Court of Human Rights and also two judgments from Spain and Germany. Bearing in mind those decisions, the court concludes that the law ought to employ sufficiently clear terms, as well as determine under which specific cases the access to personal data may occur. The law should also define the duration of the measure and the rules and deadlines for erasing the data.
The Court points out that even Law no 32/2008 of 17 July 2008 (which transposed Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006) presents a greater level of protection as far as data protection is concerned.
In conclusion, the Court states that the right to self-determination in electronic communications was violated by the decree under analysis. However, it was not a unanimous decision: two judges

expressed their opposition. One of the judges agreed with the decision but did not endorse the reasoning. The other judge voted against the entire decision.

c. Impact on national legislation

Following the declaration of unconstitutionality, which was influenced by the CJEU case *Digital Rights Ireland Ltd*, the Portuguese Parliament was forced to enact another Intelligence System Act, which only occurred in 2017 (Law no 4/2017, 25 August).

Analysis

a. Role of the Charter

The national Court used judicial interaction techniques for the purposes of legitimacy. Knowing that the CJEU, the European Court of Human Rights and other Member States had relevant case law on this matter, the court aimed to understand if the national solution followed the previous decisions of those courts.

b. Judicial dialogue

b.1. Vertical interaction

The Court provides a consistent interpretation between the decree and the case law produced by the Court of Justice of the European Union and the European Court of Human Rights. Articles 7 and 8 of the Charter and Article 8 of the European Convention on Human Rights are both cited by the Court when describing the applicable international legal framework.

Additionally, the Court uses a comparative reasoning when quoting judgments from the courts of other member states.

The Court mentions the following judgments from the CJEU:

- Judgment *Roquette Frèrres*, 22 October 2002, Case C-94/00;
- Judgment *Volkerund Markus Schecke*, 9 November 2010, Case C-92/09 and C-93/09;
- Judgment *Digital Rights Ireland Ltd*., 8 April 2014, Case C-293/12 and C-594/12.

The Court cites the following judgments from the European Court of Human Rights:

- Judgment *Malone* v *United Kingdom* (case 8691/79), 2 August 1984;
- Judgment *Segerstedt-Wiberg and others* v *Sweden* (case no 62332/2000), 6 June 2006.
- Judgment *Amann* v *Switzerland* (case no 27798/95), 16 February 2000;
- Judgment *Valenzuela* v *Spain* (case no 27671/95), 30 July 1998;
- Judgment *Prado Bugallo* v *Spain* (case no 58496/00), 18 February 2003.

b.2. Horizontal dialogue (European) – Consistent interpretation

The Court cites the following previous decisions:

- Judgment no 241/2002 (29 May 2002);
- Judgment no 486/2009 (28 September 2008);
- Judgment no 306/2003 (25 June 2003);
- Judgment no 368/2002 (25 September 2002);
- Judgment no 355/97 (7 May 1997);
- Judgment no 442/07 (14 August 2007);
- Judgment no 230/08 (21 April 2008).

Furthermore, when analysing the Portuguese doctrine, the Court also briefly mentions a judgment of the German Federal Constitutional Court, 2 March 2006 (cited in Bruscamente no verão passado – A Reforma do Código de Processo Penal*, Revista de Legislação e Jurisprudência,* Ano 137.º, julho-agosto 2008).
Additionally, the Court mentions the opinions of the Consultative Council of the Attorney General's Office (no 16/94, 26 October 1995 and no 21/200, 16 June 2000) and opinion no 29/98 (16 April 1998) of the National Data Protection Commission.
When analysing the definition of 'criminal procedure', the court briefly mentions judgments from other Member States (Judgments no 49/99, 5 April, and no 184/2003, 23 October, of the Spanish Constitutional Court and Judgment of the 1st Senate of the German Constitutional Court, 24 April 2013).

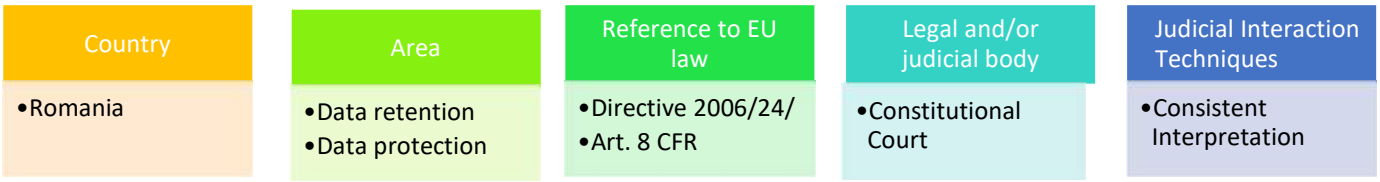
Casesheet no 7[56] *– Romania, Curtea Constituțională a României (Romanian Constitutional Court), 424 D/2014 & 478/D/2014, 8 july 2014*

Link to the full text:
https://www.ccr.ro/files/products/Decizia44020141.pdf

Core issues
To what extent is the interference of public authorities in private life proportionate?

[56] This Casesheet has been drafted on the basis of the template provided by Sergiu Popovici.

At a glance



Case(s) description

a. *Facts*

The unconstitutionality exception arose in two criminal cases before the Judecătoria (the common local court) Constanța and Judecătoria Târgoviște, both courts raising the exception of unconstitutionality *ex officio*, in cases where the prosecutors requested the release of data retained by electronic communications service providers. The two courts hesitated to grant the prosecutors' request, arguing that Law 82/2012 and Article 152 of the RCrPC were unconstitutional, following the invalidation of Directive 2006/24/EC by the CJEU.

b. *Reasoning of the Court*

The Public Ministry (the authority under which prosecutors are organised) argued that despite the invalidation of Directive 2006/24/EC by the CJEU, the national implementing law was still constitutional, essentially stating that the national authority's interference with the right to private life was proportional.

In its reasoning, the RCC had little margin of interpretation.

Firstly, the RCC itself had already declared that Law no 298/2008, the first implementation in Romania of Directive 2006/24/EC, had been unconstitutional, by Decision no 1258 of 8 October 2009. References to this former decision contain the only mention of the jurisprudence of the ECtHR, namely two decisions, *Prince Hans-Adam II of Lichtenstein* v *Germany* and *Klass and others* v *Germany*.

Comparing the first Romanian implementation of Directive 2006/24/EC with Law 82/2012, the Court found that while complementary data had been better defined, several situations may be identified where national authorities could request the retained data without any judicial review, and found that the system of administrative and criminal sanctions established by the new law was not sufficient to provide guarantees against interferences with the right to private life and freedom of expression of the persons involved.

Secondly, as the Romanian implementation of Directive 2006/24/EC was largely identical to the Directive itself, the Court's finding concerning the compatibility of Law 82/2012 with the rights to private life, personal data protection and freedom of expression represents a summary of the CJEU's motivation in joint cases C-293/12 and C-594/12, the Court expressly recognising the direct and compulsory effect of the CJEU's decision.

Finally, the Court found that Article 152 RCrPC was constitutional, since release of retained data was conditioned by prior approval from a judicial authority, and therefore provided sufficient guarantees concerning interferences with the rights to private life, to personal data protection and to freedom of expression. Although constitutional, the Court showed that the text had remained without object following the invalidation of Law 82/2012, on which it relied for application.

In light of these arguments, the RCC found that Law 82/2012 was unconstitutional in its entirety and Article 152 RCrPC, while constitutional, became inapplicable.

c. *Impact on national cases*

Pursuant to Law no 47/1992 on the functioning of the RCC, normative provisions declared unconstitutional shall have no effect after the publication of the RCC's decision in the Official Monitor. Effectively, Law 82/2012 was repealed by the analysed decision. Moreover, despite Article 152 of the RCrPC being found constitutional, as it had Law 82/2012 as its starting point, following publication of the analysed decision the text remained objectless.
Following the immediate impact mentioned above, Law no 235/2015 for the amendment of Law 506/2004 was adopted, establishing the conditions under which the competent authorities may require stored identification data from providers of electronic communication services. Since the stated purpose of the law was not to replace Law 82/2012 or to establish obligations for the service providers to retain data, it was decided that not all requirements of the analysed decision needed to be met by the new law.
The issue with Article 152 RCrPC was still left unsolved, since the text was reliant on the special law regulating the service providers' obligation to retain data, a special law which Law 235/2015 was not, by its own declaration. The remaining issue was finally resolved by Law no 75/2016, which amended Article 152 RCrPC in such a way as to make it self-reliant, thus rendering Article 12^1 of Law 506/2004, introduced by Law 235/2015, almost irrelevant.
The interim period where Law 235/2015 was in force, before the amendment of Article 152 RCrPC by Law 75/2016, generated a lot of inconsistent jurisprudence by the national courts, some granting prosecutors' requests to disclose retained data based on Article 152 RCrPC and reliant on Article 12^1 of Law 506/2004, while some others found that the requirements imposed by the analysed decision were not met by the new law, and therefore denied such requests. The matter reached the Romanian High Court of Cassation and Justice (HCCJ), seized with a request for a decision in the interest of the law, aimed at harmonising national jurisprudence, compulsory to all national courts. By the time of the HCCJ's Decision 15 of 26 September 2016, published in the Official Monitor no 892 of 8 November 2016, however, Article 152 of the RCrPC had already been amended, which led the Court to stating that the issue was no longer current, so a decision in the interest of the law was not necessary.
The new Article 12^1 of Law 506/2004, introduced by Law 235/2015, was also contested in front of the RCC. By its Decision No 589 of 21 September 2017, published in the Official Monitor No 89 of 30 January 2018, the RCC re-evaluated all of the criteria raised by the analysed decision, and found that Law 235/2015 was constitutional.

Analysis

a. Role of the Charter

The Charter was invoked, *inter alia*, as grounds for the review of the constitutionality of several national provisions concerning the retention of data generated or processed in connection with the provision of electronic communication services.

b. Judicial dialogue

b.1. Vertical interaction

The main technique employed by the RCC in the analysed decision is *consistent interpretation*. The Court expressly stated the necessity to conform with the jurisprudence of the CJEU invalidating Directive 2006/24/EC, as well as with a prior RCC decision, no 1258 of 8 October 2009, by which the same Court had declared that Law no 298/2008, the first implementation in Romania of Directive 2006/24/EC, had been unconstitutional.
Implicitly, the court also uses *comparative reasoning* in order to assess whether the motivations it previously gave and those of the CJEU are also applicable in the case at hand. Comparative reasoning is also used when assessing the case in comparison with similar situations raised in other Member States.

Proportionality is used in the same manner as that of the CJEU's decision invalidating Directive 2006/24/EC.
The RCC acknowledges that insofar as the facts are similar, the CJEU's findings in the decision invalidating Directive 2006/24/EC apply *mutatis mutandis* to the case.
Internal vertical interaction is also found, inherent to all constitutionality reviews by the RCC: the national courts, if in doubt whether a Romanian normative act is compatible with the Constitution, forward a question to the RCC, the only court enabled to interpret the Constitution and its incompatibilities with other normative acts.

b.2. Horizontal dialogue (European)

The issue is not discussed, although the substantial content of freedom of expression and the right to private life are, in their essence, the same in Articles 11 and 7 CFREU as in Articles 10 and 8 of the ECHR. The Court mainly relied on the CJEU's motivation in joint cases C-293/12 and C-594/12, with only marginal reference to the jurisprudence of the ECtHR
The RCC made references to similar decisions taken by the German Federal Constitutional Court, by the Czech Constitutional Court and by the Bulgarian Supreme Administrative Court.

Casesheet no 8 – Ireland, Graham Dwyer* v *Data Commissioner, The High Court, no 351/2015, 6 December 2018

Link to the full text:
http://www.courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/ad470420aa70fcb78025835b003902f8?OpenDocument

At a glance

Case(s) description

a. Facts

On 27 March 2015, Mr Graham Dwyer was convicted by a jury of the murder of Ms Elaine O'Hara, for which he received a life sentence on 25 April 2015. The investigation leading to the trial used the mobile telephony data generated by the phone provided by the Plaintiff's employer to the Plaintiff. This data was retained and accessed under the 2011 Act.

Dwyer claimed that data gathered from his phone, under the 2011 Communications (Retention of Data) Act, should not have been used at his 2015 trial before the Central Criminal Court.

The data, which was generated by Dwyer's work phone, placed the phone at a specific place at a particular time. That data was used to link Dwyer to another mobile phone the prosecution says Dwyer acquired and used to contact Ms O'Hara.

Mr Dwyer claimed that Section 3(1) of the 2011 Act contravened Article 15(1) of the 2002 Directive read in light of Articles 7, 8, 11 and 52 of the Charter and Articles 8 and 10 of the ECHR, in so far as it permits the retention of telephony data in a manner which is general and indiscriminate.
This part of the claim is in addition to the plea that provisions of the 2011 Act are repugnant to the Constitution having regard to the duty of the State under Article 40.3.1˚ (to vindicate personal rights), 40.3.2˚ (protect from unjust attack) and 40.6.1˚ (liberty to exercise right of expression).

The State had argued that the laws that allow the authorities to access and utilise retained data are important in the detection, prevention and investigation of serious crime, including cybercrime, organised crime gangs, murder and terrorism. The Irish High Court has ruled that Irish law on the retention of telecommunications data contravenes EU law and the European Convention on Human Rights.

b. Reasoning of the Court

The Court said this ruling does not mean telephone data accessed and retained contrary to EU law used by the prosecution in Dwyer's trial will lead to the quashing of his murder conviction. Stressing the primacy of European law, it found that sections of Ireland's retention laws contravene EU law and the findings of the European Court of Human Rights. He said the European Court had found the fighting of serious crime cannot justify the general and indiscriminate retention regime.

The Court remarked that the State should tread carefully when trenching upon the dignity and privacy of the human person in the sphere of telephony data retention and access.

Analysis

a. Role of the Charter

Recalling *Digital Rights Ireland*[57], which declared invalid the Directive of 2006 on data retention, the Court held that the obligation on service providers to retain data for the purpose of making it accessible to the competent national authorities did raise questions under Articles 7 and 8.

The 2006 Directive laid down the obligations on service providers to retain certain data which was generated or processed by them and to ensure that that data was available for the purpose of investigation, detection and prosecution of serious crime, as defined by each Member State in national law.

In that respect, the ECJ noted that the data to be retained:

'*make it possible, in particular, to know the identity of the person with whom a subscriber or registered user has communicated and by what means, 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.*

'*Those data, taken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them*' (par. 26-27).

Referring to Article 52(1) of the Charter, the ECJ explained that any limitation on rights had to be provided for by law and respect the essence of those rights. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or meet the need to protect the rights and freedoms of others. The ECJ held that the interference did satisfy an objective of general interest: the material objective of the Directive was to contribute to the fight against serious crime and ultimately to public security.

The ECJ next considered the proportionality of the interference. The principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate objectives pursued and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives. The ECJ held that in this case, in view of the important role played by the protection of personal data in light of the right to respect for private life and the extent and seriousness of the interference with that right, the EU legislature's discretion was reduced. Having regard to the question of appropriateness, the ECJ acknowledged that the retention of data is a valuable tool in criminal investigations and must be considered appropriate for attaining the objective of the Directive. Under the necessity criterion, the ECJ held that the fight against serious crime is of the utmost importance in order to ensure public security and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, the ECJ found that even this fundamental objective of general interest could not justify the retention measure established by the 2006 Directive.
For these reasons, the ECJ concluded that the 2006 Directive did not lay down clear and precise rules governing the extent of the interference with the fundamental rights provided in Articles 7 and 8 of the Charter. Thus, the interference was not circumscribed by provisions to ensure that it was limited

[57] *Digital Rights Ireland Ltd (C-293/12)* v *Minister for Communications and Others*, (Joined Cases C-293/12 and C-594/12, 8 April 2014, ECLI:EU:C:2014:238.

to what was strictly necessary. The ECJ also found that the 2006 Directive did not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data. The lack of a requirement that the data must be retained within the EU was also critical. In those circumstances, the ECJ found that the EU exceeded the principle of proportionality in light of Articles 7, 8 and 52(1) of the Charter by adopting the 2006 Directive and the Directive was declared invalid.

After *Digital Rights Ireland*, another most important case followed, *Tele 2 Sverige*[58], which has been taken into account in the reasoning of the Court.

In particular, as regards the first case, *Tele 2 Sverige*, situated in the context of the compliance of the Directive 2002/58 with the Charter, confirmed *Digital Rights*, pointing out the obligation of Nation States for not '*adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary*' (par. 108). '*National legislation is precluded, for the purpose of fighting crime, from the general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication*' (par. 112). '*Furthermore, 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, has to be precluded when it 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*' (par. 125).

b. Judicial dialogue

b.1. Vertical interaction

The Court recalls the ECJ case law standpoints:

a) Legislative measures must be subject to adequate safeguards. Thus, they must lay down clear and precise rules indicating in which circumstances and under which conditions the providers of electronic communications services must grant the competent national authorities access to the data. Such measures need to be legally binding. To ensure that the access is limited to what is strictly necessary, national legislation must also lay down the substantive and procedural conditions governing access by the competent national authorities to the retained data.
b) General access to all retained data, regardless of whether there is even an indirect link with the intended purpose, cannot be regarded as limited to what is strictly necessary. Therefore, the national legislation must be based on objective criteria in order to define the circumstances and conditions under which the competent national authorities are to be granted access to the data. Access can only be granted to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime. Access to the data of other persons may also be justified where there is objective evidence that the data might, in a specific case, make an effective contribution to combating

[58] *Tele 2 Sverige AB* v *Post- och telestyrelsen, and Secretary of State for the Home Department*, Joined Cases C-203/15 and C-698/15,21 December 2016, ECLI:EU:C:2016:970.

such activities.

c) It is essential that access should as a general rule, except in cases of validly established emergency, be subject to prior review carried out either by a court or by an independent administrative body.
d) A person whose data has been accessed must be notified as soon as that notification is no longer liable to jeopardise any investigations. That notification is necessary to enable the persons affected to exercise, *inter alia*, their right to a legal remedy.
e) National legislation must make provision for the data to be retained within the EU and for the irreversible destruction of the data at the end of the data retention period. Member States are required also to ensure review by an independent authority of compliance with the level of protection guaranteed by EU law.

The Court also recalls chronologically the main steps of the European courts. The ECtHR in *Big Brother Watch and others* v *the UK* (App. Nos. 58170/13, 62322/14 & 24960/15, ECtHR 13th September, 2018) (**'*Big Brother Watch*'**) found a violation of Article 8 of the ECHR because, among other considerations, the impugned legislation had been acknowledged by the UK as violating fundamental rights in EU law. Briefly, the UK concession that the legislation was not limited to 'serious crime' and that access to retained data did not have to undergo 'a prior review by a Court or an administrative body' meant that the legislation was not in accordance with EU law and ultimately with UK law.
Afterwards, the ECJ accepted a referral made under Article 267 TFEU from the Cour constitutionelle (Belgium) (*Ordre des barreaux francophones et germanophone & Others (Case C-520/18)*) which arose from an action to annul a 2016 law repealing 2013 laws that transposed the invalid 2006 Directive. The Defendants in their cover note lodged with this Court on 12 October 2018 highlighted that the Belgian Court asked whether legislation is precluded where the object is to comply with the positive obligation under Articles 4 and 8 of the Charter, which require effective investigation and punishment of child sex offences.

The Court also quoted the case *Ministerio Fiscal* and *Ministerio Fiscal* [59] delivered on 2 October 2018 by the ECJ (a preliminary reference from the Spanish courts seeking clarification on the interpretation of 'serious crime' in *Tele2*). This case involved access to retained data to identify the owners of SIM cards activated with stolen mobile telephones. The ECJ found that national legislation did not require that access be limited to the objective of fighting 'serious crime' where the interference itself is not serious, affirming that the interference that access to such data entails is therefore capable of being justified by the objective, to which the first sentence of Article 15(1) of Directive 2002/58 refers, of preventing, investigating, detecting and prosecuting 'criminal offences' generally, without it being necessary that those offences be defined as 'serious' (par. 62). Therefore, the access of public authorities to data for the purpose of identifying the owners of SIM cards activated with a stolen mobile telephone, such as the surnames, forenames and, if need be, addresses of the owners, entails interference with their fundamental rights, enshrined in those articles of the Charter, which is not sufficiently serious to entail that access being limited, in the area of the prevention, investigation, detection and prosecution of criminal offences, to the objective of fighting serious crime (par. 63).

On the same day, the ECJ accepted a reference from the Conseil d'État (France) (*Quadrature du Net & Others (Joined Cases C-511/18 and C-512/18*) which included the question of particular relevance, according to the Defendant's note lodged with this Court on 12 October 2018, as to whether a '*general*

[59] *Ministerio Fiscal*, Case C-207/16, 2 October 2018, ECLI:EU:C:2018:788.

and indiscriminate obligation' may be justified by reference to the right to security guaranteed in Article 6 of the Charter and the requirements of national security which is the sole responsibility of the State under Article 4 TFEU.

b.2. Constitutional aspects and EU law

The Court held that '*the requirements of the Charter to the Constitution*' is ill founded because '*the Irish Superior Courts have exclusive jurisdiction to define the scope and limits of the rights protected under the Constitution which have been guaranteed over many decades long before the Charter was proclaimed or given legal effect*'. Further, '*the logic that informed the ECJ analysis does not necessarily apply in precisely the same way to constitutional analysis*'.

b.3. Horizontal interaction (European)

It is noteworthy, as was pointed out by the Court, that it would be preferable to address EU law first followed by and combined with the ECHR law on access to 'retained data'.
The reason for selecting ECHR law in that order is that the ECHR law enhances the embryonic-like status of EU law for access to data. The Court noted in this regard Article 52(3) of the Charter:
'*In so far as this Charter contains rights which correspond to rights guaranteed by the ECHR, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.*'

Casesheet no 9 – Portugal, Tribunal Central Administrativo do Sul (Central Administrative Court of the South) - 2937/16.6BELSB

Casesheet no 9[60] – Portugal, Tribunal Central Administrativo do Sul (Central Administrative Court of the South) - 2937/16.6BELSB

Link to the full text:

http://www.dgsi.pt/jtca.nsf/170589492546a7fb802575c3004c6d7d/f10b04d65e9975b28025812300515d9e?OpenDocument

Core issues
Whether an interested party in an insolvency proceeding, by requesting information on the procedure without concealing the identity of the candidates, calls into question the protection of the candidates' personal data.

At a glance

Country	Area	Reference to EU law	Legal and/or judicial body	Judicial Interaction Techniques
•Portugal	•Right to access •Data protection	•Art. 8 CFR	•Administrative Court	•Consistent interpretation

Case(s) description

1. *Facts*

Aida, a Portuguese citizen, participated in a public competition with the Director of the Human Resources Management and Training services of the Directorate-General for School Administration, under the supervision of the Portuguese Ministry of Education.
Not having succeeded in this competition, she asked the Ministry of Education to consult the proceedings, in order to see what the profiles of the other candidates were and which specific competencies they had for the position.
The Ministry of Education denied access to these documents, and Aida brought the case to court. The lower court denied Aida's claim, with the justification that full consultation of the tender procedure is only permitted without revealing the identity of the candidates.
Not accepting this decision, Aida appealed to the Central Administrative Court of the South.

2. *Reasoning of the Court*

First, the Court briefly describes the appealed decision.
After this, the Court defines the concept of 'personal data' and of 'processing personal data'. The Court concludes that the plaintiff's claim entails access to personal data (the candidates' names).
According to Article 6 of the Portuguese Data Protection Act, personal data may lawfully be processed on grounds of the legitimate interests of a third party. Therefore, Aida had to prove that she had a legitimate interest. As mentioned in the appealed decision, Aida simply asked for all the

[60] This Casesheet has been drafted on the basis of the template provided by Afonso Brás and Sara Azevedo.

information concerning the tender procedure, without presenting a justification. Nevertheless, in the request for the appeal she stated that the identity of the other candidates was necessary to fully exercise her right to appeal against the final decision of the tender procedure.
The court ruled in favour of the plaintiff, considering that the right to appeal against the tender procedure could only be effectively exercised if the candidates' names were provided.

Analysis

a. Role of the Charter

There is a relationship between the case and the Charter. The Court makes use of the Portuguese Data Protection Act (Law no 67/98) in order to know what personal data means, the processing of personal data and what a third party is for the purpose of data protection.
In order to know what 'personal data' means, the Court considers Article 8 of the Charter, in particular the doctrine about it that exists, in order to demarcate the correct meaning of that concept.
At the same time, the Court uses the Opinion issued by the European Union Data Protection Working Group, in relation to Directive 95/46/EC, in order to further clarify the meaning of personal data.
We can therefore say that there is a direct relation between this decision and the CFR and that the meaning of 'personal data' reached by the Court is consistent with that of the CFR.

b. Judicial dialogue

b.1. Vertical interaction

The Court only considers the decision of the lower court. The Administrative Court of the Circle of Lisbon decided against the plaintiff, arguing that the access to the names of other candidates could only have been provided if Aida had justified the legitimate character of her interest. As mentioned above, Aida appealed to the Central Administrative Court of the South, stating that she needed the identity of the other candidates to fully exercise her right to appeal against the final decision of the tender procedure.

b.2. Horizontal dialogue (European)

There is an indirect relation with the ECHR. In fact, when the Court, in order to understand when we can know that information contains personal data, cites the Handbook on Data Protection Legislation produced by the European Union Agency for Fundamental Rights and the Council of Europe, and quotes, at the same time, the ECHR.
The Court thus concludes that both types of information are protected in the same way by European data protection legislation. The ECtHR has repeatedly stated that the concept of 'personal data' is the same in the ECHR.

Lawfulness of processing

Casesheet no 10 – Romania, Curtea de Appel Cluj, (Court of Appeal Cluj), 740/33/2013, *Smaranda Bara and Others* v *Casa Națională de Asigurări de Sănătate and Others*, appellate, 14 December 2015

Casesheet no 11 –Romania, Înalta Curte de Casație și Justiție (High Court of Cassation and Justice), Case no 3306/1/2015, Decision no 37 of 7 December 2015

Casesheet no 10[61] – Romania, Curtea de Appel Cluj, (Court of Appeal Cluj), 740/33/2013, Smaranda Bara and Others v *Casa Națională de Asigurări de Sănătate and Others, appellate, 14.12.2015*

Link to the full text:
http://portal.just.ro/33/SitePages/Dosar.aspx?iddosar=3300000000059933&idinst=33
EU:C:2015:638

Core issues
Whether EU law precluded a public administrative body from transferring personal data to another public administrative body for the purpose of their subsequent processing, without the data subjects being informed of that transfer and processing.

At a glance

Country	Area	Reference to EU law	Legal and/or judicial body	Judicial Interaction Techniques
•Romania	•Lawfulness of data processing	•Art. 8 CFR	•Court of Appeal	Consistent interpretation

Case(s) description

1. *Facts*

Ms Smaranda Bara and numerous other Romanian citizens are self-employed workers. The Romanian tax authority (ANAF) transferred data relating to their declared income to the National Health Insurance Fund (CNAS), which then required the payment of arrears of contributions to the health insurance regime. The persons concerned contested, before the Court of Appeal Cluj (Romania), the lawfulness of that transfer under the Data Protection Directive (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995), which governs the processing of personal data when they are contained within a filing system. They submitted that their data were used for purposes other than those for which those data had initially been communicated to the tax authority, without their prior explicit consent and without their having previously been informed.

2. *Reasoning of the Court*

The national court summed up the legal reasoning of the CJEU. The Charter has not been mentioned in its judgment.

[61] Casesheet drafted on the basis of the template provided by Diana Lavinia Botău.

The Court of Appeal mainly held that the tax data transferred to the CNAS by the ANAF are personal data within the meaning of Article 2(a) of Directive 95/46/EC. Both the transfer of the data by the ANAF and their subsequent processing by the CNAS therefore constitute 'processing of personal data' within the meaning of Article 2(b) of the Directive.

In accordance with the provisions of Chapter II of Directive 95/46/EC, entitled 'General rules on the lawfulness of the processing of personal data', subject to the exceptions permitted under Article 13 of that Directive, all processing of personal data must comply, first, with the principles relating to data quality set out in Article 6 of the Directive and, secondly, with one of the criteria for making data processing legitimate listed in Article 7 of the Directive. Furthermore, the data controller or his representative is obliged to provide information in accordance with the requirements laid down in Articles 10 and 11 of Directive 95/46/EC.

As regards Article 10 of the Directive, it states that the data controller must provide a data subject, from whom data relating to himself are collected, with the information listed in subparagraphs (a) to (c), except where he already has that information. That information concerns the identity of the data controller, the purposes of the processing and any further information necessary to guarantee fair processing of the data. The requirement to inform the data subjects about the processing of their personal data is all the more important since it affects the exercise by the data subjects of their right of access to, and right to rectify, the data being processed, set out in Article 12 of Directive 95/46/EC, and their right to object to the processing of those data, set out in Article 14 of that Directive.

However, the applicants were not informed by the ANAF of the transfer to the CNAS of personal data relating to them.

ANAF submitted that Article 315 of Law No 95/2006 provided for the transfer to the regional health insurance funds of the information necessary for the determination by the CNAS as to whether persons earning income through self-employment qualify as insured persons.

Article 315 of Law No 95/2006 expressly provides that 'the data necessary to certify that the person concerned qualifies as an insured person are to be communicated free of charge to the health insurance funds by the authorities, public institutions or other institutions in accordance with a protocol'. However, the data necessary for determining whether a person qualifies as an insured person, within the meaning of the abovementioned provision, do not include those relating to income, since the law also recognises persons without a taxable income as qualifying as insured. Therefore, Article 315 of Law No 95/2006 cannot constitute, within the meaning of Article 10 of Directive 95/46/EC, prior information enabling the data controller to dispense with his obligation to inform the persons from whom data relating to their income are collected as to the recipients of those data. Accordingly, it cannot be held that the transfer at issue was carried out in compliance with Article 10 of Directive 95/46/EC.

As to whether Article 13 of the Directive applies to that failure to inform the data subjects, it is apparent from Article 13(1)(e) and (f) that the State may restrict the scope of the obligations and rights provided for in Article 10 of the same Directive when such a restriction constitutes a necessary measure to safeguard 'an important economic or financial interest of a Member State […], including monetary, budgetary and taxation matters' or 'a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e)'. Nevertheless, Article 13 expressly requires that such restrictions are imposed by legislative measures.

However, the definition of transferable information and the detailed arrangements for transferring that information were not laid down in a legislative measure but in the 2007 Protocol agreed between the ANAF and the CNAS, which was not the subject of an official publication.

Therefore, it cannot be concluded that the conditions laid down in Article 13 of Directive 95/46/EC are complied with. On the other hand, Article 11(1) of the Directive provides that a controller of data which were not obtained from the data subject must provide the latter with the information listed in subparagraphs (a) to (c). That information concerns the identity of the data controller, the purposes of the processing, and any further information necessary to ensure the fair processing of the data. Amongst that further information, Article 11(1)(c) of the Directive refers expressly to 'the categories of data concerned' and 'the existence of the right of access to and the right to rectify the data concerning him'.

However, the CNAS did not provide the applicants in the main proceedings with the information listed in Article 11(1)(a) to (c) of the Directive.

In accordance with Article 11(2) of Directive 95/46/EC, the provisions of Article 11(1) of the Directive do not apply, in particular, when the registration or communication of the data is laid down by law. However, the provisions of Law No 95/2006 and the 2007 Protocol do not establish a basis for applying either the derogation under Article 11(2) or that provided for under Article 13 of the Directive.

Therefore, Articles 10, 11 and 13 of Directive 95/46/EC must be interpreted as precluding measures such as those at issue in the proceedings, which allow a public administrative body to transfer personal data to another public administrative body and their subsequent processing, without the data subjects having been informed of that transfer or processing.

c. Impact on national cases

The national courts recognise the authority of the CJEU's judgments and this case has been widely publicised.

Analysis

a. Judicial dialogue

a.1. Vertical interaction

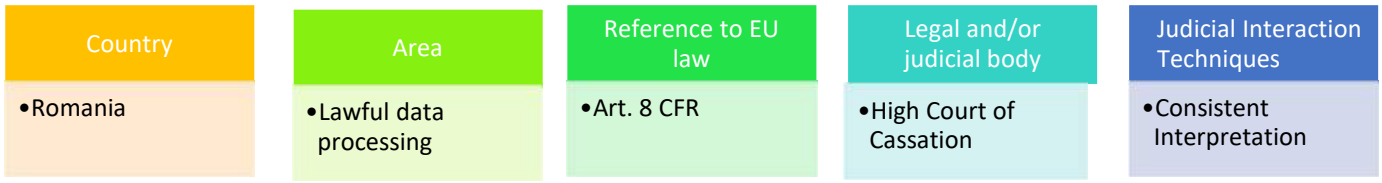
The national Judge did not refer at all to the CFR and CJEU and ECtHR case law.
The interactions between the courts did not trigger changes to the legislative framework; however, they clarified the proper way of interpreting and applying the national law, in accordance with Directive 95/46/EC.
The national court does not make citations and engage with an assessment of other national judgments. However, it referred to the CJEU, for a preliminary reference. Also, no constitutionality review was involved.

Casesheet no 11[62] – Romania, Înalta Curte de Casație și Justiție, (High Court of Cassation and Justice), Case no 3306/1/2015, Decision no 37 of 7 December 2015

Link to the full text:
http://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=126147

Core issues
Is anonymisation a sufficient guarantee not to undermine data protection, by safeguarding the right of information?

At a glance



Case(s) description

a. Facts

The plaintiff registered a request with the Ministry of National Education, based on Law 544/2001, to disclose the content of the Report of the Review Board of the Prime Minister concerning the Ovidius University of Constanța. The Constanța Tribunal, as the First Instance Court, rejected the plaintiff's claim, having found that the defendant had disclosed a summary of the findings of that report and the measures taken. The plaintiff filed a special appeal with the Constanța Court of Appeal, claiming that Law No 544/2001 had been incorrectly interpreted. According to the plaintiff, the name alone is insufficient to identify the persons involved, and therefore Law No 677/2001 had not been properly interpreted, since disclosing the names of the persons targeted by the control action would have been in agreement with data protection legislation.
The Constanța Court of Appeal stressed the novelty of the issue claimed in the special appeal and forwarded a question to the HCCJ for a preliminary decision on the matter.

b. Reasoning of the Court

The Court made express reference to the necessity to comply with both the CFREU and the ECHR, as well as other instruments of EU or Council of Europe legislation. However, no direct reference to the European texts was made, as well as no mention of CJEU or ECtHR jurisprudence.
Commencing with a review of national jurisprudence on the matter, the HCCJ found that sometimes courts had considered that the names alone are not sufficient to identify persons involved, and

[62] Casesheet drafted on the basis of the template provided by Sergiu Popovici.

therefore are not protected by Law No 544/2001. Many other courts, however, found that the names represent personal data, and are subject to protection regardless of their ability to lead to the identification of the persons involved.
The Court found that, with regard to the relationship between legislation on information of public interest and that of personal data protection, while in principle these two categories are independent, they may overlap when information of public interest and personal data are found in the same document, regardless of their form or medium. In such an overlapping situation, a coherent and uniform approach is necessary, which may provide adequate protection of all the rights involved and, in particular, to proportionality and just balance between the right to be informed and the right to private life, essential in a democratic society. The overlap is possible only if information concerning the personal data of private persons is not susceptible to affect the exercise of a public office; on the contrary, that information becomes of public interest, which would then take prevalence over the right to personal data protection.
Taking into account these elements, and the phrasing of the national texts, the Court found that in the sense of Article 2(1)(c) of Law No 544/2001 and Article 3(1)(a) of Law No 677/2001, the name and surname of a private person represent information related to personal data, regardless of the fact that, in a given situation, they are sufficient to provide identification of that person.
Moreover, in the case of requests of free access to information of public interest based on Law No 544/2001, when that information and personal data are present in the content of the same document, regardless of its form or medium, access to information of public interest is granted only after the anonymisation of information regarding personal data; should personal data be anonymous, any refusal to reveal information of public interest by the requested authority would be unjustified.

c. Impact on national cases

This case has been mentioned in Decision no 1430 of 6 April 2017 as grounds for the HCCJ to reject the claim of a plaintiff looking to reveal the name of a person who interrupted by telephone the intervention of a paramedical crew (the phone number was revealed to the plaintiff, but not the name of the caller).
It can be predicted that the decision (still rather recent) will be mentioned by later jurisprudence concerning requests to reveal the names of persons involved in certain activities, at all levels of the national courts.

Analysis

a. Role of the Charter

In its ruling, the Court did not make a separate analysis of the provisions of the Charter, despite expressly mentioning the necessity to conform with it. Protection of the names of the persons involved in actions covered by information of public interest was analyses in substance exclusively from the perspective of national law.

b. Judicial dialogue

b.1. Vertical interaction

The High Court of Cassation and Justice made no reference to the CFREU; despite the fact that the concept of personal data has become part of the Romanian legal landscape exclusively through European legislation; there is no concrete reference to European texts or to jurisprudence of the CJEU or the ECtHR, the Court relying exclusively on the phrasing of national legislation to give its reasoning.

As regards *consistent interpretation,* the Court aimed to interpret national legislation from the perspective of compliance with the CFREU, the ECHR, the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and Directive 95/46/CE.
Proportionality was a technique used when balancing the legal interest of persons to have access to information of public interest with the right to personal data protection.

b.2. Horizontal dialogue (European)

Horizontal interaction with other jurisprudence of the HCCJ (regular composition of three judges): Decision no 3,699 of 9 October 2014, by which the Court (Administrative and fiscal section) decided that the personal data of the participants in a contest are protected by Article 12(1)(d) of Law No 544/2001.
Horizontal interaction with the Romanian Constitutional Court, which by Decisions no 1,175 of 11 December 2007 and 220 of 9 May 2013 found that the provisions of Law No 544/2001 were constitutional.

Casesheet no 12[63] – Italy, First Instance Criminal Court, Case no 325/2018, Decision of 15 November 2018

Core issues
Is data processing of political opinions (to be included in special categories of data) lawful?

At a glance

Country	Area	Reference to EU law	Legal and/or judicial body	Judicial Interaction Techniques
Italy	•Lawful data processing	Art. 9 GDPR	•Criminal Court - First Instance	•Consistent Interpretation

Case(s) description

a. Facts

The facts regard the publication of the data within a local news article in a national circulation newspaper. The object of the conduct consisted in the identification data of the offended person, specifically regarding the complete address of the residence of the offended person, associated with data concerning his neo-fascist political opinions. The elements of special illegality are indicated in the absence of the consent of the interested party and in the non-traceability of the processing of the data to Articles 18, 24, 137 legislative decree 196 of 2003. The event of the crime consisted in making the offended person traceable in the context in which it was described as having been involved in the planning of neo-fascist attacks and the specific intent has been described as 'the purpose of profiting from it for oneself and others, or of causing damage to others'.

b. Reasoning of the Court

Unlike what the defence claims, it cannot be generally and abstractly argued that it has become a criminally legitimate fact in itself to make subjects who embrace political opinions that are not (or not yet) publicly promoted by themselves identifiable through their nominative indication and associated with the indication of their residence (as well as philosophical convictions).
It is therefore necessary to evaluate concretely, pursuant to Article 9(2)(g) EU Regulation 2016/679, whether the data processing of the offended person was 'necessary for reasons of significant public interest on the basis of EU law or of the Member States', as well as whether it was 'proportionate to the aim pursued', if it respected 'the essence of the right to data protection' and provided for 'appropriate and specific measures to protect the fundamental rights and interests of the data subject'.
The purpose of the article signed by the accused was to inform the readers of the local news with the famous headline about the existence of a large cell, active in the city of Milan, of a self-styled school of politics linked to a neo-fascist association composed of 14 people, of whom three were seriously suspected of having planned attacks against police headquarters, prefectures, magistrates, the

[63] Casesheet drafted provided on the basis of the template provided by Dr Stefano Caramellino.

headquarters of the collection agent, ministers, banks, post offices and the Head of State, with a view to simultaneous action in three large cities, 'to create a hint of terror', and hitting the population to induce 'the people ... to ask for help'.
The relevance of the local public interest with certainty exists not only in the news itself, but also in the unique identifiability of the physical persons active in the Milan area. Precisely because of the political vocation of the cell that had possible terrorist aspiration, the interest in knowing the identity of the persons belonging to this group is public, since each of the readers of the local news is, for geographical reasons, in the situation of being able to come into contact with such natural persons and to receive requests, invitations, messages of any kind from each of the aforementioned adepts, aimed at obtaining if not explicitly support then information potentially useful to their projects based on the seriousness of their terrorist nature. In other words, the public interest in the local knowledge of the identity of the adherents of the Milanese cell consists in identifying the subjects that can use their social or interpersonal relationships, in a more or less veiled or indirect way, for terrorist purposes.
It must therefore be affirmed that each reader of the local news of Milan, as a potential acquaintance of today's offended person in the political context of the city, had a concrete and actual interest in unambiguously knowing that it is precisely today's offended person, identified in a way that cannot be confused with another of the same name on the basis of his residence, who was a person strongly suspected of being close to subjects seriously suspected of having joined together to cultivate neo-fascist terrorist projects.
The data processing referred to in the indictment was proportionate to the aim pursued.
In fact, there was no means that could achieve the same information goal through a less expensive compression of the protection of the personal sphere of the [injured person]. Given the well-known diffusion of the surname and the existence of the same names on the same territory, which can now be verified with an elementary computer search, the indication of the residence of the data subject was the least expensive means to protect, quite dutifully, the public image of his namesake who had not kept his own conduct and who did not share his political orientation.
The data subject was made identifiable with the minimum means concretely possible, so that only the political aspects of her family and private life could be drawn from the article.

Analysis

c. Role of the Charter

In its ruling, the Court did not make a separate analysis of the provisions of the Charter. Nonetheless, it argues that the data subject had 'appropriate and specific measures to protect her fundamental rights and interests'.

d. Judicial dialogue

d.1. Interaction between legal provisions

With regard to the existence of a legal basis suitable for defining and characterising the relevance of the public interest covered by the data subject for processing, the national law currently in force specifies the notion of 'reasons of significant public interest' in Article 2-sexies decree Legislative Decree 196 of 2003.
This State law provision, which entered into force on 19 September 2018, allows the processing of sensitive personal data, such as those pertaining to political opinions, not only by identifying the subjects to which the public authorities attribute the public interest in the processing of data, but also by means of a referral provision open to provisions in force in the law of the European Union and

provisions of law that provide for the processing of sensitive data. This provision of deferment, very broad in its literal tenor, expressly enables the interpreter, including the judge, to find out if there are provisions in the EU rights that can legitimise the processing of sensitive personal data if there are reasons of significant public interest. It may well be any EU law or Member State law, since it is only of secondary state laws that the referral rule requires that they 'specify the types of data that can be processed, the operations that can be performed and the reason for the interest of the relevant public, as well as appropriate and specific measures to protect the fundamental rights and interests of the data subject'.
In the GDPR we find express forecasts that recognise the specificity of journalism, its central value for the purposes of freedom of expression and information as essential to democratic societies and the consequent duty to reconcile the protection of personal data with the aforementioned freedoms: these are recitals 153 and 85 of EU regulation 2016/679 itself. This last provision allows individual Member States, with reference to the processing of data and facts for journalistic purposes, to recognise exceptions or exemptions even to the principles laid down in the specific chapter with which the general regulation on data protection begins (Articles 5-11).
Therefore, the requirement of a sufficient legal basis to find a relevant interest must be satisfied, by referring to Article 85 of EU regulation 2016/679, which can be deduced from Article 2-sexies d.lgs. public in relation to the data being processed.

d.2. Vertical interaction: partially different interpretation

On 24 September the Grand Chamber released *Case C-136/17* (CG, CNIL and a) and held that the prohibition or restrictions relating to the processing of special categories of personal data apply also to the operator of a search engine in the context of his responsibilities, powers and capabilities as the controller of the processing carried out in connection with the activity of the search engine, following a request by the data subject.

Although the issue at stake here is not the lawfulness of the processing of special categories of data but the right to erasure for special categories of data, some differences have to be highlighted in order to identify the different approaches followed by the national court and the Grand Chamber[64].

In particular, the Grand Chamber holds that the operator of a search engine is in principle required to accede to requests for de-referencing in relation to links to web pages containing personal data which fall within the special categories referred to by those provisions. Such an operator may refuse to accede to a request for de-referencing if he establishes that the links at issue lead to the content comprising personal data that falls within the special categories referred to in Article 8(1) but whose processing is covered by the exception in Article 8(2)(e) of the Directive, provided that the processing satisfies all the other conditions of lawfulness laid down by the Directive, and unless the data subject has the right under Article 14(a) of the Directive to object to that processing on compelling legitimate grounds relating to his particular situation. If the operator of a search engine has received a request for de-referencing relating to a link to a web page on which personal data that fall within the special categories referred to in Article 8(1) or (5) of Directive 95/46 are published, the operator must, on the basis of all the relevant factors of the particular case and taking into account the seriousness of the interference with the data subject's fundamental rights to privacy and protection of personal data laid down in Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, ascertain. In particular, he has to look at the reasons of substantial public interest referred to in Article 8(4) of the

[64] See http://curia.europa.eu/juris/document/document.jsf?text=&docid=218106&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=3278784, ECLI:EU:C:2019:773.

Directive and in compliance with the conditions laid down in that provision, whether the inclusion of that link in the list of results displayed following a search on the basis of the data subject's name 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, protected by Article 11 of the Charter.

In conclusion, information relating to legal proceedings brought against an individual and information relating to an ensuing conviction are data relating to 'offences' and 'criminal convictions' within the meaning of Article 8(5) of Directive 95/46, and the operator of a search engine is required to accede to a request for de-referencing relating to links to web pages displaying such information, where the information relates to an earlier stage of the legal proceedings in question and, having regard to the progress of the proceedings, no longer corresponds to the current situation, in so far as it is established in the verification of the reasons of substantial public interest referred to in Article 8(4) of Directive 95/46 that, in the light of all the circumstances of the case, the data subject's fundamental rights guaranteed by Articles 7 and 8 of the Charter of Fundamental Rights of the European Union override the rights of potentially interested internet users protected by Article 11 of the Charter.

Intellectual property and data protection: balance of interests

Casesheet no 12 – Romania, Înalta Curte de Casație și Justiție, (High Court of Justice and Cassation) - Decision no 1059 of 16 June 2017

Casesheet no 13[65] – Romania, Înalta Curte de Casație și Justiție, (High Court of Justice and Cassation) - Decision no 1059 of 16 June 2017

Link to the full text:
http://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=141605

Core issues
Whether the administrator of a web domain may be held liable for breach of the industrial property rights of a third party by a user of that domain (owner of the website), and whether that party may require from the administrator of the web domain the disclosure of the personal data of users of the culpable owner's website

At a glance

Country	Area	Reference to EU law	Legal and/or judicial body	Judicial Interaction Techniques
•Romania	•Unlawfulness of data processing	•Directive 2004/48/EC •Directive 89/204/EC •Regulation 40/94 •Art. 7 CFR	•High Court of Cassation	•Consistent interpretation

Case(s) description

a. *Facts*

The plaintiffs made a claim according to special legislation and in tort against the defendants for unlawful use, on their website, of a catalogue looking to commercialise perfumes by direct reference to the denominations and indicators protected by the plaintiff's intellectual/industrial property rights. The plaintiffs also made their claim against S SA, the administrator of the web domain (.ro) of the website in question, moreover asking that the court compel S SA to disclose information concerning the users of the website (the persons who accessed the other defendant's catalogue and who may have been implicated in the distribution of the perfumes through the other plaintiff's website).
The Bucharest Tribunal granted the plaintiff's request against the owner of the website but rejected the claim (in tort and concerning the disclosure of personal data) against the administrator of the web domain. The litigation reached the HCCJ in a first cycle, the supreme court deciding to repeal the

[65] Casesheet drafted on the basis of the template provided by Sergiu Popovici.

initial decision of the Bucharest Court of Appeal and to send the case for retrial of the appeal. The second special appeal was the subject of scrutiny by the Court in the analysed decision.

b. Reasoning of the Court

The High Court of Cassation and Justice rejected the plaintiffs' special appeal, and maintained that the defendant S SA, the administrator of the web domain, could not be held liable for damages suffered by the plaintiffs, and may not (let alone be obliged to) disclose the personal information of the persons who accessed the website of the other defendant.
In its reasoning, the Court started from an analysis of Article 8 GEO 100/2005, correspondent to Article 8 of Directive 2004/48/EC, which provides that information on the origin and distribution networks of the goods or services which infringe an intellectual property right has to be provided by the infringer or by the person found to be providing on a commercial scale services used in infringing activities, upon request of the competent court.
The Court decided that, in order to asses both the claims (in tort and concerning disclosure of personal data), it needed to analyse whether S SA, the administrator of the web domain, was a person providing commercial services used in infringing the intellectual rights of the plaintiffs. The court found that S SA, as administrator of the domain .ro, had provided, through two subdomains, services consisting exclusively on storage and hosting.
In the above-mentioned assessment, the Court relied on the rulings of the CJEU in joint cases C-237-239/08, *Google France SARL* and case C-324/2009, *L'Oreal* v *Ebay*, and found that, since through the two subdomains S SA had only provided services of hosting and storage, not administration, it had no connection to data on the websites and no gain from it.
Unlike the persons directly involved in the infringement, who are clearly obliged to disclose information concerning their own activity, in the case of suppliers of services of electronic communications, the issue is whether they may disclose personal data which they had processed on account of a legal authorization.
The Court found that the general claim concerning disclosure, involving the activity of another defendant, was not precise enough, and required more analysis of the context. In that analysis, the Court found that the plaintiffs claimed that S SA itself had committed an infringement, and therefore assumed that it had access to data concerning the commercial activity of the other defendant. The claim in the special appeal was thus found to have been based on the legal relationship between the two defendants, not between the S SA and its other clients.
Since the request for disclosure of the information was made in the context of infringement done by the other defendant, based not on a legal relationship between S SA and its clients, the Court found that the request was not sufficiently well grounded on Article 8 GEO 100/2005, and the necessity arose to analyse the proportionality between the request of disclosure, as a means to protect intellectual property, and other fundamental human rights of the website users, such as the right to private life and to protection of personal data.
In its assessment of proportionality, the Court relied on the decision given by the CJEU in case C-461/10, *Bonnier Auto*, paras. 59-60, and found that disclosure of the identity data of an internet user, prohibited by the principle of personal data protection, was not allowed in the case at hand, the object of which was infringement of intellectual property by a person other than the respective user.
For the abovementioned reasons, the Court found that the plaintiffs' special appeal was unfounded, and that S SA was not liable for damages caused by infringement of intellectual property rights by an owner of a website belonging to a subdomain it managed, and was not allowed to disclose to the plaintiffs the identity data of the users of that respective website.

Analysis

a. Role of the Charter

In its ruling, the Court did not make a separate analysis of the provisions of the Charter, analysing the protection of personal data exclusively from the perspective of national law, with reference to the jurisprudence of the CJEU.
The High Court of Cassation and Justice relied exclusively on national legislation, but did make several references to the jurisprudence of the CJEU. It did not make any reference to the Charter, nor to the relationship between the CFR and the ECHR. There were no references to the jurisprudence of the ECtHR.

b. Judicial dialogue

b.1. Vertical interaction

There are elements of vertical interaction between the HCCJ and the lower courts, as for instance a special appeal. In this case, there were two procedural cycles: the first, starting with the Bucharest Tribunal, then with the Bucharest Court of Appeal and the HCCJ, ended with the first decision of the Supreme Court, repealing the decision of the latter and sending the case for retrial to the Bucharest Court of Appeal, where the second cycle started, and ended with the final decision of the HCCJ, subject of the present analysis. Indications of the Supreme Court in the first cycle are compulsory to all courts in the second cycle, including the HCCJ itself.
The High Court of Cassation and Justice made no reference to the Charter concerning personal data protection, despite the fact that national law, the only one to be analysed, originates from the legislation of the European Union.
The Court did make reference to the jurisprudence of the CJEU when assessing the proportionality between the right of information of the damaged party and the right of third parties to personal data protection.
The Court made no observations concerning the ECHR or the jurisprudence of the ECtHR.

Casesheet no 14[66] – Romania, Bucharest County Court - 29152/3/2007, Bărbulescu Bogdan Mihai v S.C. Secpral Pro Instalații S.R.L., ordinary, 07.12.2007

Link to the full text:
http://portal.just.ro/3/SitePages/Dosar.aspx?iddosar=300000000175504&idinst=3

Core issues
Is the right of the employer to monitor professional performance compatible with the right to privacy of correspondence in the workplace of the worker?

At a glance

Country	Area	Reference to EU law	Legal and/or judicial body	Judicial Interaction Techniques
•Romania	•Right to private life	•Directive 2006/24/EC •Arts. 7 and 8 CFR	•County Court	

Case(s) description

a. *Facts*

The applicant was employed as a sales engineer. The employer's internal regulations prohibited the use of company resources by employees. However, the regulations did not contain any reference to the possibility of the employer monitoring employees' communications.

The employer recorded the applicant's Yahoo Messenger communications in real time. On 13 July 2007, the applicant was summoned by his employer to give an explanation for forty-five pages of private correspondence he had exchanged with his brother and his fiancée, using the employer's internet site ID. The messages related to personal matters and some were of an intimate nature. On 1 August 2007 the employer terminated the applicant's contract of employment.

The applicant challenged his dismissal in an application to the Bucharest County Court. He asked the court to set aside the dismissal, to order his employer to pay him the amounts he was owed in respect of wages and any other entitlements and to reinstate him in his post, to order the employer to pay him damages for the harm resulting from the manner of his dismissal, and to reimburse his costs and expenses.

b. *Reasoning of the Court*

[66] Casesheet drafted on the basis of the template provided by Diana Lavinia Botău.

The reasoning of the County Court does not explicitly refer to the EU Charter. The reasoning mainly states that the procedure for conducting a disciplinary investigation is expressly regulated by the provisions of Article 267 of the Labour Code. The employer conducted the disciplinary investigation in respect of the applicant by twice summoning him in writing to explain himself and the applicant had the opportunity to submit arguments in his defence regarding his alleged acts.

The Court took the view that the monitoring of the internet conversations in which the employee took part using the Yahoo Messenger software on the company's computer during working hours cannot undermine the validity of the disciplinary proceedings in the instant case.

The fact that the provisions containing the requirement to interview the suspect in a case of alleged misconduct and to examine the arguments submitted in that person's defence prior to the decision on a sanction are couched in imperative terms highlights the legislature's intention to make respect for the rights of the defence a prerequisite for the validity of the decision on the sanction.

In the present case, since the employee maintained during the disciplinary investigation that he had not used Yahoo Messenger for personal purposes but in order to advise customers on the products being sold by his employer, an inspection of the content of the applicant's conversations was the only way in which the employer could ascertain the validity of his arguments.

The employer's right to monitor employees in the workplace, particularly as regards their use of company computers, forms part of the broader right, governed by the provisions of Article 40(d) of the Labour Code, to supervise how employees perform their professional tasks.

Given that it has been shown that the employee's attention had been drawn to the fact that, shortly before the applicant's disciplinary sanction, another employee had been dismissed for using the internet, the telephone and the photocopier for personal purposes, and that the employees had been warned that their activities were being monitored, the employer cannot be accused of showing a lack of transparency and of failing to give its employees a clear warning that it was monitoring their computer use.

Internet access in the workplace is above all a tool made available to employees by the employer for professional use and the employer indisputably has the power, by virtue of its right to supervise its employees' activities, to monitor personal internet use.

Such checks by the employer are made necessary by, for example, the risk that through their internet use, employees might damage the company's IT systems, carry out illegal activities in cyberspace for which the company could incur liability, or disclose the company's trade secrets.

The court considered that the acts committed by the applicant constitute a disciplinary offence within the meaning of Article 263(2) of the Labour Code since they amount to a culpable breach of the provisions of his employer's internal regulations, which prohibit the use of computers for personal purposes.

The aforementioned acts are deemed by the internal regulations to constitute serious misconduct, the penalty for which is termination of the contract of employment on disciplinary grounds.

Therefore, the court considered that the decision complained of was well-founded and lawful, and dismissed the application as unfounded.

The County Court's judgment was challenged in an appeal, at the national level; eventually, the case ended up before the European Court of Human Rights (app. no 61496/08). The applicant complained, in particular, that his employer's decision to terminate his contract had been based on a breach of his right to respect for his private life and correspondence as enshrined in Article 8 of the Convention and that the domestic courts had failed to comply with their obligation to protect that right. The application was allocated to the Fourth Section of the Court. On 12 January 2016 a Chamber of that Section held, by six votes to one, that there had been no violation of Article 8 of the Convention. The

dissenting opinion of Judge Pinto de Albuquerque was annexed to the Chamber judgment. On 12 April 2016 the applicant requested the referral of the case to the Grand Chamber and on 6 June 2016 a panel of the Grand Chamber accepted the request and delivered the judgment on 5 September 2016.

c. Impact on national cases

The County Court's decision had an actual impact on the parties. However, the case ended up before the Grand Chamber of the European Court of Human Rights and has been widely publicised. Therefore, we can presume it has a real impact on related national case law.
The applicant challenged the judgment issued by the Bucharest County Court, before the Bucharest Court of Appeal. His appeal was dismissed. After finishing the internal proceedings, the applicant filed an application against Romania at the European Court of Human Rights. He complained, in particular, that his employer's decision to terminate his contract had been based on a breach of his right to respect for his private life and correspondence as enshrined in Article 8 of the Convention and that the domestic courts had failed to comply with their obligation to protect that right. The application ended up before the Grand Chamber, which found that the 'domestic authorities did not afford adequate protection of the applicant's right to respect for his private life and correspondence and that they consequently failed to strike a fair balance between the interests at stake'.

Analysis

Judicial dialogue

Vertical interaction

The national court did not make citations and engage with an assessment of other national judgments. However, the Court of Appeal referred to CJEU case law. Also, no constitutionality review was involved.

Horizontal dialogue (European)
The court did not make citations and/or engage with an assessment of other national judgments. Also, there was no constitutionality review involved. The decision did lead to a judgment issued by the European Court of Human Rights.

Subsequent case decided by the ECtHR

The ECtHR considered that the Contracting States must be granted a wide margin of appreciation in assessing the need to establish a legal framework governing the conditions in which an employer may regulate electronic or other communications of a non-professional nature by its employees in the workplace. Nevertheless, the discretion enjoyed by States in this field cannot be unlimited. The domestic authorities should ensure that the introduction by an employer of measures to monitor correspondence and other communications, irrespective of the extent and duration of such measures, is accompanied by adequate and sufficient safeguards against abuse.

Despite the rapid developments in this area, proportionality and procedural guarantees against arbitrariness are essential. In this context, the Court considered that domestic authorities should treat the following factors as relevant:
(*i*) whether the employee has been notified (in a clear manner and in advance) of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures;

(*ii*) the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy;

(*iii*) whether the employer has provided legitimate reasons to justify monitoring the communications and accessing their actual content;

(*iv*) whether it would have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employee's communications;

(*v*) the consequences of the monitoring for the employee subjected to it and the use made by the employer of the results of the monitoring operation;

(*vi*) whether the employee had been provided with adequate safeguards, especially when the employer's monitoring operations were of an intrusive nature.

The Court examined how the national authorities took the criteria set out above into account in their reasoning when weighing the applicant's right to respect for his private life and correspondence against the employer's right to engage in monitoring, including the corresponding disciplinary powers, in order to ensure the smooth running of the company.

Notwithstanding the respondent State's margin of appreciation, the Court considered that the domestic authorities did not afford adequate protection of the applicant's right to respect for his private life and correspondence and that they consequently failed to strike a fair balance between the interests at stake. Therefore, the Court found that there has been a violation of Article 8 of the Convention.

Casesheet no 15[67] – Italy, Court of Padua, n. 709/2018, 24 December 2018

Core issues
Is the right of the employer to monitor professional performances proportionate as a measure to balance the right to privacy of the employer with the right to protect other individuals' rights?

At a glance

Country	Area	Reference to EU law	Legal and/or judicial body	Judicial Interaction Techniques
Italy	•Right to private life	•Arts. 7 and 8 CFR	•First Instance Court	•Dissenting judicial interprertation

Case(s) description

a. Facts

A worker at a call centre appeals a dismissal for misconduct by challenging the violation of Article 4 of the *Workers' Statute* (Law 300/1970) which provided – before the entry into force of *Jobs Act* (d.lgs. 151/2015) - that audio-visual equipment and other equipment through which the remote control of workers' activities is possible can also be used exclusively for organisational and production needs, for the protection of the safety of work and for the integrity of the company assets and can be installed by agreement stipulated with the sector union representation or by the company trade union representatives.
In fact, the employer, as a result of checks on the performance by the employer, within the scope of its corporate organisation, caught her during activities involving the illegitimate display of data traffic of people not corresponding to actual work needs, as it did not derive from specific customer requests. As a result of investigations, 34 of the 46 ascertained activities were carried out after the entry into force of the Jobs Act, which amended the Workers' Statute providing that information collected can be used for all purposes related to the employment relationship and that the worker should be given adequate information on how to use the tools and carry out controls and this to be in accordance with the national data protection framework.

b. Reasoning

The purpose of Article 4 of Law 300/1970 is not only to establish a system of guarantees of a substantial nature and procedure to protect the privacy of the worker, but also to put the latter in a position to know of such guarantees. Therefore, the provision applicable is the one before the entry into force of the *Jobs Act*. The theory of defensive controls assumes importance, according to which monitoring measures were not taken with the intent to monitor the contractual obligations of the worker but in order to ascertain illegal conduct detrimental to the company assets and rights of third parties.

[67] This casesheet has been drafted on the basis of the Italian judgement delivered by Judge Francesco Perrone.

The misconducts attributed to the worker are illegitimate both under criminal law violations for illegal access to the computerised and telematics system and under civil law for violation of the privacy of third parties.
In this case, it seems to be correct to refer to the control exercised by the employer in the context of the defensive checks, as it is aimed at ascertaining the existence of behaviours characterised by profiles of unlawfulness other than the mere breach of contract.
Furthermore, the control tool adopted by the company has been the only one available to reach the aim pursued.
With regard to the seriousness of the conducts established, taking into account that they were carried out by a public service representative and also involved an undue intrusion into the assets of sensitive data belonging to an unaware user of an essential public service, it must be considered established that they are serious enough to justify dismissal.

Analysis – *Legal context*

Protection of privacy at the workplace, Italy

Article 15 of Constitution of the Italian Republic establishes the fundamental right to liberty and secrecy of correspondence and any other kind of communication.
Limitations on this right are permitted only on the basis of an order from a judicial authority and only in such cases established by law.

Section 4 of Law No 300 of 20 May 1970 ('*Statuto dei Lavoratori*'), which has been recently reformed by Section 23 of Legislative Decree No 151 of 14 September 2015 ('*Jobs Act*'), provides for: (i) a specific regulation governing the power of surveillance and monitoring by employers over electronic communications in the workplace; and (ii) the general conditions for remote control over employees in the workplace.

Dispositions provided in Section 4 of the *Statuto dei Lavoratori* are inserted within the framework of Legislative Decree No 196 of 30 June 2003 ('*Privacy Code*'), which is a general text governing the collection and processing of personal data by any kind of public or private entity.
In particular, Section 114 (*Remote controls*) par. 3 of the *Privacy Code,* provides as follows:

> *'The dispositions of the Privacy Code shall apply without prejudice to Section 4 of the Statuto dei Lavoratori'.*

Section 4 ('*Audio-visual installations and other tools of control*') par. 1 of the *Statuto dei Lavoratori*, in its new wording, provides as follows:

> '*Audio-visual installations and other tools of control which give even the possibility of remote controls over the work activity of employees may be used only in view of organisational and productive necessities, of the safety of the work and of the protection of the corporate assets, and they may be installed only in case of prior collective agreement concluded by the company-based trade unions […]. In the absence of such agreement, audio-visual installations and other tools of control may be installed only in force of prior authorisation of the Territorial Direction of Work [Direzione Territoriale del Lavoro] or […] in force of prior authorisation of the Ministry of Labour*'.

Section 4 par. 2 of the *Statuto dei Lavoratori*, in its new wording, provides as follows:

> '*The provision sub § 1 does not apply either to tools used by the employee for carrying out his work or to tools for the registration of accesses and of presences in the workplace*'.

Section 4 par. 3 of the *Statuto dei Lavoratori*, in its new wording, provides as follows:

> '*The information collected in accordance to parr. 1 and 2 may be used in view of every aim related to the employment relationship, under the condition that the employee is provided with adequate information on the way these tools are used and on the way the controls are carried out, and in accordance with provisions laid down by the Privacy Code*'.

Therefore, an analysis of Section 4 of the *Statuto dei Lavoratori* demonstrates that the domestic legislation governing the power of surveillance and control over the activity of the employees in the workplace is based on four fundamental rules.
Firstly, the installation of tools used for the direct control, surveillance, and monitoring by the employer of work activity carried out by his/her employees is prohibited (Section 4 § 1 of the *Statuto dei Lavoratori*).
Secondly, the national law provides for specific objective conditions that are required for the installation of audio-visual tools and other tools of control that give even the possibility of remote control over the activity of employees (Section 4 par. 1 of the *Statuto dei Lavoratori*).
Thirdly, the national law does not provide for any specific objective conditions with regards to the installation and use of work tools that give the employer the possibility of remote control over the activities of employees (e.g. tablets, mobile phones, computers, laptops, and GPS technology, where the employee has been supplied with these types of work tools by his or her employer) (Section 4 par. 1 of the *Statuto dei Lavoratori*).
Finally, information that has been collected in accordance with parr. 1 and 2 may be used by the employer for any purpose that is related to the employment relationship. However, this must comply with the condition that the employee is adequately informed (in accordance with provisions laid down by the *Privacy Code*) on: (i) the way these tools of control are used; and (ii) the method by which control and surveillance is carried out.

Both the previous and new wording of Section 4 of the *Statuto dei Lavoratori* raise two significant questions that have been the subject of debate.
Firstly, no rules are provided for with respect to the conditions or limits on the power of control over the private electronic tools of the employee, such as the personal *Facebook* or *Twitter* account of the employee or other general personal social media accounts.
Secondly, the mixed usage of electronic working tools (both business and personal use) supplied by the employer (such as mobile phones, tablets, corporate cars equipped with GPS technology) is a common practice established by company policies. However, no specific rules have been provided for under Section 4 that deal with the power of control exercised by these types of work tools.

I. Case law of the Labour Chamber of the Court of Cassation

Considering the recent entry into force of the reform *Jobs Act*, there is no case law of the national courts dealing with the interpretation of Section 4 of the *Statuto dei Lavoratori* in its reformed wording. However, the Italian Legislator when reforming the wording of Section 4 of the *Statuto dei Lavoratori* adopted a general approach in applying the principles laid down in the established case law that had already been developed by the Court of Cassation when interpreting Section 4 before its reformed wording (i.e. before the entry into force of the reform *Jobs Act*[68]).

[68] Section 4 par. 1 ('*Audio-visual installations*') of the *Statuto dei Lavoratori*: the wording in force before the entry into force of section 23 of the reform *Jobs Act*, provided as follows:
'*It prohibited the use of audio-visual installations and of any other tool having the purpose of remote control of the activity of the employees*'.
Section 4 par. 2 of the *Statuto dei Lavoratori*, in its previous wording, provided as follows:

Therefore, even if the existing case law remains a development on Section 4 of the *Statuto dei Lavoratori* (i.e. the previous wording), current case law could provide guidance to the judiciary when dealing with questions related to such matters.

The most relevant and debated issue that has been developed in the case law of the Court of Cassation is that of the so-called 'defensive controls' ('*controlli difensivi*').
Defensive controls are a specific type of remote control that have the direct purpose of establishing illegal or unlawful conduct carried out by employees, such as criminal conduct during the performance of work contracts.
The question of compliance with a law that allows this type of control has been strongly debated. On the one hand, Section 4 par. 1 of the *Statuto dei Lavoratori* expressly prohibits the use of any tool of control that has the purpose of controlling the proper fulfilment of the work contract by the employee. However, on the other hand, the literal wording of Section 4 does not provide any legal sanction for serious misconducts carried out by employees during the course of their employment.
Initially, the Court of Cassation held that defensive controls were in any case permissible, so that guaranties provided under Section 4 of the *Statuto dei Lavoratori* would never apply to the illegal or unlawful conducts carried out by the employee during the course of their employment (Court of Cassation, judgment no 4746 of 3 April 2002).
In subsequent cases the Court of Cassation moved towards a more restrictive reading of Section 4 of the *Statuto dei Lavoratori*. The Court of Cassation held that Section 4 of the *Statuto dei Lavoratori* would apply even to defensive controls, which can only be deemed lawful when all conditions provided under Section 4 have been complied with. Thus, all the guaranties established by Section 4 of the *Statuto dei Lavoratori* must be observed by the employer.
In practice, this means that defensive controls may be deemed lawful only in cases where the employer, while carrying out surveillance activity using tools of control that have been duly installed in compliance with the guaranties and aims provided by Section 4 par. 1 of the *Statuto dei Lavoratori*, and 'occasionally' discovers the illegal conduct of the employee ('*controllo preterintenzionale*': see Court of Cassation, judgments no 4375 of 23 February 2010, no 16622 of 1 October 2012).
However, in a final development, the Court of Cassation retracted its position and held that defensive controls fall outside of the scope of Section 4 par. 1 of the *Statuto dei Lavoratori*, so that they are in any case allowed (Court of Cassation, judgment no 19091 of 17 May 2013).

Court of Cassation, judgment no 2722 ***of 23 February 2012***

In judgment no 2722 of 23 February 2012, the Court of Cassation ruled on a case that involved the inspection of the corporate e-mail account of an employee who was suspected to have revealed and disclosed confidential information regarding a client of the bank that employed her.
The Court of Cassation held, in this specific case, that the activity of control was in compliance with Section 4 of the *Statuto dei Lavoratori*, given that the control was not directly motivated towards monitoring the proper fulfilment of the employee's work duties (which is prohibited by par. 1 of Section 4), but the purpose of control was to ensure the protection of corporate assets and the public image of the bank (i.e. the fulfilment of one of the specific objective aims established by par. 1).

Court of Cassation, judgment no 10955 of 27 May 2015

'*Installations and other tools of control required by organisational and productive necessities or by the safety of the work, by means of which even the possibility of remote control of the activity of the employees is given, may be installed only in case of prior collective agreement concluded by the company-based trade unions or, in the absence of company-based trade unions, only in case of prior agreement concluded by the internal committee*'. Section 4 par. 3 of the *Statuto dei Lavoratori*, in the previous wording, provided as follows:
'*In the absence of an agreement, at the request of the employer the Labour Inspectorate shall provide for rules regarding the use of such installations in so far as is necessary […]*'.

Neither in the new nor former wording of Section 4 of the *Statuto dei Lavoratori* is there any provision that deals with the conditions and modalities of the control of the private electronic tools of the worker, such as private e-mail accounts, private *Facebook* or *Twitter* accounts and general private social media accounts, which make possible intensive types of remote surveillance on the employees.
In judgment no 10955 of 27 May 2015, the Court of Cassation ruled on a case involving an employee who spent a lot of time on *Facebook* during work hours. In order to gather evidence that the employee was not fulfilling his employment duties, the employer created a fake female *Facebook* profile, joined the *Facebook* friends list of the employee, and began chatting with him during work hours.
The Court of Cassation held, in this specific case, that the creation of a fake *Facebook* profile with the aim to control the use of social media networks during work hours was in compliance with the provisions of Section 4, given that the press that the employee was assigned to became jammed during his abandonment of his work station. Thus, the purpose of control in this situation was to ensure the safety of the workplace rather than to monitor the proper fulfilment of employment duties by the employee. Thus, the means and method of control in this case complied with the conditions provided for by Section 4.

Court of Cassation, judgment no 9904 of 13 May 2016

In judgment no 9904 of 13 May 2016, the Court of Cassation ruled on a case that involved the installation of an electronic ID badge reader that had the capabilities to detect any absence, suspension, and break in any work activity. It was also capable of immediately comparing all information that related to all the workers employed in the company.
The Court of Cassation held, in this specific case, that this type of surveillance was unlawful for the following reasons. On the one hand, this allows for the company to have direct control in overseeing the proper fulfilment of work duties by its employees, which is in itself prohibited by par. 1 of Section 4. On the other hand, the objective conditions provided for by Section 4 of the *Statuto dei Lavoratori* were not observed because any guarantees of privacy and dignity that the employee may enjoy were breached by the employer (see also judgment no 2531 of 9 February 2016 where the Court held that a remote control tool that allowed a supervisor to directly view (in real time) the computer screen of the employee was unlawful).

In conclusion, there is no case law of the national courts that specifically references the new wording of Section 4 of the *Statuto dei Lavoratori*.
However, the Italian Legislator, when reforming the wording of Section 4 of the *Statuto dei Lavoratori*, applied the general principles already established in the case law involving the interpretation of Section 4 of the *Statuto dei Lavoratori* in its previous wording.
Therefore, the existing case law could be of future assistance to the judiciary when it deals with questions relating to such matters.

II. Special legal action for the protection of privacy.

According to Section 145 of the *Privacy Code*, an aggrieved individual can lodge an application before the administrative Authority for the Protection of Personal Data (the so-called *Garante per la protezione dei dati personali*), which is empowered, *inter alia*, to hear any claim involving the violation of laws that govern the protection of personal data. This does not prejudice the individual's right to bring an action before a civil or administrative judge.
Special provisions granting specific rights are provided for in the matter of working relationships (Sections 111-116 of the *Privacy Code*), but no special procedural remedies are provided in cases where infringement of the law has occurred in the workplace.
The Decree of the Authority for the Protection of Personal Data of 1 March 2007 provides that employers and corporate supervisors may have legal access to the computers that have been supplied

to employees only when the employees have been duly and fully informed about the conditions and modalities of such access.

Judicial dialogue

Vertical interaction (European and National level)

The Court does not mention either the Charter or the GDPR but seems to bear in mind Article 9 GDPR, which provides that processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

The control activity of the employer must in any case be compatible with the principles expressed by the jurisprudence of the European Court regarding privacy. Article 8 presents a bipartite structure consisting of a first paragraph enunciating the content of the protected right and a second part that enumerates the three assumptions in the presence of which a State is entitled to subject the right to restrictions:

a) that the restriction is grounded in the law;

b) that the restriction is justified by the necessity of pursuing at least one of the legitimate purposes exhaustively listed by the law;

c) that the restriction is necessary in a democratic society.

In fact, the purpose of the control, for the protection of the rights of others, is to be considered legitimate. The restriction is founded in a law that is sufficiently accessible and predictable, being able to substitute jurisprudential interpretative guidelines. Finally, the control measure was not aimed at indiscriminately affecting the entire company staff, but was directed at a specific category of employees, public service representatives, responsible for the processing of the personal data of service users, for whose activity there is a need for highly qualified control.

The Court held that the catalogue of privacy measures at the workplace defined by the ECHR in the Barbulescu case is not exhaustive but exemplifying.

This judgment is in line with the ruling by the Court of Cassation no 4776/2007 which in a case of control over the extra-professional use of the company telephone network considered the conduct lawful as instrumental to the protection of corporate assets, as well as the sentence of the Court of Cassation no 10955/2018 concerning a case of access to an employee's personal Facebook account, considered lawful as instrumental to the protection of the security of the establishment jeopardised by the jamming of a machine that occurred during the unjustified expulsion of the worker. For these reasons, the monitoring measure must be considered proportionate according to the scope of Article 8 ECHR.

Horizontal dialogue

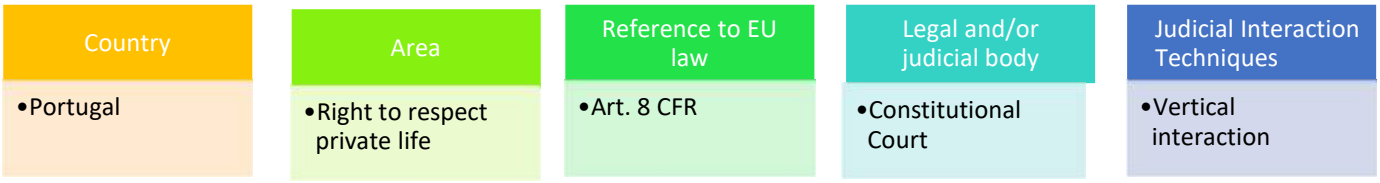
The Court undertakes a comparative analysis of the legal discipline on *automated monitoring* and *spot checks* as regards the State Parties of the ECHR.

Casesheet no 16[69] – Portugal, Tribunal Constitucional (Constitutional Court), 241/2002, 29 May 2002

Link to the full text:
http://www.tribunalconstitucional.pt/tc/acordaos/20020241.html

Core issues
Whether a court for the purpose of administering justice may order the collection of personal information from citizens who are parties to legal proceedings, even if the information collected concerns the personal data and private lives of those citizens.

At a glance



Case(s) description

Facts

A Portuguese citizen was fired from a company for allegedly divulging information on the internet. Not accepting the dismissal, he brought a case against the company in a Labour Court. For the purposes of proof, the Court ordered, based on the Portuguese Code of Civil Procedure, evidence to be collected from telecommunications operators, including information on traffic data and the detailed billing of telephone lines installed at the address of the dismissed citizen.
Article 519 of the Civil Procedure Code, in force at the time of the decision, stipulated that a person who was party to a judicial case should cooperate in the discovery of the truth by providing what was deemed necessary, unless this would cause an intrusion into private or family life.
The interpretation of the Court ordering that cooperation was that the data collected did not call into question the respect of the citizen's private life, thus the Court delivered a judgment on that basis.
In order to reverse the Court's decision, the citizen decided to appeal against that decision, stating that the evidence obtained was null and void, for violation of his right to inviolability of domicile and correspondence as well as his right to privacy.

Reasoning of the Court

The Constitutional Court firstly notes that the Constitution of the Portuguese Republic has always been concerned with the protection of citizens' private lives. This is protected both under Article 26 and in Article 34 of the Constitution. Based on these fundamental rights, the Court points out that the secrecy of telecommunications covers not only the content of such telecommunications, but also the traffic itself.

[69] This casesheet has been drafted on the basis of the template provided by Afonso Brás and Sara Azevedo

The Court recognises that there may be exceptions to the secrecy of telecommunications, particularly at the criminal level. In fact, when such a serious crime is committed on a social level, the Constitution considers that a derogation from that secrecy is warranted to guarantee social peace.
The question is whether this derogation is also justified when a public interest in the administration of justice is at stake. Here, the Constitutional Court considers and denies that understanding, concluding that it is not therefore lawful to extend that restriction based on this argument. Because of this understanding, and in the light of the present case, the Court considers that the invoice of a telecommunication contract include personal data of the citizen concerned, thus violating his right to the protection of privacy and the protection of personal data. Therefore, the Court concludes that the interpretation given to Article 519 of the Portuguese Civil Procedure Code by the judge of the Labour Court, in the sense that while it may be requested in labour proceedings, by judicial order, from telecommunication operators, information on traffic data and detailed invoicing of telephone line installed at the address of a party is unconstitutional.

Analysis

Role of the Charter

On the date that the decision of the Constitutional Court was given, the CFR, although it had already been adopted, still had no binding force. It is therefore understandable that the Court did not refer to it. Even so, the Court refers to Directive 46/95/EC on data protection. If the Charter were already binding, then Articles 7 and 8, with respect to private life and personal data, would certainly be referred to.

There is therefore no direct relation between the case and the CFR, and the Court only considers the possible rights breached from a national perspective, although it is influenced by supranational legal instruments, namely Directive 46/95/EC.

Judicial dialogue

Vertical interaction

What is at stake in this case is a constitutional review of a lower judicial decision.

In Portugal, the Constitutional Court is the only competent Court to assess the possible unconstitutionality of rules. If in a judicial proceeding in a lower court the constitutionality of a rule applicable to the specific case is raised, the lower court must refer the case to the Constitutional Court for it to adjudge such unconstitutionality. In this case, we are faced with an appeal against a lower court judgment, inasmuch as that unconstitutionality was only alleged later. As far as the question of the conformity of a provision with the Constitution is concerned, it is only the Constitutional Court, which is the last court of appeal, that can decide.
In the present case there was a constitutional revision of a sentence because of an interpretative divergence.
In fact, the lower court interpreted Article 519 of the Portuguese Code of Civil Procedure in such a manner as to allow the court to order the collection of information and personal data of one of the parties in a judicial case decided in a Labour Court, even if such information derives from the private life of that party.
The Constitutional Court, on the other hand, took the view that such an interpretation violates the Constitution because the interest in the administration of justice cannot be a valid justification for derogating from a restriction that only yields to serious cases such as a crime that affects social peace.

Thus, by resolving this interpretive conflict, the Court established as unconstitutional the interpretation given by the lower court. Since we are talking about the Constitutional Court, which is the last and most important court in Portugal, this understanding has become definitive, obliging all lower courts to respect it.
We can therefore affirm that the interpretation of the Constitutional Court is in accordance with the provisions of Articles 7 and 8 of the CFR, being an interpretation consistent with this Charter and ensuring effective protection of those rights, thus complying with the purposes of the CFR.

Part III - Hypotheticals

This part is dedicated to the hypotheticals drawn from the case law addressed in the previous parts. The hypotheticals include reference to legislation and case law as well as provocative questions that will be used as a trigger discussion during the residential training event.
It is important to highlight that the purpose of the hypotheticals is to give the trainees a chance to critically analyse the provisions of their own legal system as regards the fields covered in the Handbook and to verify their compliance vis-à-vis the standard of protection of fundamental rights guaranteed by the EU Charter. Thus, the scenarios presented in each of the hypotheticals do not entail a 'correct' answer; rather they provide for different answers and will (hopefully) trigger new questions and doubts that will improve the level of protection of fundamental rights at a national as well as European level.

The hypotheticals address in particular:

1. The territorial scope of the EU data protection law and data transfers to third countries
2. The lawful processing: special categories of data and automated process
3. The balance of interests: data protection v data retention

Hypothetical no 1 – Territorial scope of the application of EU data protection law

General Data Protection Regulation

Article 3 Territorial Scope

1. This Regulation applies 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.
2. This Regulation applies to the processing of the personal data of data subjects in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.

Article 49

Derogations for specific situations

1. In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject, due to the absence of an adequacy decision and appropriate safeguards;
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
(d) the transfer is necessary for important reasons of public interest;
(e) the transfer is necessary for the establishment, exercise or defence of legal claims;
(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

Third country

Definition:

A natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

GDPR: rec 47, 69; Arts 4.9, 4.10, 6(1)(f), 13(1)(d), 14(2)(b)

Guidelines for trainers:

This hypothetical is based on the section regarding the scope of the GDPR (p. 14 ff.) and Casesheet no 4.
The objective of the hypothetical is the analysis of useful criteria for the judges and lawyers in assessing the territorial application of the GDPR regardless of the fact that the controller is an EU entity.

Please pay attention to the objective criteria provided by Article 3 GDPR

<u>*Level I*</u>
A is a non-EU entity which has an office in an EU Member State that does not carry out any processing activities itself but develops customer relationships and acquires a considerable number of clients for the entity and, thus, has a large share in the economic success of the entity.

Level I.A - Lawyers
A is the controller of the processing of personal data (collected in the EU) as it stores customer data. A has its establishment in France. Thus, A is carrying out the data processing of its customer data in the context of the activities of its French (and thus EU) establishment. Nonetheless, as A has a large customer base, it accumulates a large amount of customer data. Therefore, A stores the customer data in a cloud service operated by US entity B.

Guidelines for trainers:

Level I.A addresses the fact that data processing implies also a data transfer to third countries. Please reflect on whether the activity of storage in a foreign cloud service may imply also a data transfer to third countries or if the application of Article 3 is sufficient.

You are asked to play the role of the lawyer representing A before the First Instance Court.

1. Does the GDPR apply to non-EU entities?
2. Which arguments would you use to justify the idea that the purposes and means of the processing are determined by B?
3. How could you demonstrate that the processing is carried out in the context of A's and not B's activities?

Level I.b – Judges
Mr Bean lodged a complaint before the local First Instance Court, requesting the removal of the cache copies stored within A's and B's repositories.
He argued that inclusion of data regarding himself in the cache copies located in the US can hardly be considered of public interest.
He lodged a complaint arguing that the presence of a permanent organisation, such as A France, represents that stable and concrete connection with the Italian territory, which justifies the application of the GDPR to his case.

You are asked to play the role of the First Instance Court.

1. Is the development of customer relationships to be framed within the concept of establishment[70]?
2. Which indices do you use to assess the targeting of EU individuals?
3. Would you balance the underlying interest of Mr Bean's request with any other rights?
4. Which ECJ case-law do you bear in mind?

Guidelines for trainers:

Level I addresses similar questions to those posed in the case of Google Spain, requiring the trainees to determine whether the definition of establishment may justify the presence of permanent organisation or whether the activity of targeting EU individuals can be considered on the basis of any indices.

Level II
[Similar facts – different defendant]
Mr Bean is a Moroccan and lodges a complaint arguing that the data processing has also been carried out by B in the US.

Level II.a – Lawyers
Mr Bean consulted a lawyer as regards the possible avenues by which to request not only the erasure of his data but also damages for a data protection breach.
You are asked to play the role of the lawyer representing Mr Bean before the court.

1. Which further arguments do you use to argue for the applicability of the GDPR?
2. Can the territorial scope of the GDPR be analysed in connection with other relevant provisions of the GDPR?
3. What would be the advantages for taking into account the discipline of data transfers to third countries?
4. Which ECJ case law should you bear in mind?

Guidelines for trainers:

Level II addresses the issue of subjective requirements. If data processing has been carried out also in thr US by B, trainers are required to assess how many processings have been carried out.

[70] An example included in the Guidelines 3/2018, p. 8 mentions as follows: 'A pharmaceutical company with headquarters in Stockholm has located all its personal data processing activities with regards to its clinical trial data in its branch based in Singapore. According to the company structure, the branch is not a legally distinct entity and the Stockholm headquarters determines the purpose and means of the data processing carried out on its behalf by its branch based in Singapore.'

Level II.b – Judges
Mr Bean requested an injunction in front of the same court so as to block the availability of the cache copies on the webpages of search engine A, on the grounds of the right to be forgotten, requesting that A be responsible also for deleting all other cache copies stored in B.
You are asked to consider issuing an injunction.

Guidelines for trainers:

Level II addresses the specific issue of the territorial or non-application of the right to be forgotten. Please bear in mind Casesheet no 4.

1. Would you apply the GDPR directly?
2. In your reasoning would you refer to the Charter in order to give more emphasis to your arguments?
3. Which criteria would you use in order to evaluate the request of Mr Bean?
4. Which decision would you provide in order to ensure a proportionate remedy to the claimant?
    a. In case you decide in favour of Mr Bean, would you extend the delisting only to the national context or would you evaluate under which conditions the delisting may be extended worldwide?
    b. Would you take into account the Opinion of the Advocate General Szpunar released on 10 January 2019 in Case C-507/17 and the subsequent judgment of the Grand Chamber of 24 September 2019, which stated that '**where a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request.**'

<u>*Level III*</u>
[Follow up of previous facts]
The First Instance Court issues the injunction to delist the result and extended also to the cache copies stored in B. A complies with the injunction, but B does not. B argues that the GDPR does not apply to data processing conducted in third countries.

Guidelines for trainers:

Level III addresses the specific situation in which the injunction to delete cache copies has an extraterritorial effect. Please reflect on whether the argument that data transfer to third countries may be useful in fostering the application of the GDPR to the case, considering that most probably Mr Bean gave his consent to the 'data transfer'.

Level III.a – Lawyers
You are asked to play the role of the lawyer representing Mr Bean before the court.
1. Which arguments would you use to support the position of Mr Bean?

2. Would you deem it relevant to qualify data processing in third countries rather than data transfer to third parties?
3. Does the consent given by Mr Bean play any role?

Guidelines for trainers:

Level III addresses the issue of judicial interaction techniques as possible solutions for analysing the complexity of the case.

Level III.b – Judges
You are asked to play the role of the court receiving the challenge.

1. Would you consider the request not to apply EU law legitimate?
2. Which criteria would you use in order to distinguish between data processing in third parties and data transfer to third parties?
3. Which type of judicial techniques would you use to decide the case?
4. Should you refer any questions to the ECJ for a preliminary ruling, which questions would you address?[71]

[71] The first question referred to in Case C-362/2014 *Maximilan Schrems* v *Data Protection Commissioner* was: 'Whether in the course of determining a complaint which has been made to an independent office holder who has been vested by statute with the functions of administering and enforcing data protection legislation that personal data is being transferred to another third country (in this case, the United States of America) the laws and practices of which, it is claimed, do not contain adequate protections for the data subject, that office holder is absolutely bound by the Community finding to the contrary contained in [Decision 2000/520] having regard to Article 7, Article 8 and Article 47 of [the Charter], the provisions of Article 25(6) of Directive [95/46] notwithstanding?'

Hypothetical no 2 – Lawful processing and racial data

General Data Protection Regulation

Article 6 Lawful Processing (par.1)

Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of the official authority vested in the controller;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Article 9 Special categories of data (par.1, par. 2 (*a* - *b*)

1. 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.

2. 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;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State

law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(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;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 22 Automated Processing

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

3. In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

4. Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in Article 9(1), unless point (a) or (g) of Article 9(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION

Article 7 Protection of personal data

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 21 Non-discrimination

1. Any discrimination based on any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited.

2. Within the scope of application of the Treaty establishing the European Community and of the Treaty on European Union, and without prejudice to the special provisions of those Treaties, any discrimination on grounds of nationality shall be prohibited.

Guidelines for trainers:
This case will address the relationships between lawful processing and personal data. If useful, you can read this case together with Casesheets no 13, 14 and 15 and compare different factual and legal situations.

Level I
Mrs Doubtfire is a Bangladesh citizen and she would like to sign a life insurance contract with an EU insurance company. The insurance company requires the consent of the data subject for the purposes of the data processing.
After the scrutiny phase, Mrs Doubtfire is denied the life insurance.

Guidelines for trainers:
Please reflect on a few elements such as the nationality of the data subject or elements which could be related to racial discrimination. Are these elements sufficient in order to take a position or is it necessary to resort to the relevance of her consent in order to argue in favour or against Mrs Doubtfire? The defensive strategy is relevant. However, the easiest way to obtain a judicial remedy should be chosen.

Level I.A - Lawyers

You are asked to play the role of the lawyer representing Mrs Doubtfire before the First Instance Court.

1) Which legal arguments do you use to lodge a complaint against the insurance company?
2) Which are the variables that you take into account in preparing your defensive strategy?
3) Is the consent given by Mrs Doubtfire sufficient for data processing?

Level I.b – Judges

You are asked to play the role of the First Instance Court.

1) Which legal provisions would you apply?
2) Accordingly, how would you use the reference to the Charter?

Level II
[Similar facts – more details]

Guidelines for trainers:
This level includes the issue of automated processing. Please consider whether or not the consent may act as a waiver for the processing of racial data.

Mrs Doubtfire provides a specific consent to the processing of her racial data. The insurance company after analysing her dossier denies the life insurance on the basis of the low income she is in receipt of, according to her employment contract, which makes her not eligible for life insurance.
Nonetheless the decision was based solely on automated processing including profiling.

Level II.a – Lawyers

1) How can you demonstrate that data processing is discriminatory?
2) Is the application of the GDPR sufficient to make such an assessment or could it be useful to apply other legal provisions?
3) How could you trigger the application of a judicial technique which takes into account the consistent interpretation of the Charter?

Guidelines for trainers:
You should consider if the data processing carried out by the insurance company is based on racial data or other categories of data. Briefly, Mrs Doubtfire gives her consent for the processing of her racial data, but the decision to reject her request is apparently based on other grounds, such as the low income she receives according to her employment contract.

Level II.b – Judges

1) On which basis could you propose a preliminary ruling to the ECJ?
2) Given your national legal framework, which question could you refer to the Court?

Level III

[Follow up of previous facts]

Mrs Doubtfire challenges the data processing, arguing that her consent was specific for the data processing of particular categories of data but not for the automated processing.

Guidelines for trainers:
Is there perhaps a lack of clarity in Article 22 GDPR, which allows further steps? Are the exceptions provided by Article 9 GDPR applicable to the automated data processing? If not, can it be argued that the insurance company carried out a lawful processing?

Level III.a – Lawyers

You are asked to play the role of the lawyer representing Mrs Doubtfire before the court.

1) Which legal provisions of the GDPR do you use to support the arguments on unlawful processing?
2) Would you argue that the limitations provided by Article 22 GDPR do not apply to the exceptions set forth by Article 9 GDPR?

Level III.b – Lawyers

You are asked to play the role of the lawyer representing the insurance company before the court.

1) How do you argue for the lawful processing?

Level III.b – Judges

You are asked to play the role of the court receiving the challenge.

1) Which European case law could you use to assess if discriminatory practices may be based also on data processing of non-racial data?
2) How could the use of the Charter influence the assessment of a discriminatory practice through unlawful data processing?

Hypothetical no 3[72] – Balance of conflicting interests: data protection and law enforcement

Charter of Fundamental Rights of the European Union

Article 7 Respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 8 Protection of personal data

Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

Article 52

1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.
2. Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties.
3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.
4. In so far as this Charter recognises fundamental rights as they result from the constitutional traditions common to the Member States, those rights shall be interpreted in harmony with those traditions.
5. The provisions of this Charter which contain principles may be implemented by legislative and executive acts taken by institutions, bodies, offices and agencies of the Union, and by acts of Member States when they are implementing Union law, in the exercise of their respective powers. They shall be judicially cognisable only in the interpretation of such acts and in the ruling on their legality.
6. Full account shall be taken of national laws and practices as specified in this Charter.
7. The explanations drawn up as a way of providing guidance in the interpretation of this Charter shall be given due regard by the courts of the Union and of the Member States.

[72] This hypothetical is modelled on the basis of *Miniterio Fiscal*, Case C-207/16 decided on 2 October 2018 (ECLI: EU: C: 2018: 788).

Article 2 GDPR (par. 1 & 2) Material scope

1. This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

2. (a) (b) (c) (d)

This Regulation does not apply to the processing of personal data:
in the course of an activity which falls outside the scope of Union law;
by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU; by a natural person in the course of a purely personal or household activity; by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Article 15 Directive 58/2002/EC (par. 1)
Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.

Article 8 European Convention of Human Rights
Right to respect for private and family life

1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Guidelines for trainers:
This hypothetical has been drafted on the basis of the section on the balance of data protection with other fundamental rights and interests (p. 28) and Casesheet no 8.

Level I

Mr de Villaloba lodged a complaint with the police for a robbery during which his wallet and mobile telephone were stolen. Afterwards, the police requested the investigating magistrate to order various providers of electronic communications services to provide (i) the telephone numbers activated at that time with the identity code of the stolen mobile telephone and (ii) the personal data relating to

the identity of the owners or users of the telephone numbers corresponding to the SIM cards activated with the code, such as their surnames, forenames and, if need be, addresses. Nonetheless, the investigating magistrate refused that request, deeming it as not necessary to identifying the perpetrators of the offence and not dealing with serious offences. The Public Prosecutor's Office appealed against that order before the referring court, claiming that communication of the data at issue ought to have been allowed by reason of the nature of the facts. The referring court explains that the State's interest in punishing criminal conduct cannot justify disproportionate interferences with the fundamental rights enshrined in the Charter. In that regard, the referring court considers that, in the main proceedings, the GDPR and Directive 2002/58 establish a link with the Charter.

Guidelines for trainers:
Level I addresses the issue of limits to data retention. It immediately recalls the ECJ case law on data retention launched by the case Digital Rights and followed up by Tele 2 Sverige/Watson and Ministerio Fiscal.

Level I.A - Lawyers

You are asked to play the role of the lawyer representing Public Prosecutor's Office before the First Instance Court.

1) Which legal arguments do you use to lodge a complaint against the data retention?
2) Is the concept of serious offence relevant to the legitimacy of the retention?
3) Which relevant EU case law would you use in your reasoning?

Level I.b – Judges
You are asked to play the role of the First Instance Court.

1) Do you consider referring for a preliminary ruling to the ECJ?
2) If yes, which questions would you refer to the ECJ?
3) How do you balance the protection of Articles 7 and 8 as enshrined in the Charter with the prosecution of serious crime, in light of Article 52 of the Charter?

<u>*Level II*</u>
[Similar facts – different object of the complaint]
After a while, Mr de Villaloba lodged a complaint for unlawful processing, arguing that his right to data protection has been undermined by data retention techniques.

Guidelines for trainers:
Please, consider taking into account the following standpoints in your reasoning:

- ***General access to all retained data, regardless of whether there is even an indirect link with the intended purpose, cannot be regarded as limited to what is strictly necessary;***
- ***Access can only be granted to the data of individuals suspected of planning, committing or having committed a serious crime or of being implicated in one way or another in such a crime.***
- ***Access to the data of other persons may also be justified where there is objective evidence that the data might, in a specific case, make an effective contribution to combating such activities;***
- ***It is essential that access should as a general rule, except in cases of validly established urgency, be subject to prior review carried out either by a court or by an independent administrative body;***
- ***A person whose data has been accessed must be notified as soon as that notification is no longer liable to jeopardise any investigations. That notification is necessary to enable the persons affected to exercise, inter alia, their right to a legal remedy.***

Level II.a – Lawyers
You are asked to play the role of the lawyer representing Mr de Villaloba before the First Instance Court .

1) How do you try to demonstrate that data retained do not concern national security?
2) Which criteria do you use to argue that the data processing has been unlawful?
3) How could you trigger the application of a judicial technique which takes into account the consistent interpretation of the Charter?

Level II.b – Judges
You are asked to play the role of the First Instance Court.

3) On which basis could you propose a preliminary ruling to the ECJ?
4) Should you refer any questions to ECJ for a preliminary ruling, would you rely on the question referred in the so-called 'Schrems II Case?'[73]

Level III
Follow up of previous facts

Mrs de Villaloba fails in achieving restoration under unlawful processing and brings the matter before the ECtHR for violation of the right to private life.

Level III.a – Lawyers
You are asked to play the role of the lawyer representing Mrs de Villaloba before the ECtHR.

3) Which arguments do you develop in order to include data protection within Article 8 ECHR?
4) Which ECtHR case law do you rely on?

Level III.b – Judges
You are asked to play the role of the ECtHR.

1) How would you interpret the linkage with mass surveillance case-law and in particular with Cases *Zacharov* v *Russia* (Application n. 47143/06 - Judgment 4 December 2015) and *Szabo and Vissy* v *Hungary* (Application n. 37134/14 - Judgment 12 January 2016)?
2) How could you develop horizontal interaction by using the Charter in connection with the ECHR?

Guidelines for trainers:
The following notes could be useful in inspiring your comparative reasoning[74].

[73] The first two questions referred in Case C-311/18 are the following: 'In circumstances in which personal data is transferred by a private company from a European Union (EU) member state to a private company in a third country for a commercial purpose pursuant to Decision 2010/87/EU[1] as amended by Commission Decision 2016/2297[2] ('the SCC Decision') and may be further processed in the third country by its authorities for purposes of national security but also for purposes of law enforcement and the conduct of the foreign affairs of the third country, does EU law (including the Charter of Fundamental Rights of the European Union ('the Charter')) apply to the transfer of the data notwithstanding the provisions of Article 4(2) of TEU in relation to national security and the provisions of the first indent of Article 3(2) of Directive 95/46/EC[3] ('the Directive') in relation to public security, defence and State security? (1) In determining whether there is a violation of the rights of an individual through the transfer of data from the EU to a third country under the SCC Decision where it may be further processed for national security purposes, is the relevant comparator for the purposes of the Directive: The Charter, TEU, TFEU, the Directive, ECHR (or any other provision of EU law); or the national laws of one or more member states?'

[74] See Factsheet – Mass surveillance, February 2019, available at https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf.

The case of Zacharov* v *Russia

4 December 2015 (judgment – Grand Chamber)

This case concerned the system of the secret interception of mobile telephone communications in Russia. The applicant, an editor-in-chief of a publishing company, complained in particular that mobile network operators in Russia were required by law to install equipment enabling law enforcement agencies to carry out operational search activities and that, without sufficient safeguards under Russian law, this permitted blanket interception of communications.

The Court held that there had been a violation of Article 8 of the Convention, finding that the Russian legal provisions governing interception of communications did not provide for adequate and effective guarantees against arbitrariness and the risk of abuse which was inherent in any system of secret surveillance, and which was particularly high in a system such as that in Russia where the secret services and the police had direct access, by technical means, to all mobile telephone communications. In particular, the Court found shortcomings in the legal framework in the following areas: the circumstances in which public authorities in Russia are empowered to resort to secret surveillance measures; the duration of such measures, notably the circumstances in which they should be discontinued; the procedures for authorising interception as well as for storing and destroying the intercepted data; the supervision of the interception. Moreover, the effectiveness of the remedies available to challenge the interception of communications was undermined by the fact that they were available only to persons who were able to submit proof of interception and that obtaining such proof was impossible in the absence of any notification system or possibility of access to information about interception.

The case of Szabó and Vissy* v *Hungary

12 January 2016 (judgment)

This case concerned Hungarian legislation on secret anti-terrorist surveillance introduced in 2011. The applicants complained in particular that they could potentially be subjected to unjustified and disproportionately intrusive measures within the Hungarian legal framework on secret surveillance for national security purposes (namely, 'section 7/E (3) surveillance'). They alleged that this legal framework was prone to abuse, notably for want of judicial control.

In this case the Court held that there had been a violation of Article 8 of the Convention. It accepted that it was a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies, including massive monitoring of communications, in pre-empting impending incidents. However, the Court was not convinced that the legislation in question provided sufficient safeguards to avoid abuse. Notably, the scope of the measures could include virtually anyone in Hungary, with new technologies enabling the Government to intercept masses of data easily, concerning even persons outside the original range of operation. Furthermore, the ordering of such measures was taking place entirely within the realm of the executive and without an assessment of whether interception of communications was strictly necessary and without any effective remedial measures, let alone judicial ones, being in place. The Court further held that there had been no violation of Article 13 (right to an effective remedy) of the Convention taken together with Article 8, reiterating that Article 13 could not be interpreted as requiring a remedy against the state of domestic law.