FRICoRe

Judicial Training Project

Fundamental Rights In Courts and Regulation

CASEBOOK

EFFECTIVE DATA PROTECTION AND FUNDAMENTAL RIGHTS

COUR DE JUSTIC
DE L'UNION

SSM

Scuola Superiore della Magistratura

UNIVERSITY OF TRENTO

THIS PUBLICATION IS FUNDED BY THE EUROPEAN UNION'S JUSTICE PROGRAMME (2014-2020)

Effective Data Protection and Fundamental Rights

Edited by Paola Iamiceli, Fabrizio Cafaggi, Chiara Angiolini

Publisher: Scuola Superiore della Magistratura, Rome – 2022

ISBN 9791280600271

Published in the framework of the project:

Fundamental Rights In Courts and Regulation (FRICoRe)

Coordinating Partner:

University of Trento (*Italy*)

Partners:

Scuola Superiore della Magistratura (*Italy*)

Institute of Law Studies of the Polish Academy of Sciences (INP-PAN) (*Poland*)

University of Versailles Saint Quentin-en-Yvelines (*France*)

University of Groningen (*The Netherlands*)

Pompeu Fabra University (*Spain*)

University of Coimbra (*Portugal*)

Fondazione Bruno Kessler (*Italy*)

The present Casebook builds upon the ReJus Casebook - Effective Justice in Data Protection. In particular, new streams of questions have been added (specifically in chapters 1, 3, 4, 5, 7, 9). Furthermore, new developments have been considered both in EU and national caselaw.

Edition: May 2022

Scientific Coordinator of the FRICoRe Project:

Paola Iamiceli

Coordinator of the team of legal experts on Effective Data Protection:

Paola Iamiceli

Project Manager:

Chiara Patera

Co-editors and Co-authors of this Casebook:

Co-editors: Paola Iamiceli (Project Coordinator), Fabrizio Cafaggi, Chiara Angiolini

Introduction: Fabrizio Cafaggi and Paola Iamiceli

Ch. 1: Sandrine Clavel, Fabienne Jault-Seseke

Ch. 2: Sandrine Clavel, Chiara Angiolini

Ch. 3: Sandrine Clavel, Mateusz Grochowski

Ch. 4: Chiara Angiolini

Ch. 5: Sandrine Clavel, Mateusz Grochowski

Ch. 6: Chiara Angiolini, Sandrine Clavel, Federica Casarosa, Maria Magierska

Ch. 7: Chiara Angiolini, Sandrine Clavel, Fabienne Jault-Seseke, Paola Iamiceli, Katarzyna Południak-Gierz

Ch. 8: Sandrine Clavel, Mateusz Osiecki

Ch. 9: Chiara Angiolini, Sébastien Fassiaux

Note on national experts and contributors:

The FRICoRe team would like to thank Olga M. Ceran for her support in the initial design of the addressed questions and the chapters' editing, and all the judges, experts, and collaborators who contributed to the project and to this Casebook by suggesting national and European case law *(in alphabetical order)*

Chiara Tea Antoniazzi *
Marc Bosmans
Roberta Brusco*
Luigi Cannada Bartoli*
Francesca Capotorti*
Stefano Caramellino*
David Castillejos Simon*
Mélanie Clément-Fontaine*
Aurelia Colombi Ciacchi
Jarosław Czarnota*
Krystyna Dąbrowska
Fiorella Dal Monte*
Silvia Dalle Nogare*
Nicole Di Mattia*
Carmen Domocos*
Lorette Dubois*
Rossana Ducato
Malte Engeler*
Martina Flamini*
Andrea Maria Garofalo
Florence Gaullier*
Inès Giauffret
Karin Kieffer*
Maud Lagelée-Heymann
Lottie Lane
Sandra Lange
Maria Teresa Leacche*
Tobias Nowak
Isabella Oldani*
Aniel Pahladsingh
Charlotte Pavillon
Simon Peers
Romain Perray*
FrancescoPerrone
Piotr Polak
Lyubka Petrova
Gianmatteo Sabatino*
Pedro Santos Azevedo
Wojciech Sawczuk*
Markus Thoma
Sil van Kordelaar
Lavinia Vizzoni*
Margaux Voelckel*
Anne Witters
Célia Zolynski
The students of Master PIDAN* (UVSQ/Sacla)

*: contributors in the framework of the RE-Jus project

Table of Contents:

Introduction: A Brief Guide to the Casebook

Cross-project methodology

The FRICoRe Casebook on *Effective Data protection and fundamental rights* builds upon the collaborative venture developed in previous projects of judicial training and, more recently, in the Re-Jus project. The core element of its methodology concerns the active dialogue established between **academics and judges of various European countries** on the role of the Charter and that of its article 47, here particularly developed in the field of data protection law. In continuity with previous projects, including Re-Jus, this collaboration combines rigorous methodologies with judicial practices, and provides the trainers with the sort of rich comparative material that should always characterise transnational trainings. Training includes not only the transfer of knowledge, but also the creation of a learning community composed of different professional skills. Like in a previous experience, this casebook is due to evolve both in content and in method over time, with additional suggestions arising from its use in training events.

We firmly believe that transnational training of judges should be based on a rigorous analysis of **judicial dialogue** between national and European courts and, when existing, among national courts. In the field of data protection, such dialogue often builds upon or runs next to the activity of national administrative authorities, individually or as coordinated within the European Data Protection Board in which they are grouped. Although the administrative authorities may not refer questions to the Court of Justice, their decisions may be challenged before the courts or they may themselves bring an action before a court under the current legislation. Moreover, the CJEU is competent for deciding upon the validity of the Board's decisions when challenged by a natural or a legal person concerned by it under Article 263 TFEU, or when the validity question is referred by a national court pending a proceeding in which that decision needs to be applied (recital 143 of the General Data Protection Regulation, hereinafter GDPR).

Like in previous projects, judicial dialogue is a key dimension of the approach followed in this Casebook. We investigate the full life cycle of a case, from its birth with the preliminary reference, to its impact in different Member States. We examine the ascendant phase and analyse how the preliminary reference is made, and whether and how it is reframed by the Advocate General and the Court. We then analyse the judgments and distinguish them according to the chosen degree of detail when they provide guidance both to the referring court and to the other courts that have to apply the judgments in the various Member States. Although the analysis does not extend to all Member States, compared with the Re-Jus Casebook on Data Protection, a larger set of national caselaw has been considered in this edition.

Indeed, judicial dialogue develops both vertically and horizontally, at both national and supranational levels. Preliminary references represent the main driver of this dialogue. Linked with preliminary references procedures, horizontal interaction among national courts takes place when the principles identified by the Court of Justice of the European Union (hereinafter CJEU) are applied in pertinent cases, mostly in the same and sometimes in connected fields. Also depending on the type of reference enacted, the guidance provided by the CJEU may consist in specific rules or in general principles to be applied. Very frequently the latter may consist in the principle of effectiveness or the one of equivalence, due to be balanced against the principle of national procedural autonomy.

Diverging approaches may be provoked by the same CJEU's judgement and a national vertical dialogue may emerge, involving constitutional courts, higher courts and first instance courts.

The horizontal dimension of this dialogue may be observed only indirectly when, starting from the same decision of the Court of Justice, possibly different outcomes are examined in different Member States.

Whereas by its intrinsic nature the European Data Protection Board provides an opportunity for coordination, cooperation and consistency among the national administrative authorities, the same framework does not exist for national courts. Moreover, although the 95/46/EC directive and now the General Data Protection Regulation (2016/679/EU Regulation., hereinafter GDPR) have provided a common legal framework for all Member States, the impact of such legislation upon national caselaw is still diversified, particularly so when the right to data protection needs to be balanced against other fundamental rights such as the right of expression and the one to information (CJEU, C-507/17, *Google CLL v. CNIL, para. 67*). The impact of EU caselaw on delisting (*Google Spain*, C-131/12; *CG and Others*, C-136/17, *Google c. CNIL,* C-507/17) is a good example. On the one side, cross-national convergences (*e.g.,* in French, Italian and Polish decisions) may be observed when delisting is considered an adequate and proportionate remedy to strike a balance between data protection and the freedom of expression (being, *e.g.*, the right to press untouched). On the other side, in some legal systems, national judges may struggle more than their colleagues in other Member States in reconciling the right to be delisted with the rules on protection of personality rights (*e.g.,* this is the case for Poland). Furthermore, national judges may develop different approaches regarding the degree of activism expected by search engines, social networks and host providers in removing unlawful contents from the internet, although this is still a largely debated issue (see *Glawischnig-Piesczek,* C-18/18, and some applications in Italy and France in chapter 8 of this Casebook)

Comparing different stories, taking into account national specificities, enables national courts, different from the referring ones, to better anticipate the impact of EU law on the adjudication of national cases. This is why the **comparative perspective** provided by this Casebook may clarify the impact of the judgment or of a cluster of judgments addressing the same issue (for example *ex officio* power to examine unfairness of contract clauses) on the case law of Member States different to that of the referring court. In some cases, the impact can be examined through judgments expressly referring to the CJEU's decisions; in other cases, the Casebook suggests interpretative tools to address issues discussed in national case law through the lens of the CJEU's decision. The **impact analysis** is very important for judges other than the referring one. Their effort to interpret and to adapt the judgment to their national legal context is often underestimated. While formally the CJEU judgments are binding on Member State courts, their application requires a careful analysis of which substantive and procedural rules may be affected by the judgment, in particular the application of Article 47 of the Charter and the principle of effectiveness.

Based on the methodology adopted in Re-Jus and now in Fricore, the analysis does not focus on single CJEU judgments but on **clusters of judgments** around common issues. Often, CJEU judgments touch on many questions depending upon how the preliminary references are framed, and it might be more effective to choose a subset of complementary issues and examine them in sequence across several cases, rather than to focus on a single judgment. This approach may add a bit of complexity, but it reflects the problem-solving approach, rather than the conventional doctrinal perspective. The internal coordination of chapters ensures the possibility of reconstructing the judgment across different chapters.

The casebook is complemented by a Database (https://www.fricore.eu/content/database-index) that endorses the methodological approach of judicial dialogue, giving continuity to the one established in the Re-Jus Project and integrating the whole set of materials developed therein. It is organised around EU judgments and their impact on national legal systems. Two series of national judgments are examined in the Database: those directly concerning cases brought before the CJEU within a preliminary reference procedure, and those that apply or take into consideration the CJEU case law when addressing national

cases outside of a referral procedure. Hence, the database is specific, and it reflects the idea that judicial dialogue is a pillar of EU law.

We would like to encourage both the use of the Casebook and that of the Database in training courses organised by national schools, which is subject to constant updating during the course of the project, thanks to contributions coming both from the Schools of the Judiciary and from the workshops' participants.

The main issues addressed in this Casebook

Building on the Re-Jus Casebook on *Effective Data Protection*, the Fricore Casebook aims at examining the impact of the EU Charter of Fundamental Rights (hereinafter CFREU) on the EU and national caselaw in the field of data protection from the perspective of the judicial dialogue occurred between the Court of Justice, national courts and, only indirectly, data protection authorities.

Largely based on EU secondary legislation (95/46/EC directive and now the GDPR), this dialogue has in fact developed a fundamental right perspective based on articles 7 and 8 of the Charter more and more (*e.g., Schrems I*, C-362/14; *Facebook Ireland Ltd, Maximillian Schrems*, C-311/18). In some cases, the dialogue incorporates the framework established in the European Convention of Human Rights and, more particularly, in its Article 8 (*e.g.*, in *Digital Rights Ireland,* Joined Cases C-293/12 and C-594/12).

How is the role of national judged in protection affected by the acknowledgment of fundamental rights at EU level and to what extent?

Firstly, unlike in other domains of EU law, in the field of data protection the Charter goes well beyond the acknowledgment of a fundamental right. Indeed, not only does Article 7 and, more particularly, Article 8 CFREU, establish the pillars of data protection regulation regarding the principles of fairness, lawfulness and finality, also expanded in secondary legislation, but they also define the bases for an effective enforcement; more particularly, Article 8 does so when recognising, on the one hand, the right to access and that of data rectification and, on the others, the monitoring power of an independent authority.

Secondly, since fundamental rights are at stake, Article 52 CFREU, shall be applied, meaning that any limitation on the exercise of such rights must be provided for by law and respect the essence of those rights and freedoms and shall be subject to the ***principle of proportionality***, therefore 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. What the impact of this principle on the judicial dialogue between EU and national courts in the field of data protection comes to, is widely clarified along this Casebook (see part. *Puškár*, C-73/16, ch. 8 with regard to the procedural aspects of the right to an effective remedy in data protection; *Digital Rights Ireland,* C-293/12, and C-594/12 and *LaQuadratureDuNet,* C-511/18, C-512/18; C-520/18, ch. 3 with regard to the limitation of fundamental rights in case of data processing carried out by States for the purpose of protecting public security; *Asociaţia de Proprietari*, C-708/18, ch. 4, with regard to the interpretation of the legal basis of the legitimate interest in light of Articles 7, 8 and 52 CFREU).

Thirdly (and this is the focus of the present Casebook), since data protection is regulated at EU level, another fundamental right comes into play, namely, the ***right to an effective remedy and a fair trial*** under Article 47 CFREU. Although the latter is seldom explicitly recalled in EU caselaw, its relevance cannot be denied in this dialogue (see, *e.g.*, *Schrems*, C-362/14; *Facebook Ireland and Schrems*, C-311/18; *Puškár*, C-73/16). The right to an effective judicial protection is more often referred to in the framework

of the principle of effectiveness (*e.g.*, *Promusicae*, C-275/06; *Google v. CNIL* C-507/17; *Rijkeboer*, C-553/07; *C-40/17, Fashion ID*). Although Article 47 CFREU does not apply directly to administrative authorities, referred to as judicial protection (including judicial review of administrative authorities' decisions), its impact extends to the (effective and sincere) cooperation among data protection authorities in cross-border cases, as recently shown by the CJEU (C 645/19, *Facebook Ireland Ltd*).

The right to an effective remedy does not only play a role within individual redress proceedings, but also in the context of **collective redress**. As the CJEU has recently observed, "[a]uthorising consumer protection associations (…) to bring, by means of a representative action mechanism, actions seeking to have processing contrary to the provisions of that regulation brought to an end, independently of the infringement of the rights of a person individually and specifically affected by that infringement, undoubtedly contributes to strengthening the rights of data subjects and ensuring that they enjoy a high level of protection. (…) the preventive function of actions brought by consumer protection associations, such as the Federal Union, could not be guaranteed if the representative action provided for in Article 80(2) of the GDPR allowed only the infringement of the rights of a person individually and specifically affected by that infringement to be invoked." (*Facebook Ireland Limited,* C-319/20).

Moving from this perspective, the Casebook examines the role of fundamental rights and the one of the principles of effectiveness and proportionality in the EU and national caselaw in the field of data protection. By doing so, it aims at guiding judges and other legal experts in the application of data protection regulation through the illustration of cases in which the CJEU has used the fundamental right framework and the mentioned principles as tools for interpreting current legislation and defining both the balancing of rights and modes of enforcement.

More particularly, the Casebook illustrates:

a) whether and how effectiveness and proportionality have contributed to define the scope of application of data protection with regards both to its territorial scope (chapter 1) and to its material one (chapter 2);
b) whether and to what extent effectiveness and proportionality have shaped the balance between data protection and general interests (such as public security) calling for specific limitations to the protection of personal data (chapter 3);
c) whether and to what extent effectiveness and proportionality have contributed to define the lawfulness of processing with regard to the assessment of its legal bases and the modes in which consent can be rendered to make the data subject's protection effective (chapter 4);
d) whether and to what extent effectiveness and proportionality have shaped the balance between data protection and other fundamental rights and freedom (such as, e.g., the right to intellectual property under Article 17(2) CFREU and the one to an effective remedy against its infringements under Article 47 CFR, addressed in chapter 4, or the freedom of expression and to receive or impart information under Article 11 CFR, addressed in chapter 5);
e) whether and why Article 47 CFREU, the principle of effectiveness and the one of proportionality matter when judicial enforcement is made dependent upon the exhaustion of administrative enforcement procedures (chapter 6);
f) what is the impact of Article 47 CFREU and the mentioned principles upon the choice of sanctions and remedies and their application (chapter 7) and, vice-versa, the impact of data protection on access to justice in cases in which personal data are needed to access to court (chapter 8);
g) whether effective protection may be improved by joint application of data protection law and consumer law in cases in which the data subject is also a consumer (chapter 9).

Compared with the Re-Jus Casebook on data protection, on which the Fricore elaboration is largely based, new streams of questions have been added (particularly, those under (*c*), (*d*) and (*g*)), and new developments have been considered both in EU and in national caselaw.

The structure of the Casebook: some keys for reading

The Casebook is divided into nine chapters.

Chapter 1 shows how the principle of effectiveness has contributed to define the scope of application of EU data protection law in order to guarantee an effective protection of data subjects in relation to data processing occurred in the context of the activities of an establishment of the controller in the territory of the Member State and, more extensively, within a real and effective activity carried out through stable arrangements on that territory (*Google Spain*, C-131/12; *Weltimmo*, C-230/14; *Schrems-I*, C-362/14; *Amazon*, C-191/15; *Holstein*, C-210/16). Taking into consideration the most recent developments, judges may be guided in the application of such principles to the case of de-referencing. In this regard, in light of the principle of the effective protection of data subjects, a search engine operator grants a request for de-referencing under those provisions, that operator is required to carry out that de-referencing only on the versions of the search engine corresponding to the Member States, using, where necessary, measures which effectively prevent or, at the very least, seriously discourage an internet user conducting a search, from one Member State, based on 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 (*Google c. CNIL* , C-507/17). In the CJEU's perspective, the need for an effective protection of data subject is also relevant for defining both the territorial scope of powers of administrative authorities in light of multiple places of processing across MSs (*Holstein*, C-210/16) and the duty of cooperation among those (*Weltimmo*, C-230/14) without the duty of cooperation being an obstacle to full and independent exercise of enforcement powers (*Holstein*, C-210/16). The last part of the chapters provides an up-to-date view on the CJEU's scrutiny over the Commission's decisions concerning data transfer to third countries having special regard to the role of effectiveness and proportionality of safeguards in favour of data subjects in these regards.

Chapter 2 partly builds on the analysis provided by the Re-Jus Casebook concerning the broad interpretation of the concept of personal data, processing and controller based (among other elements) on the principle of effective protection of data subjects (*Breyer*, C-582/14; *Google Spain,* C-131/12; *Lindqvist*, C-101/01). More recent and critical issues are addressed in the second part with regard to the cases in which multiple processors intervene and, again in light of effective judicial protection, may be found jointly liable (*Holstein*, C-210/16; and *Jehovah*, C-25/17, *Fashion ID,* C-40/17).

Charter 3 deals with the complex question concerning data retention within electronic communications and public communication networks and the role played by the CJEU in the annulment of Directive 2006/24 due to lack of proportionality affecting the measures therein allowed through data retention to combat serious crime (*Digital Rights Ireland,* C-293/12). Recent caselaw has indeed provided guidance on the application of the principle of proportionality, as incorporated in Article 15, Directive 2002/58, allowing for restrictions to data protection consisting in necessary, appropriate and proportionate measures within a democratic society to safeguard national security and the prevention of crime (*Schwarz*, C-291/12; *Willem*, C-446/12 to C-449/12; *Puškár*, C-73/16; *Staatssecretaris*, C-70/18; *Tele2*, C-203/15). The Court has not only contributed to define the situations of serious threat to national security, the type of personal data that may be retained, in the given circumstances, and the relevance of time limits for such retention but also the need for the adoption of pertinent decisions by competent authorities,

subject to the principle of proportionality and to judicial review by courts or independent administrative authorities (*La quadrature du Net*, C-511/18, C-512/18, C-520/18).

Chapter 4 addresses the impact of fundamental rights and the one of the principles of effectiveness and proportionality in the interpretation of the GDPR rules regulating the legal bases for processing (Article 6 GDPR). More particularly, the Casebook shows how proportionality has influenced the concept of legitimate interest as a legal basis for processing (*Asociatja de Proprietari,* C-708/18) and how the modes in which consent can be rendered has been affected by the need for effective protection of the data subject (*Planet49,* C-673/17; *Orange Romania,* C-61/2019).

The principle of proportionality is at the core of the analysis developed in *Chapter 5*, concerning the balance between data protection and freedom of expression, the latter including the one to publish and receive information. The caselaw developed both at EU and national level faces challenging issues in this regard: not only when it aims at ensuring that the balance ensures the preservation of the core essence of fundamental rights and freedoms, e.g., when sensitive data is processed (*GC and Others* C-136/17), but also when more controllers are involved, some of which are mere host providers. In the latter case, the balancing exercise needs to be adjusted against the exemption rule included in the 2000/31 Directive on e-commerce (Article 15) and more refined criteria need to be determined depending on the complexity of the monitoring activity expected from the controller in relation with contexts, such as social networks, in which similar contents may be easily replicated with minor divergences (*Glawischnig-Piesczek*, C-18/18).

Chapter 6 introduces the complex enforcement system of data protection, based on the two pillars of administrative and judicial enforcement. Whereas specific means for coordination and cooperation within the Union are expressly provided in the GDPR, the same does not occur for judicial enforcement, in which mechanisms of cooperation (at civil and criminal level) are defined out of this specific Regulation (Article 81-82 TFEU). Nor does the Regulation provide for specific coordination mechanisms between administrative and judicial procedures, apart from establishing that the right to an effective remedy shall include judicial review of administrative authorities' decisions (Article 78 GDPR). Moving from the perspective of the CJEU and the one of the ECtHR when relevant, the Casebook examines the role of Article 47, CFR, in filling in this gap, focusing on the cases in which national procedural autonomy has conditioned access to courts upon the exhaustion of administrative procedures (*Puskàr*, C-73/16). The foundations of the duty of cooperation among administrative authorities in light of the principle of effectiveness are also presented in this chapter (*Facebook Ireland and Schrems*, C-311/18).

The choice of sanctions and remedies in light of Article 47 CFREU and the principles of effectiveness, proportionality and dissuasiveness is the subject of *Chapter 7*. Whereas the GDPR refers to Article 47 CFR, when acknowledging the right to an effective remedy before the court (GDPR, recital 141), and Article 83 states that each supervisory authority shall ensure that the imposition of administrative fines shall in each individual case be effective, proportionate and dissuasive, the same is not explicitly foreseen in respect of remedies. The latter must, however, be effective under Article 78 GDPR; under Article 82 GDPR, compensation must also be effective. In all these respects the CJEU provides useful guidance on how to administer the choice of sanctions and remedies in accordance with the above mentioned general principles. Chapter 8 presents this analysis distinguishing between sanctions, corrective remedies and the right to compensation. The case of corrective remedies and, within this, the role of cancellation and delisting provide a useful example on how effectiveness and proportionality have been used in judicial dialogue at both EU and national level.

Chapter 8 introduces another view on the relation between data protection and access to justice, namely the possible limitations imposed by the former on the latter. This relation has an impact on critical challenges faced by national judges concerning, in particular: i) the admissibility of pieces of evidence

concerning a breach of data protection in court; ii) the impact of the principles of proportionality and effectiveness, Article 8 and Article 47 CFREU on the regulation on access to personal data which are necessary for initiating civil proceedings; iii) the use of evidence derived from unlawful processing in proceedings (*Puškár*, C-73/16; *Rīgas satiksme*, C-13/16).

Chapter 9 concludes the analysis on effective protection of data subjects taking into account the effects of the possible application of consumer law in cases in which the data subject is also a consumer and the infringement of data protection law may also be regarded through the consumer protection lens. The recent adoption of the 2020/1828/EU Directive on representative actions in the field of consumer protection clarifies that such contamination is possible and may reinforce the effectiveness of data protection. Moving from this perspective and taking into account recent developments in EU and national caselaw (e.g., *Fashion ID*, C-40/17, and more recently, *Facebook Ireland Limited*, C-319/20), the Casebook examines whether and to what extent procedures and remedies provided in consumer law, such as collective actions or remedies against unfair practices or the breach of information duties may improve the effective of data and consumer protection jointly.

1. Impact of the Charter on the territorial scope of data protection

1.1. Introduction

Extraterritoriality is currently the subject of important debates in the field of data protection. Within the European Union (hereinafter EU), as the level of protection under the national legislation implementing the European directives varies from one Member State to another, the question of which law is applicable to cross-border processing has been raised and submitted to the CJEU. Issues regarding the jurisdiction of courts in litigation related to cross-border processing, as well as issues regarding the territorial reach of the powers of national supervisory authorities, have also been considered. In **section 1.1**., this chapter will analyse how the CJEU has interpreted and complemented the EU legislation in order to coordinate Member States' national systems, and what the role of the Charter has been in this interpretation. The GDPR includes new provisions on the territorial scope of the protection and brings new challenges.

Concerning relations with third countries, the issue of the reach of European data protection has raised even more serious problems. Data controllers have often argued that they are located outside the EU to try to escape EU data protection legislation. And given the immaterial nature of data, it is a challenge for national authorities to prevent controllers from transferring data collected in the EU abroad, where the applicable rules offer a lower level of protection. Relations with the United States of America in particular, where many important digital businesses are headquartered, are complicated, since the American understanding of data protection differs substantially from the European one. Here, once again, the Charter has been an essential instrument for the CJEU in defining the scope of EU data protection and the regulation of transfers of data outside of the EU, as demonstrated in **section 1.2**.

1.2. Intra-EU relations

Main question addressed

1. Should the principle of effectiveness have an impact on the definition of the territorial scope of data protection laws? What is the geographical scope of controllers' obligations?
2. Should the data protection authority of a Member State exercise competence to hear claims lodged by persons victims of unlawful processing of their personal data, where the law of another Member State is applicable because the data processing was carried out in the context of the activities of an establishment of the controller situated in the territory of that Member State?
3. a) Can a national data protection authority exercise the powers conferred by data protection law against a data controller, when the data controller carries out its activities, fully or in part, in the territory of another Member State? If not, does the principle of effective access to justice impose a duty of cooperation between Member States' supervisory authorities?
b) Where different Member States data protection authorities exercise competence over the same data processing because several entities jointly contribute to the processing of data, does the data protection authority of the Member State where the entity mainly responsible for the processing is established have any priority or supremacy over other Member State data protection authorities, to decide on the lawfulness of the processing?

4. Which court has jurisdiction to order that wrongful data published on a website accessible in several Member States be rectified and/or removed?
5. Should Member States' data protection authorities assess the adequacy of data protection in third countries, where personal data collected in the EU is to be transferred, in terms of EU principles and/or legislation?

6. Should they find that the data protection offered in a third country is not adequate, should Member States oppose the transfer of personal data collected in the EU to that country?

1.2.1. Question 1: Interpretation of the connecting factor defining the territorial scope of a Member State's law on data protection and of the GDPR

Should the principle of effectiveness have an impact on the definition of the territorial scope of data protection laws?

Cluster of relevant CJEU cases :

Within the cluster of cases, identification of the main case(s) that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

➢ 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**)

➢ Judgment of the Court (Third Chamber), 1 October 2015, Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14 (**Weltimmo**)

Cluster of cases:

➢ 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**)

➢ Judgment of the Court (Third Chamber), 1 October 2015, Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14 (**Weltimmo**)

➢ Judgment of the Court, (Grand Chamber), 6 October 2015, *Schrems* v. *Data Protection Commissioner*, C-362/14 (***Schrems I***)

➢ Judgment of the Court (Third Chamber), 28 July 2016, *Verein für Konsumenteninformation* v. *Amazon EU Sàrl*, C-191/15 (***Amazon***)

➢ Judgment of the court (Grand Chamber), 5 June 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH & Facebook Ireland Limited*, C-210/16 (**Wirtschaftsakademie**)

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *Google LLC v. CNIL*, C-507/17 (***Google v. CNIL***)

➢ Judgment of the Court (Grand Chamber), 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, C-311/18 (***Schrems II***)

Relevant legal sources

EU Level

Directive 95/6/EC 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

Article 4 (National law applicable); Recital (10), (18), (19) and (20)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 [GDPR]

Article 3 'Territorial scope'; Recitals 1, 4, 9 to 11, 13, 22 to 25 and 65:

The case(s):

In all referral cases, the general pattern is the same and concerns the application of Directive 95/46/EC. A data subject, domiciled in one Member State, requests correction of/protection against an alleged unlawful processing of its personal data from national authorities/courts, under the law of that Member State, and the data controller that is the party mainly responsible for processing the data is established in a different Member State. However, this data controller's activity expands to the Member State where the data subject is domiciled in diverse ways. In particular, the cases referred deal with situations where:

- The operator of a search engine, established in a third country, sets up a branch or subsidiary, in the Member State where the data subject is domiciled, promoting and selling advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State (*Google Spain*, C-131/12);
- The data controller's company is registered in another Member State and runs a property dealing website concerning properties situated in the territory of the Member State where the data subject is domiciled (*Weltimmo*, C-230/14);
- An undertaking, established in another Member State, directs its activities to the Member State where the data subject is domiciled, by concluding electronic commerce contracts with consumers resident in that Member State (*VKI / Amazon*, C- 191/15);
- An undertaking's website is accessible in a Member State, and this undertaking, established in a different Member State, concludes in the course of electronic commerce contracts with consumers resident in the first Member State (*VKI / Amazon*, C- 191/15);
- A company established in another Member State collects and processes data throughout the entire EU territory, through a local company solely responsible for promoting the sale of advertising established in the Member State where the data subject is domiciled (*Wirtschaftsakademie,* C-210/16).

In each case, the data controller disputes that the data processing is "carried out in the context of an establishment of the controller in the territory of the Member State" whose law is claimed (by the data subject) to be applicable, arguing that the data processing is undertaken abroad, the tasks of the local establishment being of a different nature than that of data processing.

Preliminary question(s) referred to the Court:

In all cases, the Court was, in substance, referred the following question:

Should article 4(1) of Directive 95/46 be interpreted as permitting, in circumstances such as those at issue in the main proceedings, the data protection authorities of a Member State to apply their national law on data protection with regard to a data controller whose main establishment is located in another Member State/ third country, given the links existing with the first Member State?

More specifically:

- In Google Spain,

(1) When the undertaking providing the search engine sets up an office or subsidiary, in a Member State, for the purpose of promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State; or
(2) When the parent company designates a subsidiary located in that Member State as its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking; or
(3) When the office or subsidiary established in a Member State forwards requests and requirements addressed to both it and the parent company, located outside the EU, by data subjects and by the authorities with responsibility for ensuring observation of the right to data protection, even where such collaboration is engaged in voluntarily;
(4) When a search engine uses crawlers or robots to locate and index information contained in web pages located on servers in that Member State; or
(5) When it uses a domain name pertaining to a Member State and arranges for searches and the results thereof to be based on the language of that Member State; or
(6) When the controller undertakes the temporary storage of the information indexed by internet search engines and refuses to disclose the place where it stores those indexes, so that the connecting factor is uncertain; or
(7) Where the centre of gravity of the conflict is located in that Member State where more effective protection of the rights of Union citizens is possible in light of Article 8 of the [Charter]?

- In *Weltimmo*, under circumstances where the data controller's company is registered in another Member State but runs a property dealing website concerning properties situated in the territory of the Member State where the data subject is domiciled and:
  – at which the activity of the controller of the personal data was directed,
  – where the properties concerned were situated,
  – from which the data of the owners of those properties were forwarded,
  – of which those owners were nationals, and
  – in which the owners of that company lived.
- In *Amazon,* under circumstances where the data controller established in a Member State, processing personal data in the course of electronic commerce, directs its commercial activities to another Member State and concludes contracts with consumers resident in that Member State, where and under the law of which the protection is sought?
- In *Wirtschaftsakademie*, under circumstances where a parent company based outside the EU (USA) has legally independent establishments (subsidiaries) in various Member States, and the establishment located in the Member State where the protection is sought (Germany) and against which proceedings are brought, is solely responsible for promoting the sale of advertising and other marketing measures aimed at the inhabitants of this Member State, whereas the independent establishment (subsidiary) located in another Member State (Ireland) is exclusively responsible within the group's internal division of tasks for collecting and processing personal data throughout the entire territory of the EU and hence, also, in the first Member State, if decisions about data processing are in fact taken by the parent company?

Reasoning of the Court:

In the main case at hand, ***Google Spain***, the Court, although not expressly referring to Article 47 of the Charter, 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 EU legislation on data protection, that the EU legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive, and to prevent that same protection from being circumvented, by prescribing a particularly broad territorial scope.

Consequently, the Court decided 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 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 in the territory of a Member State, in this instance, the Spanish territory.

The Court concluded that in such circumstances, one cannot accept 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 assigns special importance.

On the question related to the location 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.

Conclusion of the Court:

The processing of personal data is carried out in the context of the activities of an establishment of the controller in the territory of a Member State, within the meaning of Article 4 (1) (a) of Directive 95/46:

- when the operator of a search engine sets up a branch or subsidiary, in a Member State, which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State (*Google Spain*),
- the controller exercises a real and effective activity — even a minimal one —in the territory of a Member State, through stable arrangements, in the context in which that processing is carried out. In order to ascertain whether that is the case, the referring court may, in particular, consider the fact (i) that the activity of the controller in respect to that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State's language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has a representative in that Member State, who is responsible for recovering the debts resulting from that activity and for representing the controller in the administrative and judicial proceedings relating to the processing of the data concerned (*Weltimmo*); but an establishment cannot exist in a Member State merely because the undertaking's website is accessible there (*Amazon*).

Elements of judicial dialogue:

There is a strong judicial dialogue within the CJEU, since the connecting factor for the territorial application of Member States' data protection laws is being progressively determined by the Court. Case after case, the CJEU brings new clarifications to the interpretation of such a connecting factor.

In ***Weltimmo***, the Court elaborated on the reasoning in *Google Spain*, to state that the concept of 'establishment' should be given a flexible definition, which distances itself from a formalistic approach whereby undertakings are established solely in the place where they are registered. Accordingly, both the degree of stability of the arrangements and the effective exercise of activities in a Member State other than the one where the controller's company is registered, must be interpreted in light of the specific nature of the economic activities and the provision of services concerned. Given the objective pursued by that directive, consisting in ensuring effective and complete protection of the right to privacy and in avoiding any circumvention of national rules, the presence of only one representative can, in some circumstances, be enough to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question. Moreover, in order to attain that objective, it should be considered that the concept of 'establishment', within the meaning of Directive 95/46, is extended to any real and effective activity — even a minimal one — exercised through stable arrangements.

However, in ***Amazon***, the Court specifies that, even if under its previous case-law the concept of 'activities carried out in the context of an establishment' was extended to any real and effective activity, even a minimal one, as long as exercised through stable arrangements, such an establishment cannot exist in a Member State merely because the undertaking's website is accessible there.

In ***Wirtschaftsakademie***, the Court relies on *Weltimmo* and *Google Spain,* to decide that German law is applicable, and therefore that the German data protection authority is competent, to deal with the processing of data of German residents undertaken jointly by Facebook Inc., (USA) and Facebook Ireland. Facebook Germany is responsible for promoting and selling advertising space and carries on activities addressed to persons residing in Germany. For the Court, since the processing of data is intended to enable Facebook to improve its system of advertising, the activities of the German establishment must be regarded as inextricably linked to the processing of personal data for which Facebook Inc., is jointly responsible together with Facebook Ireland. Even if the processing of data is not strictly carried out 'by' the German establishment, it is carried out 'in the context of the activities' of this establishment. This expression cannot be interpreted restrictively, given the objective of ensuring the effective and complete protection of data subjects.

In ***Google v. CNIL***, 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 in the territory of a Member State escaping the obligations and guarantees laid down by Directive 95/46 and Regulation 2016/679.

The CJEU's case law in light of the GDPR:

The case law of the CJEU was taken into account by the legislator when adopting the GDPR. It inspired the drafting of Article 3.

With the GDPR, where provisions are directly applicable in Member States, the issue of the territorial scope of Member States' laws on data protection within the EU should vanish. The same EU rules will apply everywhere in the EU territory. But new issues will certainly arise, and might bring further interest in the Charter. We surely know, for instance, that the implementation of the Regulation may vary from one Member State to another, notably given the principle of procedural autonomy of Member States. There, the CFR could be a decisive tool in achieving better harmonisation and effectiveness of the rights enshrined in the GDPR (compare with consumer protection).

While the intra-EU reach of data protection has generally been resolved by the enactment of the GDPR, focus will now turn to the territorial scope of the Regulation. What processing is subject to the Regulation? What connecting factor to the EU is required in order to have such processing subject to the Regulation?

The territorial scope of the Regulation is defined in Article 3, according to which:

"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 personal data of data subjects who are 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 of 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."

Compared to Article 3 of Directive 95/46, the provision is more precise and seems to expand the territorial scope of EU data protection. The territorial scope of the Regulation is defined according to two different connecting factors.

The first connecting factor targets any "processing carried out in the context of an establishment" located in the Union. This connecting factor is very similar to the one laid down in Directive 95/46, but the GDPR provision endorses the broad meaning of this factor that the CJEU has been progressively building. The connecting factor concerns an establishment of the processor as well as of the controller; and it is expressly stated that the place where the processing is taking place (in or outside of the Union) is irrelevant.

The second connecting factor is based on the residence of the data subject in the Union. Such a connecting factor carries a strong potential for extraterritoriality of the EU legislation, since it makes it applicable to a "controller or processor not established in the Union". However, the grasp of the EU legislation is kept within reasonable limits by subjecting the application of the Regulation based on the residence of the data subject in the Union to additional connections: that the processing activities are related to (a) the offering of goods or services to data subjects in the Union; or (b) the monitoring of data subjects' behaviour as far as such a behaviour takes place within the Union.

The implementation of these criteria has not yer risen issues to be referred to the CJEU. The numerous preliminary questions relating to the GDPR do not concern its territorial scope.

Impact on national case law in a Member State different from the state of the court referring the preliminary question to the CJEU

Italy

Milan *Tribunale*, 4 January 2017, 23838/2016 (available on the Re-Jus Database)

After pointing out that the damage suffered by the applicant had substantially occurred at the time when and in the place where the applicant had become aware that his personal data, relating to the bankruptcy "C. P", was still on the web, the Italian judge, recalls the domestic and European laws as well as the European case law applicable in the case. Directive 95/46/CE, read in light of the *Google Spain* and *Weltimmo* judgments, provides that national provisions adopted by a Member State pursuant to the Directive are applied to the processing of personal data where the processing is carried out in the context of the activities of an establishment of the controller in the territory of that Member State. In this context, the ECJ has clarified that, "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 engine profitable". With regard to such judgments, the Milan *Tribunale* concludes that national provisions laying down the powers and competence of the national data protection authority must apply in the case.

1.2.2. Question 1a: Geographical scope of controllers' obligations

What is the geographical scope of controllers' obligations?

Cluster of relevant CJEU cases

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *Google LLC v. CNIL,* C-507/17 (***Google v. CNIL***)

The case

The French Data protection authority (CNIL) served formal notice on Google that, when granting a request from a natural person for links to web pages to be removed from the list of results displayed following a search conducted on the basis of that person's name, it must apply that removal to all its search engine's domain name extensions.

Google refused to comply with that formal notice, confining itself to removing the links in question from only the results displayed following searches conducted from the domain names corresponding to the versions of its search engine in the Member States. The case was to be decided by the Council of State (here is the link of the FRICoRe Database to the preliminary reference).

Preliminary question(s) referred to the Court:

'(1) Must the "right to de-referencing", as established by the [Court] in its judgment of 13 May 2014, [*Google Spain and Google* (C-131/12, EU:C:2014:317)] on the basis of the provisions of [Article 12(b) and subparagraph (a) of the first paragraph of Article 14] of Directive [95/46], be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to deploy the de-referencing to all of the domain names used by its search engine so that the links at issue no longer appear, irrespective of the place from where the search initiated on the basis of the requester's name is conducted, and even if it is conducted from a place outside the territorial scope of Directive [95/46]?

(2) In the event that Question 1 is answered in the negative, must the "right to de-referencing", as established by the [Court] in the judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, only to remove the links at issue from the results displayed following a search conducted on the basis of the requester's name on the domain name corresponding to the State in which the request is deemed to have been made or, more generally, on the domain names distinguished by the national extensions used by that search engine for all of the Member States …?

3. Moreover, in addition to the obligation mentioned in Question 2, must the "right to de-referencing" as established by the [Court] in its judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to remove the results at issue, by using the "geo-blocking" technique, from searches conducted on the basis of the requester's name from an IP address deemed to be located in the State of residence of the person benefiting from the "right to de-referencing", or even, more generally, from an IP address deemed to be located in one of the Member States subject to Directive [95/46], regardless of the domain name used by the internet user conducting the search?'

Reasoning of the Court:

The internet is a global network without borders and the information and links are ubiquitous. In a globalised world, the access of internet users — including those outside the Union — to the referencing of a link referring to information regarding a person whose centre of interests is situated in the Union is thus likely to have immediate and substantial effects on that person within the Union itself. So, the EU legislature may lay down the obligation of de-referencing on all the versions of the search engine. But it has not done so. Moreover, EU law does not currently provide cooperation instruments and mechanisms regarding the scope of a de-referencing outside the Union. Consequently, neither the Directive 95/46 nor the Regulation 2016/679 require a search engine to carry out a de-referencing on all of its versions.

On the basis of the high level of protection throughout the EU, the de-referencing is, in principle, supposed to be carried out in respect to all the Member States.

However, the result of a balance of interests is not necessarily the same for all the Member States. EU law does not prohibit that the de-referencing granted concerns all versions of the search engine even if it does not require it. So a supervisory or judicial authority of a Member State remains competent to weigh up, in light of national standards of protection of fundamental rights the protection of personal data and the right to freedom of information and, to order the search engine to carry out a de-referencing concerning all versions, where appropriate.

Conclusion of the Court :

The de-referencing concerns the versions of the search engine in all the Member States. Nevertheless, the operator should, where necessary, use measures which 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.

Impact on the follow-up case:

The national court had to clarify whether the national authority, the CNIL, had correctly exercised its discretionary power. The French Council of State (Conseil d'Etat, 27 March 2020, to be added to the database) decided that by requiring worldwide de-referencing, the CNIL erred in law, as the CJEU has established the principle of de-referencing with a European scope. It then recalled the discretion left to

the national authorities in the context of the balancing of fundamental rights and the possibility of modifying the legal basis of the decision taken by the CNIL. However, since no legislative provision authorises worldwide de-referencing and since the CNIL's decision was taken on the basis of a principle of worldwide de-referencing without balancing fundamental rights, the Conseil d'Etat decided that there was no reason to proceed with this substitution and annulled the decision of the CNIL.

Elements of judicial dialogue:

National judges have to implement the CJUE decision and then to balance fundamental rights.

Impact on national case law in Member States other than the one of the court referring the preliminary question to the CJEU

Italy

With appeal filed on February 7, 2018, Google L.L.C., (formerly Google Inc.) and Google Italy S.r.l., brought an action before the Court of Milan, against the Italian DPA and a data subject, asking for the annulment of DPA decision no. 557 of 21 December 2017, where the DPA ordered to Google's companies to deindex globally the URLs indicated in the data subject's claim, considering the right to be forgotten of the person concerned on the basis of the *Google Spain* judgment of the Court of Justice.

1.2.3. Question 2: Coordination between national data protection authorities regarding intra- EU cross border processing

Cluster of relevant CJEU cases

➢ Judgment of the Court (Third Chamber), 1 October 2015, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14 (**Weltimmo**)

➢ Judgment of the Court, (Grand Chamber), 6 October 2015, *Schrems* v. *Data Protection Commissioner*, C-362/14 (***Schrems I***)

➢ Judgment of the court (Grand Chamber), 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH & Facebook Ireland Limited, C-210/16 (**Wirtschaftsakademie**)

Within this cluster, identification of the main case@s that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

➢ Judgment of the Court (Third Chamber), 1 October 2015, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14 (**Weltimmo**)

➢ Judgment of the court (Grand Chamber), 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH & Facebook Ireland Limited, C-210/16 (**Wirtschaftsakademie**)

Relevant Legal sources

EU Level

Directive 95/46/EC 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

Article 28(1), (3) and (6)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Article 56

Should the data protection authority of a Member State exercise competence to hear claims lodged by persons victim of unlawful processing of their personal data, where the law of another Member State is applicable because the data processing was carried out in the context of the activities of an establishment of the controller situated in the territory of that Member State?

Within the cluster of cases above, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

➢ Judgment of the Court (Third Chamber), 1 October 2015, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14 (**Weltimmo**)

Relevant legal provisions at national level

The Hungarian Law on information

Paragraph 2(1)

"This Law shall apply to all data processing operations and technical manipulation of data carried out in the territory of Hungary that pertain to the data of natural persons or to public information or information of public interest".

The case(s):

Weltimmo, a company which has its registered office in Slovakia, runs a property dealing website concerning Hungarian properties. For that purpose, it processes the personal data of the advertisers. The advertisements are free of charge for one month but thereafter a fee is payable. Many advertisers sent a request by e-mail for the deletion of both their advertisements and their personal data as from that time. However, Weltimmo did not delete that data and charged the interested parties for the price of its services. As the amounts charged were not paid, Weltimmo forwarded the personal data of the advertisers concerned to debt collection agencies.

Complaints were lodged with the Hungarian data protection authority, which declared that it was competent under Hungarian law, taking the view that the collection of the data concerned constituted processing of data or a technical operation for the processing of data concerning natural persons. The data protection authority found that Weltimmo had infringed Hungarian Law on information, and imposed a fine of approximately EUR 32 000 on the respective company.

The Budapest Administrative and Labour court, to which the case was brought by Weltimmo, decided that the Hungarian data protection authority was competent, and could apply Hungarian law even though the company had its registered office in Slovakia.

Weltimmo lodged an appeal to the Hungarian Kúria (Supreme Court), claiming that pursuant to Article 4(1)(a) of Directive 95/46, the Hungarian data protection authority was not competent in this case and could not apply Hungarian law in respect of a supplier of services established in another Member State.

The Hungarian data protection authority maintained it was competent, and that Hungarian law was applicable. It adduced new facts, in particular that: 1) Weltimmo had a Hungarian representative in Hungary, namely one of the owners of that company, who represented it in the administrative and judicial proceedings that took place in that Member State and tried to negotiate the settlement of the unpaid debts with the advertisers; 2) Weltimmo did not carry out any activity at the place where it has its registered office, in Slovakia; 3) Weltimmo had developed two property dealing websites, written exclusively in Hungarian, opened a bank account in Hungary for the recovery of its debts, and had a postal address in that Member State; 4) the question as to the Member State in which the server or servers used by that company were installed was not settled.

Preliminary question referred to the Court:

The Hungarian Supreme Court asked, in essence:

Whether Articles 4(1)(a) and 28(1) of Directive 95/46 must be interpreted as permitting, in circumstances such as those at issue in the main proceedings, the data protection authority of a Member State to exercise competence and apply its national law on data protection with regard to a data controller whose company is registered in another Member State and who runs a property dealing website concerning properties situated in the territory of the first of those two States. In particular, the referring court asked whether it was significant that that Member State was the Member State:

– at which the activity of the controller of the personal data was directed,
– where the properties concerned were situated,
– from which the data of the owners of those properties were forwarded,
– of which those owners were nationals, and
– in which the owners of that company lived.

Reasoning of the Court

The Court first pronounced on **the competence of a national supervisory authority** to act in a situation where the processing of data is carried out in the context of the activities of an establishment of the controller in the territory of another Member State. The Court judged that, pursuant to Article 28 of Directive 95/46, entitled 'Supervisory authority', dealing with the role and powers of that authority, that authority is responsible for monitoring the application, within the territory of its own Member State, of the provisions adopted by the Member States pursuant to that directive. The Court considers that each supervisory authority must hear claims lodged by any person concerning the protection of his rights and freedoms with regard to the processing of personal data, in particular victims of unlawful processing of their personal data in that Member State. It follows that the supervisory authority of a Member State, to which a complaint has been submitted, on the basis of article 28(4) of that directive, by natural persons in relation to the processing of their personal data, may examine that

complaint irrespective of the applicable law, and, consequently, even if the law applicable to the processing of the data concerned is that of another Member State.

Although not expressly referring to the ***principle of effectiveness*** in this part of the decision, by detaching the question of the competence of the data protection authority from the question of the law applicable to the processing of personal data, the Court *implicitly shows concern for the effective access to justice and protection of data subjects*: a victim of an unlawful practice should be able to seek protection from the data protection authority of the Member State where he is domiciled. It is then up to this authority to exercise its powers within the territory of its own Member State or, if powers are to be exercise beyond these limits, to cooperate with the data protection authority of the Member State where the data controller carries out its activities (see hereinafter, question 3).

Conclusion of the Court:

Where the supervisory authority of a Member State, to which complaints have been submitted in accordance with Article 28(4) of Directive 95/46, reaches the conclusion that the law applicable to the processing of the personal data concerned is not the law of that Member State, but the law of another Member State, Article 28(1), (3) and (6) of that directive must be interpreted as meaning that that supervisory authority is competent to deal with claims brought by victims of unlawful processing of their personal data in that Member State. However, it will be able to exercise the effective powers of intervention conferred on it in accordance with Article 28(3) of that Directive only within the territory of its own Member State (see hereinafter).

Elements of judicial dialogue:

Weltimmo, which deals with intra-EU relations, is echoed in *Schrems I* in relation to extra-EU relations. That decision implies that, since national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data, each of them is competent, and vested with the power, to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down by Directive 95/46. (see below, Section 2.2.).

In *Wirtschaftsakademie*, the CJEU relies strongly on *Weltimmo* in deciding that competence may be exercised by the data protection supervisory authority of a Member State, where the entity established in that Member State is not the one actually processing the data, but the one responsible, as a result of the division of tasks within the group, solely for the sale of advertising space and other marketing activities. Recalling that it had been decided in *Weltimmo* that, in view of the objective pursued by Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, the expression 'in the context of the activities of an establishment' cannot be interpreted restrictively, the Court concludes that "the supervisory authority of a Member State is entitled to exercise the powers conferred on it by Article 28(3) of that directive with respect to an establishment of that undertaking situated in the territory of that Member State even if, as a result of the division of tasks within the group, first, that establishment is responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State and, second, exclusive responsibility for collecting and processing personal data belongs, for the entire territory of the European Union, to an establishment situated in another Member State".

The contribution of the GDPR to the issue of the competence of supervisory authorities:

The GDPR includes two very interesting provisions regarding the competence of national supervisory authorities.

The first one, Article 55 entitled "Competence", does not make major changes to the competence as defined by the CJEU, although it adds some clarifications:

"1. 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 in the territory of its own Member State.

2. Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.
3. Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity."
The main innovation is introduced by article 56, entitled "Competence of the lead supervisory authority":

"1. Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60.

2. By derogation from paragraph 1, each supervisory authority shall be competent to handle a complaint lodged with it or a possible infringement of this Regulation, if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State.
3. In the cases referred to in paragraph 2 of this Article, the supervisory authority shall inform the lead supervisory authority without delay on that matter. Within a period of three weeks after being informed the lead supervisory authority shall decide whether or not it will handle the case in accordance with the procedure provided in Article 60, taking into account whether or not there is an establishment of the controller or processor in the Member State of which the supervisory authority informed it.
4. Where the lead supervisory authority decides to handle the case, the procedure provided in Article 60 shall apply. The supervisory authority which informed the lead supervisory authority may submit to the lead supervisory authority a draft for a decision. The lead supervisory authority shall take utmost account of that draft when preparing the draft decision referred to in Article 60(3).
5. Where the lead supervisory authority decides not to handle the case, the supervisory authority which informed the lead supervisory authority shall handle it according to Articles 61 and 62.
6. The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor."
On this provision, see below Question 3.

Impact on national case law in Member States different from the state of the court referring the preliminary question to the CJEU :

Italy

Milan *Tribunale*, 4 January 2017, 23838/2016 (Re-Jus database)

Italian judges refer to *Google Spain* and *Weltimmo* to confirm the competence of the Italian data protection authority, based on the presence in Italy of an establishment intended to promote and sell advertising space offered by the search engine in order to make the service offered by the engine profitable.

France

FRENCH DATA PROTECTION AUTHORITY (CNIL) 21 JANUARY 2019, DECISION N° SAN-2019-001.

According to the GDPR, the competent authority is that of the principal place of business of the controller. The CNIL states that, "in order to qualify as a principal place of business, the establishment concerned must have decision-making power with regard to data processing" and decides that for Google, this establishment is located in the USA. So there is no principal place of business in Europe. As a result, there is no need for a lead institution; national authorities are therefore free of any obligation to coordinate. The CNIL informed the European Data Protection Committee, which remained silent. The CNIL considered itself competent to hear the class action challenging Google's privacy policy.

On appeal against the decision, the Council of State (Conseil d'Etat, 19 June 2020, n° 430810, to add to the FRICORE Database) adopted the same position.

The controller's principal place of business is defined as the place of its central administration in the Union, unless decisions on the processing of personal data are taken at one of its other establishments in the Union which has the power to enforce those decisions. When the various European establishments of the controller do not have this decision-making power, it seems impossible to identify a principal establishment within the meaning of the RGPD. The Council of State deduced that, "the mechanism of the lead authority provided for in Article 56 of the GDPR cannot be implemented" and that, in accordance with Article 55 GDPR, each national supervisory authority is competent to monitor compliance with the GDPR in the territory of its Member State. This situation corresponded at the time of the entry into force of the GDPR to that of Google. Google's central administration in Europe, located in Ireland, had no decision-making power, decisions being taken in the United States.

The one-stop-shop mechanism was paralysed and each national authority was competent to deal with activities carried out in the territory of its own State. The Council of State then admitted that the CNIL had jurisdiction to investigate complaints about the processing of personal data of French users of the Android operating system and to sanction Google.

Google claimed that this system violated the non *bis in idem* principle since any national protection authority could sanction it. The Council of State dismissed the argument, noting that the CNIL would only have jurisdiction over "users located in France". Thus the jurisdiction of the national authority is limited *rationae personae*.

1.2.4. Question 3: Impact of the territorial limitation of national data protection authorities: the duty of cooperation

a) Can a national data protection authority exercise the powers conferred upon it by data protection law against a data controller, when the data controller carries out its activities, fully or in part, in the territory of another Member State? If not, does the principle of effective access to justice impose a duty of cooperation between Member States' supervisory authorities? b) Where different Member State data protection authorities exercise competence over the same data processing because several entities jointly contribute to the processing of data, does the data protection authority of the Member State where the entity mainly responsible for the processing is established have any priority or supremacy over other Member State data protection authorities, to decide on the lawfulness of the processing?

3. a) – Duty of cooperation between Member State Data protection authorities

a) Can a national data protection authority exercise the powers conferred upon it by data protection law against a data controller, when the data controller carries out its activities, fully or in part, in the territory of another Member State? If not, does the principle of effective access to justice impose a duty of cooperation between Member States' supervisory authorities?

The cases: Weltimmo and Facebook

In *Weltimmo* (see the full facts described above under question 2), the Hungarian supervisory authority considered that it was competent, and that Hungarian law was applicable, with the result that it could exercise the power conferred upon it by Hungarian law to impose a fine on the data controller although its establishment was located in another Member State. Still, the Hungarian supervisory authority was willing to exercise such power, even if it were considered that the law applicable was not Hungarian law, but the law of the Member State where the data controller carried out its activities in the context of an establishment.

Preliminary question referred to the Court:

The question asked by the referring Court in *Weltimmo* is in substance the following:

If the Hungarian data protection authority was to reach the conclusion that the law applicable to the processing of the personal data is not Hungarian law, but the law of another Member State, should Article 28(1), (3) and (6) of Directive 95/46 be interpreted as meaning that that authority would be able to exercise only the powers provided for by Article 28(3) of that directive, in accordance with the law of that other Member State, and would not be able to impose penalties?

Reasoning of the Court:

Although the decision of the Court on the territorial scope of Hungarian law in *Weltimmo* (see above, question 1) would probably lead the referring court to judge that the Hungarian data protection authority could apply Hungarian law to the processing of data, the Court nevertheless considers the issue of the powers a Member State's data protection authority is able to exercise, when its law is not applicable

because the data controller does not carry out its activities in the context of an establishment located in that Member State.

The Court states that the powers of supervisory authorities listed in the directive, such as investigative powers or effective powers of intervention, are non-exhaustive, which implies that those powers of intervention may include the power to penalise the data controller by imposing a fine on him, where appropriate (see Chapter 6).

But the Court then points to the rule of the territorial application of supervisory authorities' powers: each supervisory authority is to exercise all of the powers conferred on it in the territory of its own Member State in order to ensure, in that territory, compliance with data protection rules. Based on territorial sovereignty, the principle of legality and the concept of the rule of law, the Court concludes that the power to impose penalties cannot be exercised, as a matter of principle, outside the legal limits within which an administrative authority is authorised to act under the law of its own Member State. For the Court, this means that when a supervisory authority receives a complaint, that authority may exercise its investigative powers irrespective of the applicable law. But if it reaches the conclusion that the law of another Member State is applicable, it cannot impose penalties outside the territory of its own Member State.

However, the Court stresses -- impliedly referring to ***the principle of effectiveness*** -- that the Directive requires that each authority may be requested to exercise its powers by another Member State's authority and that the supervisory authorities are to cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information. In the absence of that provision, where the controller of personal data is subject to the law of a Member State, but infringes the right to the protection of the privacy of natural persons in another Member State, in particular by directing his activity at that other Member State without, however, being established there within the meaning of that directive, it would be difficult, or even impossible, for those persons to enforce their right to that protection. This is why national supervisory authorities should cooperate. The authority to which the original complaint has been submitted must, in fulfilment of the duty of cooperation, request the supervisory authority of the Member State whose law is applicable, to establish whether there is an infringement of that law and impose penalties if that law permits.

Conclusion of the Court:

Where the supervisory authority of a Member State to which complaints have been submitted in accordance with Article 28(4) of Directive 95/46 reaches the conclusion that the law applicable to the processing of the personal data concerned is not the law of that Member State, but the law of another Member State, Article 28(1), (3) and (6) of that directive must be interpreted as meaning that that supervisory authority will be able to exercise the effective powers of intervention conferred on it in accordance with Article 28(3) of that directive only within the territory of its own Member State. Accordingly, it cannot impose penalties based on the law of that Member State on the controller of processing of such data who is not established in that territory, but should, in accordance with article 28(6) of that Directive, ask the supervisory authority in the Member State whose law is applicable to act.

Elements of judicial dialogue:

In *Schrems I*, the Court considers, with regard to the powers available to the national supervisory authorities in respect of transfers of personal data to third countries, that Article 28(1) of Directive

95/46 requires Member States to set up one or more public authorities responsible for monitoring, with complete independence, compliance with EU rules on the protection of individuals with regard to the processing of such data. The national supervisory authorities have a wide range of powers for that purpose, in particular investigative powers, such as the power to collect all the information necessary for the performance of their supervisory duties, effective powers of intervention, such as that of imposing a temporary or definitive ban on processing of data, and the power to institute legal proceedings. Those powers, listed in a non-exhaustive manner in Article 28(3) of Directive 95/46, constitute the necessary means to perform their duties.

The Court points out that it follows from Article 28(1) and (6) of Directive 95/46 that the powers of the national supervisory authorities concern processing of personal data carried out in the territory of their own Member State, so that they do not have powers under Article 28 in respect of processing of such data carried out in a third country. However, the operation of having personal data transferred from a Member State to a third country in itself, constitutes processing of personal data carried out in a Member State. Since, in accordance with Article 8(3) of the Charter and article 28 of Directive 95/46, the national supervisory authorities are responsible for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data, each of them is therefore vested with the power to check whether a transfer of personal data from its own Member State to a third country complies with the requirements laid down by Directive 95/46.

With this reasoning, the Court ensures that, even though Member States' supervisory authorities do not have power over data processing carried out in a third country, they can indirectly monitor such processing abroad since they are vested with the power to oppose the transfer of data to that third country if it does not ensure the adequate protection of personal data. Although the principle of effectiveness it not expressly referred to, the decision implicitly relies on such a principle (see below, section 2.2).

In *Wirtschaftsakademie*, the CJUE complements *Weltimmo* by stressing that the mere fact that the processing of data is carried out in a Member State does not necessarily deprive other Member States' data protection supervisory authorities of the competence and powers laid down in Article 28 of the directive. Given that the concept of 'in the context of the activities of an establishment' (see above question 1) and of 'controller' (see below Chapter 3, question 3) are to be given a broad interpretation, a Member States law is applicable to, and its supervisory authority has competence over, the processing of data when an entity responsible solely for the sale of advertising space and other marketing activities has its establishment in that Member State, even if, as a result of the division of tasks within the group, an establishment situated in another Member State has exclusive responsibility for collecting and processing personal data for the entire territory of the EU.

The duty of cooperation in the new GDPR:

The duty to cooperate is regulated with great precision by the GDPR. Article 61 deals with "Mutual assistance" and states that:

'1. Supervisory authorities shall provide each other with relevant information and mutual assistance in order to implement and apply this Regulation in a consistent manner, and shall put in place measures for effective cooperation with one another. Mutual assistance shall cover, in particular, information requests and supervisory measures, such as requests to carry out prior authorisations and consultations, inspections and investigations.

1. Each supervisory authority shall take all appropriate measures required to reply to a

request of another supervisory authority without undue delay and no later than one month after receiving the request. Such measures may include, in particular, the transmission of relevant information on the conduct of an investigation.

2. Requests for assistance shall contain all the necessary information, including the purpose of and reasons for the request. Information exchanged shall be used only for the purpose for which it was requested.

3. The requested supervisory authority shall not refuse to comply with the request unless:

(a) it is not competent for the subject-matter of the request or for the measures it is requested to execute; or

(b) compliance with the request would infringe this Regulation or Union or Member State law to which the supervisory authority receiving the request is subject.

4. The requested supervisory authority shall inform the requesting supervisory authority of the results or, as the case may be, of the progress of the measures taken in order to respond to the request. The requested supervisory authority shall provide reasons for any refusal to comply with a request pursuant to paragraph 4.

5. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.

6. Requested supervisory authorities shall not charge a fee for any action taken by them pursuant to a request for mutual assistance. Supervisory authorities may agree on rules to indemnify each other for specific expenditure arising from the provision of mutual assistance in exceptional circumstances.

7. Where a supervisory authority does not provide the information referred to in paragraph 5 of this Article within one month of receiving the request of another supervisory authority, the requesting supervisory authority may adopt a provisional measure in the territory of its Member State in accordance with Article 55(1). In that case, the urgent need to act under Article 66(1) shall be presumed to be met and require an urgent binding decision from the Board pursuant to Article 66(2).

8. The Commission may, by means of implementing acts, specify the format and procedures for mutual assistance referred to in this Article and the arrangements for the exchange of information by electronic means between supervisory authorities, and between supervisory authorities and the Board, in particular the standardised format referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 93(2).'

The GDPR goes further, since it provides for the possibility to carry out "joint operations of supervisory authorities" (Article 62) and of course, having instituted a "lead supervisory authority", for the "cooperation between the lead supervisory authority and the other supervisory authorities concerned". Regarding this, Article 60 (1) to (3) reads:

"1. The lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.

2. The lead supervisory authority may request at any time other supervisory authorities concerned to provide mutual assistance pursuant to Article 61 and may conduct joint operations pursuant to Article 62, in particular for carrying out investigations or for monitoring the implementation of a measure concerning a controller or processor established in another Member State.

3. The lead supervisory authority shall, without delay, communicate the relevant information on the matter to the other supervisory authorities concerned. It shall without delay submit a draft

decision to the other supervisory authorities concerned for their opinion and take due account of their views."

Application of the GDPR

Relevant CJEU case:

- Judgment of the court (Grand Chamber) 15 June 2021, Case C645/19, *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA, v. Gegevensbeschermingsautoriteit* (**Facebook**)

The Case

On 11 September 2015 the President of the Privacy Commission (Belgian Data Protection Authority) brought legal proceedings seeking an injunction against Facebook Ireland, Facebook Inc., and Facebook Belgium before the Nederlandstalige rechtbank van eerste aanleg Brussel (Dutch-language Court of First Instance, Brussels, Belgium). The object of those injunction proceedings was to bring to an end what the Privacy Commission describes, *inter alia*, as a 'serious and large-scale infringement of the legislation relating to the protection of privacy' on behalf of Facebook, consisting in the collection by that online social network of information on the internet browsing behaviour both of Facebook account holders and of non-users of Facebook services by means of various technologies, such as cookies, social plug-ins (for example, the 'Like' or 'Share' buttons) or pixels. Those features permit Facebook to obtain certain data of an internet user who visits a website page containing them, such as the address of that page, the 'IP address' of the visitor to that page and the date and time of the visit in question. By judgment of 16 February 2018, the Court of First Instance in Brussels held that it had jurisdiction to give a ruling on those injunction proceedings, in so far as the action concerned Facebook Ireland, Facebook Inc., and Facebook Belgium, and declared that the application for leave to intervene made by the Privacy Commission was inadmissible. The court held that Facebook was not adequately informing Belgian internet users of the collection of the information concerned and of the use of that information. Further, the consent given by the internet users to the collection and processing of that data was held to be invalid. Consequently, that court ordered Facebook Ireland, Facebook Inc., and Facebook Belgium (i) to desist, with regard to all internet users established in Belgium, from placing, without their consent, cookies that remain active for two years on the devices used by them when browsing a web page in the Facebook.com domain or visiting the website of a third party, and from placing cookies and collecting data by means of social plug-ins, pixels or similar technological means on third party websites, in a manner that was excessive in light of the objectives thereby pursued by the Facebook social network, (ii) to desist from providing information that might reasonably mislead the data subjects as to the real extent of the mechanisms put in place by Facebook for the use of cookies, and (iii) to destroy all the personal data obtained by means of cookies and social plug-ins.

On 2 March 2018 Facebook Ireland, Facebook Inc., and Facebook Belgium brought an appeal against that judgment before the Court of Appeal. The court held that it has jurisdiction solely to give a ruling on the appeal brought in so far as that appeal concerns Facebook Belgium. Conversely, the referring court held that it lacked jurisdiction to hear that appeal in relation to Facebook Ireland and Facebook Inc. The court also held that the DPA had not demonstrated the required standing to bring the injunction proceedings in so far as those proceedings related to facts prior to 25 May 2018. In what regards the facts subsequent to that date, the court was uncertain as to the effect of the entry into force of Regulation 2016/679, in particular the effect of the application of the 'one-stop shop' mechanism provided for by that regulation, on the competences of the DPA and on its power to bring such injunction proceedings.

The court is uncertain to what extent the Court's interpretation in *Wirtschaftsakademie* is still of relevance to the application of the GDPR.

Preliminary questions referred to the Court

'(1) Should Article 55(1), Articles 56 to 58 and Articles 60 to 66 of [Regulation 2016/679], read together with Articles 7, 8 and 47 of the [Charter], be interpreted as meaning that a supervisory authority which, pursuant to national law adopted in implementation of Article 58(5) of that regulation, has the competence to initiate or engage in legal proceedings before a court in its Member State against infringements of that regulation cannot exercise that competence in connection with cross-border data processing if it is not the lead supervisory authority for that cross-border data processing?

(2) Does the answer to the first question referred differ if the controller of that cross-border data processing does not have its main establishment in that Member State but does have another establishment there?

(3) Does the answer to the first question referred differ if the national supervisory authority initiates the legal proceedings against the main establishment of the controller in respect of the cross border data processing rather than against the establishment in its own Member State?

(4) Does the answer to the first question referred differ if the national supervisory authority had already initiated the legal proceedings before the date on which [Regulation 2016/679] entered into force (25 May 2018)?

(5) If the first question referred is answered in the affirmative, does Article 58(5) of [Regulation 2016/679] have direct effect, meaning that a national supervisory authority can rely on that provision to initiate or continue legal proceedings against private parties even if Article 58(5) of [Regulation 2016/679] has not been specifically transposed into the legislation of the Member States, notwithstanding the requirement to do so?

(6) If questions (1) to (5) are answered in the affirmative, could the outcome of such proceedings prevent the lead supervisory authority from making a contrary finding when the lead supervisory authority investigates the same or similar cross-border processing activities in accordance with the mechanism laid down in Articles 56 and 60 of [Regulation 2016/679]?'

Reasoning of the Court

As a preliminary point, the court recalled that, unlike Directive 95/46, which had been adopted on the basis of Article 100 A of the EC Treaty, concerning the harmonisation of the common market, the legal basis of Regulation 2016/679 is Article 16 TFEU, which enshrines the **right of everyone to the protection of personal data** which concerns them. So the EU institutions, bodies, offices and agencies, and the competent authorities of the Member States, have to ensure a high level of protection of the rights guaranteed in Article 16 TFEU and Article 8 of the Charter.

Each supervisory authority is to be competent for the performance of the tasks assigned to it and the exercise of the powers conferred on it, in accordance with that regulation, in the territory of its own Member State (GDPR, Article 55, see judgment of 16 July 2020, *Facebook Ireland and Schrems*, C311/18, paragraph 147) and has to cooperate with other supervisory authorities in order to ensure the consistency of application and enforcement of the GDPR. They have various investigative powers (Article 58(1) and the power to bring any infringement of that regulation to the attention of the judicial authorities and, where appropriate, to initiate or engage in legal proceedings (Article 58(5) of that regulation).

With respect to '**cross-border processing'**, the 'one-stop shop' mechanism (GDPR Article 60), based on an allocation of competences between one 'lead supervisory authority' and the other supervisory authorities concerned applies: first, the supervisory authority of the main establishment or of the single establishment of the controller or processor is to be competent to act as **lead supervisory authority;** second, the various national supervisory authorities concerned must cooperate in order to reach a consensus and a single decision, which is binding on all those authorities; third, the supervisory authorities provide each other with relevant information and mutual assistance in order to implement and apply that regulation in a consistent manner throughout the EU (GDPR Article 61).

The CJEU recalls the principle of the one-stop-shop mechanism and clarifies the role of non-lead DPAs. The competence of the lead authority is, however, limited due to the **fair and effective cooperation** and the aim of a single decision that suits all DPAs concerned. The need for "fair and effective cooperation" between the lead supervisory authority and the other supervisory authorities concerned is based on recital 13 of the RGPD, which refers to consistency and not cooperation, which makes it possible to understand that cooperation is used to promote consistency (which is also specified in Article 63 of the RGPD).

This cooperation makes it possible to justify the lead authority's competence in principle and, consequently, the adoption of a single decision, even though the processing operation at issue affects several Member States. Nevertheless, exceptions are provided for. The CJEU takes up the letter of the Regulation and distinguishes two of them. The first leads to the exclusion of the one-stop shop mechanism when the processing operation only concerns an establishment in the Member State to which the DPA belongs or substantially affects data subjects in that Member State only (Article 56(2)). The second is conditioned by urgency. In exceptional circumstances, where the supervisory authority concerned considers that there is an urgent need to intervene to protect the rights and freedoms of the data subjects, Article 66 allows, allows for the adoption interim measures immediately. These measures are limited in two ways: territorially, to the territory of the State of the DPA concerned, and in time, to a period of less than three months. The adoption of definitive measures requires an urgent opinion or an urgent binding decision of the European Data Protection Committee.

Loyal and effective cooperation is still required in the context of these exceptions. Article 56(3) GDPR requires the lead supervisory authority to be informed, as it may decide to deal with the case. Moreover, the lead supervisory authority may not ignore the views of the other supervisory authorities, and any relevant and reasoned objection made by one of the other supervisory authorities has the effect of blocking, at least temporarily, the adoption of the draft decision of the lead supervisory authority. Thus, in accordance with Article 60(4) of Regulation 2016/679, where one of the other supervisory authorities concerned expresses, within a period of four weeks after having been consulted, such a relevant and reasoned objection to the draft decision, the lead supervisory authority, if it does not follow the relevant and reasoned objection or is of the opinion that that objection is not relevant or reasoned, is to submit the matter to the consistency mechanism provided for in Article 63 of that regulation, in order to obtain a binding decision, adopted on the basis of Article 65(1)(a) of that regulation, from the European Data Protection Board.

The Court states that the one-stop shop mechanism is compatible with Articles 7, 8 and 47 of the Charter: the rules on the allocation of competences to adopt decisions between the lead supervisory authority and the other supervisory authorities, as laid down by that regulation, take nothing away from the responsibility incumbent on each of those authorities to contribute to a high level of protection of those rights, with due regard to those rules and to the requirements of cooperation and mutual assistance. The use of the 'one-stop shop' mechanism cannot under any circumstances have the consequence that a national supervisory authority, in particular the lead supervisory authority, does not assume the

responsibility incumbent on it to contribute to providing effective protection of natural persons from infringements of their fundamental rights

Regarding the alleged breach of the right to an effective remedy, guaranteed in Article 47 of the Charter, the possibility that a supervisory authority other than the lead supervisory authority may exercise the power laid down in Article 58(5) of GDPR, with respect to an instance of cross-border processing of personal data, is circumscribed takes nothing away from the right of every data subject, laid down in Article 78(1) and (2) to an effective legal remedy, in particular, against a legally binding decision of a supervisory authority concerning them, or against a failure by the supervisory authority to handle a complaint that that data subject has lodged.

Conclusion of the Court

1. Article 55(1), Articles 56 to 58 and Articles 60 to 66 of 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), read together with Articles 7, 8 and 47 of the CFREU, must be interpreted as meaning that a supervisory authority of a Member State which, under the national legislation adopted in order to transpose Article 58(5) of that regulation, has the power to bring any alleged infringement of that regulation to the attention of a court of that Member State and, where necessary, to initiate or engage in legal proceedings, may exercise that power in relation to an instance of cross-border data processing even though it is not the 'lead supervisory authority', within the meaning of Article 56(1) of that regulation, with respect to that data processing, provided that that power is exercised in one of the situations where Regulation 2016/679 confers a competence to adopt a decision on that supervisory authority finding that such processing is in breach of the rules contained in that regulation and that the cooperation and consistency procedures laid down by that regulation are respected.

2. Article 58(5) of Regulation 2016/679 must be interpreted as meaning that, in the event of cross-border data processing, it is not a prerequisite for the exercise of the power of a supervisory authority of a Member State, other than the lead supervisory authority, to initiate or engage in legal proceedings, within the meaning of that provision, that the controller or processor with respect to the cross-border processing of personal data against whom such proceedings are brought has a main establishment or another establishment in the territory of that Member State.

3. Article 58(5) of Regulation 2016/679 must be interpreted as meaning that the power of a supervisory authority of a Member State, other than the lead supervisory authority, to bring any alleged infringement of that regulation to the attention of a court of that Member State and, where appropriate, to initiate or engage in legal proceedings, within the meaning of that provision, may be exercised both with respect to the main establishment of the controller which is located in that authority's own Member State and with respect to another establishment of that controller, provided that the object of the legal proceedings is a processing of data carried out in the context of the activities of that establishment and that that authority is competent to exercise that power, in accordance with the terms of the answer to the first question referred.

4. Article 58(5) of Regulation 2016/679 must be interpreted as meaning that, where a supervisory authority of a Member State which is not the 'lead supervisory authority', within the meaning of Article 56(1) of that regulation, has brought a legal action, the object of which is an instance of cross-border processing of personal data, before 25 May 2018, that is, before the date when that regulation

became applicable, that action may, from the perspective of EU law, be continued on the basis of the provisions 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, which remains applicable in relation to infringements of the rules laid down in that directive committed up to the date when that directive was repealed. That action may, in addition, be brought by that authority with respect to infringements committed after that date, on the basis of Article 58(5) of Regulation 2016/679, provided that that action is brought in one of the situations where, exceptionally, that regulation confers on a supervisory authority of a Member State which is not the 'lead supervisory authority' a competence to adopt a decision finding that the processing of data in question is in breach of the rules contained in that regulation with respect to the protection of the rights of natural persons regarding the processing of personal data, and that the cooperation and consistency procedures laid down by that regulation are respected, which it is for the referring court to determine.

5. Article 58(5) of Regulation 2016/679 must be interpreted as meaning that that provision has direct effect, with the result that a national supervisory authority may rely on that provision in order to bring or continue a legal action against private parties, even where that provision has not been specifically implemented in the legislation of the Member State concerned.

Elements of judicial dialogue

The GDPR precisely organises the dialogue between the DPAs. In **Facebook**, for the first time, the CJEU has, with regard to cooperation, added the adjective "**effective**" to "fair". The term is used four times in the judgment and appears as such in the key words of the judgment, a sign of its importance.

DPAs must respect the competence of the lead authority but at the same time they can exert relative pressure on it. The passivity of the lead authority allows them to apply to the EDPB. They also have the possibility to take urgent measures.

Impact on national case law in Member States different from the one of the court referring the preliminary question

France

see above Question 2 the case Google v. CNIL

Germany

Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI); case WhatsApp. The German authority adopted a preliminary order on 11 May 2021 prohibiting Facebook from further processing user data in Germany. It then sought an urgent positive opinion from the EDPS in order to take final action. The EDPS considered that urgency was not established and that therefore there was no need to bypass the Irish lead authority. The EDPS merely asked the Irish lead authority to investigate the case as a matter of priority.

3. b) - Absence of hierarchy between Member States' data protection authorities exercising competence over the same data processing

3. b) Where different Member State data protection authorities exercise competence over the same data processing because several entities jointly contribute to the processing of data, does the data protection authority of the Member State where the entity mainly responsible for the processing is established have any priority or supremacy over other Member State data protection authorities, to decide on the lawfulness of the processing?

Within the cluster of cases, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

➢ Judgment of the Court (Grand Chamber), 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH & Facebook Ireland Limited, C-210/16 (**Wirtschaftsakademie**)

Relevant legal sources:

EU Level

Directive 95/46/EC 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

Article 4; Article 28

The case

The ULD (a regional German supervisory authority) ordered W, an educational body, to deactivate the fan page it had set up on Facebook to exchange with potential customers, on the ground that neither W. nor Facebook informed visitors of the fan page that Facebook, by means of cookies, collected personal data concerning them and then processed the data.

W. argued that it was not responsible under data protection law for the processing of the data by Facebook or the cookies which Facebook installed, but ULD dismissed its claim. It stated that, by setting up its fan page, W. had made an active and deliberate contribution to the collection by Facebook of personal data relating to visitors of the fan page, from which it profited by means of the statistics provided to it by Facebook.

Both the German Administrative Court (Verwaltungsgericht) and Higher Administrative Court (Oberverwaltungsgericht) concluded that the ULD decision was unlawful, stating, notably, that W. was not a controller entity in relation to the data collected by Facebook. Facebook alone decided on the purpose and means of collecting and processing personal data used for the Facebook Insights function, W receiving only anonymised statistical information.

The ULD appealed to the Bundesverwaltungsgericht (Federal Administrative Court, Germany) which observed, referring to previous CJEU decisions, that the concept of controller should in principle be interpreted broadly, in the interests of effective protection of the right of privacy. Therefore there are doubts as to the powers of the ULD with respect to Facebook Germany, given that it is Facebook Ireland that is responsible, at EU level, for the collection and processing of personal data within the Facebook group. The Federal Administrative Court decided to refer six questions to the CJEU for a preliminary ruling. Questions 5 and 6 are relevant in relation to the question in the box.

Preliminary questions referred to the Court

(5) Are Article 4(1)(a) and Article 28(3) and (6) of Directive [95/46] to be interpreted as meaning that, in cases in which the supervisory authority in one Member State (in this case, Germany) takes action against a person or entity in its territory pursuant to Article 28(3) of Directive [95/46] on the grounds of failure carefully to select a third party involved in the data processing process (in this case, Facebook), because that third party infringes data protection legislation, the active supervisory authority (in this case, Germany) is bound by the appraisal made under data protection legislation by the supervisory authority of the Member State in which the third party responsible for the data processing has its establishment (in this case, Ireland) meaning that it may not arrive at a different legal appraisal, or may the active supervisory authority (in this case, Germany) conduct its own examination of the lawfulness of the data processing by the third party established in another Member State (in this case, Ireland) as a preliminary question prior to its own action?

(6) If the possibility of conducting an independent examination is available to the active supervisory authority (in this case, Germany), is the second sentence of Article 28(6) of Directive [95/46] to be interpreted as meaning that this supervisory authority may exercise the effective powers of intervention conferred on it under Article 28(3) of Directive [95/46] against a person or entity established in its territory on the grounds of their joint responsibility for data protection infringements by a third party established in another Member State only if and not until it has first requested the supervisory authority in this other Member State (in this case, Ireland) to exercise its powers?

In its decision, the CJEU rephrased the questions, which were considered together, as follows:

Should Article 4(1)(a) and Article 28(3) and (6) of Directive 95/46 be interpreted as meaning that, where the supervisory authority of a Member State intends to exercise with respect to an entity established in the territory of that Member State the powers of intervention referred to in Article 28(3) of that directive, on the ground of infringements of the rules on the protection of personal data committed by a third party responsible for the processing of that data whose seat is in another Member State, that supervisory authority is competent to assess, independently of the supervisory authority of the other Member State, the lawfulness of such data processing and may exercise its powers of intervention with respect to the entity established in its territory without first calling on the supervisory authority of the other Member State to intervene?

Reasoning of the Court

After finding that the administrator of a fan page is a controller (see Chapter 2), and that German law is applicable, and the German supervisory authority has competence over, the processing of data even if the entity established in Germany is responsible solely for the sale of advertising space and other marketing activities and if, as a result of the division of tasks within the group, the establishment situated in Ireland has exclusive responsibility for collecting and processing personal data for the entire territory of the EU (see above question 3.a.), the CJEU deals with the issue of the concurring competence of several Member States' data protection authorities resulting from the broad interpretation of Articles 4 and 28.

For the Court, referring to *Schrems I* :

"As provided for by the second subparagraph of Article 28(1) of that directive, the supervisory authorities whose task it is to supervise the application, in the territory of their own Member States, of the provisions adopted by those States pursuant to the directive are to act with complete independence in exercising the functions entrusted to them. That requirement also follows from EU primary law, in particular Article 8(3) of the CFR and Article 16(2) TFEU" (§68).

If supervisory authorities are to cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information, that directive does not lay down any criteria of priority governing the intervention of one supervisory authority as opposed to another, nor does it lay down an obligation for a supervisory authority of one Member State to comply with a position which may have been expressed by the supervisory authority of another Member State. National supervisory authorities are responsible, in accordance with Article 8(3) of the CFREU and Article 28 of Directive 95/46, for monitoring compliance with the EU rules concerning the protection of individuals with regard to the processing of personal data. As a consequence, each of them is vested with the power to check whether the processing of personal data in the territory of its own Member State complies with the requirements laid down by Directive 95/46.

Such an interpretation applies even where, given the allocation of tasks within the group, the establishment exclusively responsible for collecting and processing personal data for the entire territory of the EU has its seat in another Member State: there is no hierarchy between Member States' data protection authorities depending on the level of involvement of the local entity in the processing of data.

This decision of the Court clearly enhances the effectiveness of data protection.

Conclusion of the Court

Articles 4(1)(a) and 28(3) and (6) of Directive 95/46 must be interpreted as meaning that, where the supervisory authority of a Member State intends to exercise with respect to an entity established in the territory of that Member State the powers of intervention referred to in Article 28(3) of that directive, on the ground of infringements of the rules on the protection of personal data committed by a third party responsible for the processing of that data whose seat is in another Member State, that supervisory authority is competent to assess, independently of the supervisory authority of the other Member State, the lawfulness of such data processing and may exercise its powers of intervention with respect to the entity established in its territory without first calling on the supervisory authority of the other Member State to intervene.

Elements of judicial dialogue

-Horizontal: *Weltimmo* and *Schrems I* are reference decisions on which the Court builds this new rule.

The cases in light of the GDPR

The solution adopted in *Wirtschaftsakademie* must be read in light of Article 56 ('Competence of the lead supervisory authority') and Article 60 ('Cooperation between the lead supervisory authority and the other supervisory authorities concerned') applicable to cross-border processing. These provisions, although formally preserving the independence of Member States' supervisory authorities in relation to each other, set up a procedure meant to coordinate their decisions, under the supervision of the lead supervisory authority. Ultimately, the procedure should ensure that the lawfulness of a given processing of data, undertaken jointly by several entities established in different Member States, is not assessed differently in each Member State despite the harmonization of substantive rules as a result of the GDPR.

The lead supervisory authority is the one "*of the main establishment*" of the controller or processor. One question will be to decide whether, in a case such as *Wirtschaftsakademie*, the main establishment should be the one responsible for the processing of data for the entire EU territory.

In any case, Article 56 (2) GDPR states that, "each supervisory authority shall be competent to handle a complaint lodged with it […] if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State".

So the solution adopted in *Wirtschaftsakademie* is no longer relevant (See above, ***Facebook*)**

1.2.5. Questions 4: Coordination between national courts regarding intra-EU cross-border processing

Which court has jurisdiction to order that wrongful data published on a website accessible in several Member States be rectified and/or removed?

Within the cluster of cases, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

➢ Judgment of the Court (Grand Chamber), 17 October 2017, *Bolagsupplysningen OÜ, Ingrid Ilsjan* v *Svensk Handel* AB, Case C-194/16 (***Svensk Handel***)

Cluster of cases:

➢ Judgment of the Court (Grand Chamber), 25 October 2011, *eDate Advertising GmbH* v *X*, and *Olivier Martinez, Robert Martinez* v *MGN Limited*, Cases C-509/09 and C-161/10 (***eDate***)

➢ Judgment of the Court (Grand Chamber), 17 October 2017, *Bolagsupplysningen OÜ, Ingrid Ilsjan* v *Svensk Handel* AB, Case C-194/16 (***Svensk Handel***)

➢ Judgment of the Court (Grand Chamber), 21 December 2021, Gtflix Tv v. DR, Case C-251/20 (***Gtflix***)

Relevant legal sources:

EU Level

Regulation (EU) No. 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters

Recitals 15 and 16

Article 7 (2)

National Level

N/A

The case(s):

Svensk Handel, a trade association incorporated under Swedish law, had included Bolagsupplysningen, a company incorporated under Estonian law, in a 'blacklist' on its website, stating that the company

carried out acts of fraud and deceit. The forum on that site received approximately 1,000 comments, a number of which were direct calls for acts of violence against Bolagsupplysningen and its employees, including Ms Ilsjan.

Bolagsupplysningen and Ms Ilsjan requested Svensk Handel to remove information and comments that allegedly caused them prejudice. Since Svensk Handel refused to comply, they brought an action against Svensk Handel before the Harju Maakohus (Harju Court of First Instance, Estonia), requesting the court to order Svensk Handel to rectify incorrect information and to delete the comments that appeared on the website, to pay Bolagsupplysningen the amount of EUR 56,634.99 as compensation for sustained harm and to pay Ms Ilsjan fair compensation for non-material damage, as assessed by the court.

The Harju Maakohus (Harju Court of First Instance) held that the action was inadmissible. It could not assume jurisdiction on the basis of article 7(2) of Regulation No. 1215/2012, since it did not appear from the application that the damage had occurred in Estonia. The court found that: (1) the information and comments were published in Swedish and, without a translation, they were incomprehensible to persons residing in Estonia; (2) the occurrence of damage in Estonia had not been proved and the reference to turnover in Swedish kronor suggested that the damage had been caused in Sweden; (3) the fact that the website at issue was accessible in Estonia could not automatically justify an obligation to bring a civil case before an Estonian court.

The claimants lodged an appeal against that decision, which was dismissed by the Tallinna Ringkonnakohus (Tallinn Court of Appeal, Estonia). The claimants brought the case before the Riigikohus (Supreme Court, Estonia).

The Estonian Supreme Court considered that, concerning Ms Ilsjan, the appeal against the order of the Tallinna Ringkonnakohus (Tallinn Court of Appeal) was well founded, that the orders of that court and of the Harju Maakohus (Harju Court of First Instance) must be set aside and that the case must be referred back to the Harju Maakohus (Harju Court of First Instance) so that it could rule on the admissibility of Ms Ilsjan's claims.

Concerning the application lodged by Bolagsupplysningen, the Supreme Court took the view that it fell within the jurisdiction of the Estonian courts, at least with regard to the claim for compensation for damage that occurred in Estonia.

With regard to the claim related to the publication of the incorrect information causing harm to the company's good name and reputation, the Supreme Court observed that, according to previous CJEU case-law, injury caused by a defamatory publication to the reputation and good name of a legal person occurs in the places where the publication is distributed and in which the victim claims to have suffered injury to its reputation.

Having said that, the Supreme Court expressed doubts on: (1) whether Bolagsupplysningen could, on that basis, also seek the rectification of the incorrect information and the deletion of the comments before an Estonian court; (2) whether Bolagsupplysningen could also seek compensation for the entirety of the damage that it claimed to have suffered before the Estonian courts; (3) whether the seat and/or the place of business of a legal person provide sufficient grounds for assuming that the centre of interests of that legal person is also located there. The decision was taken to refer the question to the CJEU.

Preliminary question referred to the Court:

(1) Is Article 7(2) of [Regulation No 1215/2012] to be interpreted as meaning that a person who alleges that his rights have been infringed by the publication of incorrect information concerning him on the internet and by the failure to remove comments relating to him can bring an action for

rectification of the incorrect information and removal of the harmful comments before the courts of any Member State in which the information on the internet is or was accessible, in respect of the harm sustained in that Member State?

(2) Is Article 7(2) of [Regulation No 1215/2012] to be interpreted as meaning that a legal person which alleges that its rights have been infringed by the publication of incorrect information concerning it on the internet and by the failure to remove comments relating to that person can, in respect of the entire harm that it has sustained, bring proceedings for rectification of the information, for an injunction for removal of the comments and for damages for the pecuniary loss caused by publication of the incorrect information on the internet before the courts of the State in which that legal person has its centre of interests?

(3) If the second question is answered in the affirmative: is Article 7(2) of [Regulation No 1215/2012] to be interpreted as meaning that:

–it is to be assumed that a legal person has its centre of interests in the Member State in which it has its seat, and accordingly that the place where the harmful event occurred is in that Member State, or

–in ascertaining a legal person's centre of interests, and accordingly the place where the harmful event occurred, regard must be had to all of the circumstances, such as its seat and fixed place of business, the location of its customers and the way and means in which its transactions are concluded?'

Reasoning of the Court:

The Court deals firstly with questions 2 and 3, which are joined as follows: Should Article 7(2) of Regulation No 1215/2012 be interpreted as meaning that a legal person claiming that its personal rights have been infringed by the publication of incorrect information concerning it on the internet and by a failure to remove comments relating to that person can bring an action for rectification of that information, removal of those comments and compensation in respect to all the damage sustained before the courts of the Member State in which its centre of interests is located and, if that is the case, what are the criteria and the circumstances to be taken into account to determine that centre of interests. In other terms, which is the Court with jurisdiction, pursuant to Article 7(2) of Regulation Brussels I (revised), in a case such as the case at hand?

The Court recalls its previous interpretation of Article 5(2) of Regulation Brussels I and 7(2) of revised Regulation Brussels I, according to which, in tort matters, the victim may bring its claims before the courts of the Member State where the alleged damage occurred. The Court builds on the *Fiona Shevill* and *eDate* decisions concerning injuries caused to reputation and explains that, if the former decided, in the case of a harmful publication by way of printed press, that the victim had to fragment its claims "before the courts of each Member State in which the publication was distributed and where the victim claims to have suffered injury to his reputation, which have jurisdiction to rule solely in respect of the harm caused in the Member State of the court seised", the latter decided differently in the case of a harmful publication by way of the internet. In the context of the internet, the natural person suffering a harm has the option to bring the action concerning their entire damage before the courts of the Member State where they has the centre of their interests.

The rationale for this criterion is that:

"the alleged infringement is usually felt most keenly at the centre of interests of the relevant person, given the reputation enjoyed by him in that place. Thus, the criterion of the 'victim's centre of interests' reflects the place where, in principle, the damage caused by online material occurs most significantly. The courts of the Member State in which the centre of interests of the person affected is located are, consequently, best placed to assess the impact of such content on the rights of that person. Moreover, the criterion of the centre of interests accords with the aim of predictability of the rules governing

jurisdiction, since it allows both the applicant easily to identify the court in which he may sue and the defendant reasonably to foresee before which court he may be sued" (§33-35).

Because this approach is justified in the interests of the sound administration of justice, and not for the purpose of protecting the victim of the harmful publication, there is no reason why it should not also apply to legal persons. Consequently, a company suffering harm to its reputation because of an internet publication of false information may bring an action for compensation for its entire damage and for an injunction to remove the harmful information, before the courts of the Member State where it has the centre of its interests.

Concerning the location of the centre of interests, the Court recalls its findings in *eDate*, according to which the centre of interests of a natural person generally corresponds to the Member State of their habitual residence; however, such a person may also have his centre of interests in a Member State in which he does not habitually reside, in so far as other factors, such as the pursuit of a professional activity, may establish the existence of a particularly close link with that State. For legal persons pursuing an economic activity, the centre of interests must reflect the place where their commercial reputation is most firmly established and must, therefore, be determined by reference to the place where they carry out the main part of its economic activities. While the centre of interests of a legal person may coincide with the place of their registered office when they carry out all or the main part of their activities in the Member State in which that office is situated and the reputation that they enjoy there is consequently greater than in any other Member State, the location of that office is not in itself a conclusive criterion for the purposes of such an analysis.

"When the relevant legal person carries out the main part of its activities in a Member State other than the one in which its registered office is located, as is the case in the main proceedings, it is necessary to assume that the commercial reputation of that legal person, which is liable to be affected by the publication at issue, is greater in that Member State than in any other and that, consequently, any injury to that reputation would be felt most keenly there. To that extent, the courts of that Member State are best placed to assess the existence and the potential scope of that alleged injury, particularly given that, in the present instance, the cause of the injury is the publication of information and comments that are allegedly incorrect or defamatory on a professional site managed in the Member State in which the relevant legal person carries out the main part of its activities and that are, bearing in mind the language in which they are written, intended, for the most part, to be understood by people living in that Member State" (§42).

The Court then considers the first question, whether a person who alleges that their personal rights have been infringed by the publication of incorrect information concerning them on the internet and by the failure to remove comments relating to them can bring an action for rectification of that information and removal of those comments before the courts of each Member State in which the information published on the internet is or was accessible. The Court answers in the negative, since it is necessary to separately consider actions brought for compensation for damage, which might be fragmented as decided in *eDate*, and an action brought for an injunction to rectify and/or remove information from the website. The latter is a single and indivisible application and can, consequently, only be made before a court with jurisdiction to rule on the entirety of an application for compensation for damage (as defined above).

In this decision, the Court *implicitly relies on the* ***principle of effective access to justice*** ("The courts of the Member State in which the centre of interests of the person affected is located are, consequently, best placed to assess the impact of such content on the rights of that person") *and on the* ***principle of proportionality*** (by balancing the applicant's interest in easily identifying the court in which they may sue, with the defendant's interest in reasonably foreseeing which court they may be sued in) to propose

the criteria on which the national courts' jurisdiction may be assessed in cases where the claim concerns an order to rectify or remove information/data.

Conclusion of the Court:

A person who alleges that their personal rights have been infringed by the publication of incorrect information concerning them on the internet and by the failure to remove comments relating to them cannot bring an action for rectification of that information and removal of those comments before the courts of each Member State in which the information published on the internet is or was accessible. Such action may only be brought before courts having jurisdiction to rule on the entirety of an application for compensation for damage.

Such an action may be brought by a legal entity, in particular, before the courts of the Member State in which its centre of interests is located. When the legal entity carries out the main part of its activities in a different Member State from the one in which its registered office is located, it may sue the alleged perpetrator of the injury in that other Member State because that is where the damage occurred.

Elements of judicial dialogue:

- **Horizontal (within the CJEU):**

The issue of judicial dialogue within the CJEU is an important one. Beyond the fact that the Court refers in its reasoning (see above) to several previous decisions, notably in *Fiona Schevill* and *eDate*, the main question is the link to be made between the Court's case law relating to the interpretation of EU instruments which are specific to data protection, and that relating to the interpretation of more general EU instruments such as, in the case discussed, Regulation Brussels I.

EU legislation specifically dealing with data protection includes special rules concerning the law applicable to cross-border situations (see above, under question 1). But it does not include any specific rule on the jurisdiction of national courts in cross-border situations. Claimants and courts thus have to rely on the general rules, set by Regulation Brussels I/Brussels I bis, applying in civil and commercial matters.

- **Vertical**

The French Court of cassation (Cour de cassation made a request for a preliminary ruling concerns the interpretation of Article 7(2) of Regulation (EU) No 1215/2012 (decision of 13 May 2020) and suggested an evolution

The request has been made in proceedings between Gtflix Tv, an adult entertainment company established in the Czech Republic, and DR, another professional in that field, domiciled in Hungary, concerning an application for rectification and removal of allegedly disparaging comments about that company which DR placed online on several websites and internet forums and a claim for compensation for the damage allegedly suffered as a result.

In light of Svensk Handel, the court of cassation determined that the French courts had no jurisdiction to hear the application for the removal of allegedly disparaging comments and the rectification of information by the publication of a statement, on the grounds, *inter alia*, that Gtflix Tv's centre of interests was established in the Czech Republic and that DR is domiciled in Hungary. However, the court had doubts as to whether a person who, considering that their rights have been infringed by the dissemination of disparaging comments on the internet, seeks not only the rectification of the information and the removal of the content but also compensation for the resulting non-material and economic damage, may claim, before the courts of each Member State in which content published online is or was accessible, compensation for the damage caused in that Member State, or whether that person must make that

application for compensation before the court with jurisdiction to order rectification of the information and removal of the disparaging comments.

The French Court of Cassation decided to stay the proceedings and to refer the following question to the CJEU: 'Must Article 7(2) of Regulation No 1215/2012 be interpreted as meaning that a person who, considering that his or her rights have been infringed by the dissemination of disparaging comments on the internet, brings proceedings not only for the rectification of data and the removal of content but also for compensation for the resulting non-material and economic damage, may claim, before the courts of each Member State in the territory of which content published online is or was accessible, compensation for the damage caused in the territory of that Member State, in accordance with *eDate* or whether, pursuant *Svensk Handel*, that person must make that application for compensation before the court with jurisdiction to order rectification of the information and removal of the disparaging comments?'

The CJEU recalled *Shevill, eDate and Svensk Handel* and rejected the idea that the "necessary link of dependence" between these claims weighed in favour of the exclusive jurisdiction of the courts competent to rule on the entire damage. In this respect, the Court held that while applications for rectification of information and removal of content are single and indivisible in nature and may therefore warrant the concentration of jurisdiction upon a limited number of courts, no such justification exists for claims of compensation. Then, the Court dismissed the argument that a "necessary link of dependence" exists between applications for injunctive relief and actions for damages, as "their purpose, their cause and their divisibility are different, and there is therefore no legal necessity that they be examined jointly by a single court". The Court also considered that a concentration of jurisdiction would not always serve the interests of the sound administration of justice. Finally, the Court rejected the argument formulated by AG Hogan according to which, should the Court uphold the mosaic approach to jurisdiction inaugurated in *Shevill*, the reference to the place where the damage occurred should only be interpreted to cover the Member States where the publication in question is concretely "directed". On the basis of its case law on infringement of intellectual property rights, the Court held that the wording of Article 7(2) does not impose any additional condition regarding the determination of the competent court.

The balance between the interests of the plaintiff and the interests of the defendant is dangerously tilted towards the former.

The solution is highly questionable as it ignores the fact that the two parties were in competition.
The Grand Chamber, by emphasising the plaintiff's option to bring an action before the courts of any place where the damage occurred, stands in contrast with some of the CJEU's most recent decisions under Article 7(2) relating to infringements on competition law (see for example Case C800/19, *Mittelbayerischer Verlag KG* and Case C709/19, *Vereniging van Effectenbesitzers*) stressing the predictability needed by interpreting this provision.

Impact on national case law in Member States different from the state of the court referring the preliminary question to the CJEU:

See *Gtflix* in the Section above.

Input of the GDPR on the jurisdiction of courts:

The GDPR, which establishes a "right to an effective judicial remedy against the controller or processor" for the data subject whose rights have been infringed (see Chapter 6), introduces a specific rule on the jurisdiction of courts over such claims.

Article 79 (2) (and Recital 145) reads:

"2. Proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers."

The GDPR thus creates a specific rule on jurisdiction in favour of the data subject, who may bring their claim before the courts of the Member State of their own habitual residence. This favouring rule is quite similar to the one laid down by Regulation Brussels I / Brussels I bis in favour of consumers.

Article 79 (2) is to be read in light of Recital 147 of the Preamble of the GDRP:

"Where specific rules on jurisdiction are contained in this Regulation, in particular regarding proceedings seeking a judicial remedy including compensation, against a controller or processor, general jurisdiction rules such as those of Regulation (EU) No 1215/2012 of the European Parliament and of the Council (13) should not prejudice the application of such specific rules".

The effect of this recital should be that, if the claim of the data subject is based on contract or tort law, which will often be the case, the controller will not be able to oppose the rules laid down by Regulation Brussels I bis for contractual and tort matters, on the basis of which the CJEU case law has so far been developed.

1.3. Relations with third countries

Directive 95/46 dedicated a whole chapter (Chapter IV: Transfer of personal data to third countries) to relations with third countries, where the level of protection of data might be much lower than what is required by EU legislation. Based on the principle of sovereignty, it is for each State to define what protection applies in its territory. However, the intangible nature of data is not strictly compatible with an approach purely relying on national regulation applying in one given territory. The effectiveness of the protection calls for a more global solution, which implies political negotiations between States. The discussions with the USA, in particular, have been essential, since most major digital businesses are established there. A first decision of the Commission (Decision 2000/520/EC of 26 July 2000), whereby the Commission found that the USA "Safe Harbor Privacy Principles" were to be considered as ensuring an adequate level of protection for personal data transferred from the Community to organisations established in the United States, raised strong opposition and was finally held invalid by the CJEU. Further negotiation had to be undertaken with the USA, and ultimately led to the "Privacy Shield". Then, on the 16 of July 2020, in *Facebook Ireland Ltd, Maximillian Schrems* (C-311/18) the CJEU declared invalid the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield.

And in the meantime, the CJEU has had to provide safeguards for EU citizens, using in particular the rights enshrined in the Charter.

Identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

➢ Judgment of the Court, (Grand Chamber), 6 October 2015, *Schrems* v. *Data Protection Commissioner*, C-362/14 (***Schrems I***)

Relevant legal sources:

EU Level

Directive 95/46 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

Article 25 (1) (2) (4) (5) & (6) - Principles

Article 28 - Supervisory authority

Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.

Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related frequently asked questions issued by the US Department of Commerce

By this decision, the Commission decided that, for all the activities falling within the scope of Directive 95/46, the "Safe Harbor Privacy Principles" implemented in accordance with the guidance provided by the frequently asked questions (hereinafter "the FAQs") issued by the US Department of Commerce on 21 July 2000 are considered as ensuring an adequate level of protection for personal data transferred from the Community to organisations established in the United States.

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

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 [GDPR]

Chapter V (Articles 44 and seq.)

National Level

Irish Data Protection Act 1988 Irish Constitution

Articles 40 (personal rights, including the right to privacy) and 41 (protection of family life)

1.3.1. Question 5 & 6: The scrutiny of third countries' legislation in terms of EU law and its consequences

Should Member States' data protection authorities assess the adequacy of data protection in third countries, where personal data collected in the EU is to be transferred, in terms of EU principles and/or legislation?
Should they find that the data protection offered in a third country is not adequate, should Member States oppose the transfer of personal data collected in the EU to that country?

The case(s):

Mr Schrems, an Austrian national residing in Austria, had been a user of the Facebook social network ('Facebook') since 2008. In the EU, at the time they registered on Facebook, each user had to conclude a contract with Facebook Ireland, a subsidiary of Facebook Inc., which is itself was incorporated in the United States. Some or all of the personal data of EU residents are transferred to servers belonging to Facebook Inc., in the United States, where they are processed.

Mr Schrems lodged a complaint with the Irish Data Protection Commissioner, requesting that Facebook Ireland be prohibited from transferring his personal data to the United States. He contended that the law and the practices of the country did not ensure adequate protection of personal data.

The Commissioner concluded that the complaint was unfounded, considering he was bound on the matter by the European Commission Decision 2000/520, which establishes that the US – through its Safe Harbor Privacy Principles – ensures an adequate level of protection.

Mr Schrems challenged the decision before the High Court of Ireland. The High Court found that the electronic surveillance and interception of personal data transferred from Europe to the United States served necessary and indispensable objectives in the public interest. However, the Court judged that mass and undifferentiated access to personal data was contrary to the principle of proportionality and to fundamental values protected by the Irish Constitution, such as the rights to privacy, the inviolability of the dwelling and the right to be heard. According to the Court, in view of the serious doubt whether US procedures guaranteed protection of these rights, the Commissioner should have investigated the complaint; however, the Court also recognized that the lawfulness or otherwise of the Commissioner's determination was dependent on the interpretation of Directive 95/46 and the validity of Decision 2000/520 in light of the CFREU and of the principles expressed by the CJEU in *Digital Rights Ireland.*

Preliminary question referred to the Court:

Whether and to what extent Article 25(6) of Directive 95/46, read in light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, prevents a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from being able to examine the claim of a person concerning the protection of their rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection?

Reasoning of the Court:

The Court reaffirms the role of national supervisory authorities in light of the fundamental rights guaranteed by the Charter (especially Articles 7, 8 and 47) and of Article 25 of Directive 95/46, which is to ensure a high level of protection of the fundamental rights of individuals. Accordingly, *national supervisory authorities are responsible for verifying whether a transfer of personal data from their own Member State to a third country complies with Directive 95/46 – i.e., whether an adequate level of protection in ensured.* Otherwise, in an **implicit application of the principle of effectiveness**, the Court observes that data subjects "would be denied the right, guaranteed by Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim for the purpose of protecting their fundamental rights". For the Court, it follows from this that the level of protection offered by the United States has to be scrutinised according to EU standards.

The Court then engages in an analysis to define which authority within the EU is competent to undertake that scrutiny. The Court makes a distinction, depending on whether or not there is any decision of the European Commission finding that the third country to which data is transferred ensures an adequate level of protection. If the Commission has already assessed the adequacy of the level of protection offered in a third country, only the Court has competence to decide whether such a decision is valid, and the Court's decision is binding on national authorities and courts. In the absence of such decision, it would be Member States' responsibility, through their supervisory authorities and/or their courts, to make such an assessment (on this issue, see the discussion in Chapter 4).

In the present case, since the European Commission has adopted a decision on the level of protection in the United States, which is binding on Member States, only the Court may decide on the validity of the Commission's decision, which implies that the Court must assess whether the level of protection offered in the United States is sufficient, in terms of EU principles. On the validity of Decision 2000/520, first of all, the Court observes that compliance with the Safe Harbour Principles, issued by the US Department of Commerce and deemed by the Commission to ensure adequate protection, is based on a self-certification system; that the principles do not apply to US public authorities; and that their application may be limited on the grounds of national security, public interest, or law enforcement. Notwithstanding the general nature of this derogation, Decision 2000/520 does not refer to any US rules that limit interference with the fundamental rights of data subjects, nor to effective remedies against such interference. The Court underlines that EU legislation that interferes with the rights protected by Articles 7 and 8 CFREU must clearly delimit the scope and application of restrictive measures and impose minimum safeguards; that any derogations from the protection of personal data must be strictly necessary; and that legal remedies must be available, pursuant to Article 47 CFREU. According to the Court, "the Commission did not state, in Decision 2000/520, that the United States in fact 'ensures' an adequate level of protection by reason of its domestic law or its international commitments". The decision is declared invalid.

By this reasoning, the Court instructs Member States' supervisory authorities and courts (where there is no previous decision of the Commission) to engage in the assessment of the compatibility of foreign legislation with EU principles, in particular **the principle of proportionality**. With regard to the generalised access by US authorities to personal data transferred from the EU, the CJEU confirms that the right to respect for private life can be limited only insofar as strictly necessary, and that US "legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the EUto the United States without any differentiation, limitation or exception". Accordingly, such legislation would infringe the essence of the right protected by Article 7 CFREU.

When it appears that the level of protection in a third country is not sufficient from the assessment made by the Court or by national authorities and/or courts, the Member State's supervisory authorities are required to oppose the transfer of personal data, by a controller established in that Member State, to another controller established in that third country (the United States) where the processing of personal data is to be undertaken.

Conclusion of the Court:

Article 25(6) of Directive 95/46, read in light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520 pursuant to Directive 95/46 on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as

amended, from examining the claim of a person concerning the protection of their rights and freedoms in regard to the processing of personal data relating to him, which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.

Article 1 of the Commission's decision 2000/250, according to which the Safe Harbour Principles, issued by the US Department of Commerce, are deemed to ensure adequate data protection, is invalid, as is Article 3, inasmuch as it unlawfully restricts the powers of national supervisory authorities by essentially precluding them from acting to ensure compliance with article 25 of Directive 95/46. The CJEU concludes that the decision as a whole is invalid.

Impact on the follow-up case:

On 20 October 2015, the Irish High Court set aside the decision by the Irish Data Protection Commissioner not to investigate the complaint lodged by Mr. Schrems.

The Commissioner then initiated an investigation into the complaint filed by Mr Schrems. At the end of the investigation, the Commissioner preliminarily found that Mr Schrems' complaint was well-founded: on 31 May 2016, the Commissioner therefore commenced proceedings before the Irish High Court seeking a preliminary reference to the CJEU in relation to the Standard Contractual Clauses, which have been used by US companies following the declaration of invalidity of Decision 2000/520.

On 3 October 2017, the High Court made a referral to the CJEU (***Schrems II***) concerning the validity of the European Commission's decisions enshrining the said contractual clauses (*High Court (Commercial), Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems, 2016 No. 4809 P.*), namely:

(1) Commission Decision 2001/497/EC of 15 June 2001, on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC (Text with EEA relevance) (notified under document number C(2001) 1539) [2001] OJ L181, 4.7.2001, pp. 19-31;
(2) Commission Decision 2004/915/EC of 27 December 2004, amending Decision 2001/497/EC regarding the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (notified under document number C(2004) 5271) (Text with EEA relevance) [2004] OJ L385, 29.12.2004, pp.74-84; and,
(3) Commission Decision 2010/87/EU of 5 February, 2010, on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593) (Text with EEA relevance) [2010] OJ L39, 12.2.2010, p. 5-18.
After Decision 2000/520 was declared invalid by the CJEU, US companies started to apply alternative existing contractual instruments approved by the European Commission, i.e., the Binding Corporate Rules and the Standard Contractual Clauses. However, a new general framework for transfers of personal data from the EU to the US was deemed necessary, and the European Commission and US government — which were already negotiating a new package — accelerated talks. On 12 July 2016, Commission Implementing Decision 2016/1250 pursuant to Directive 95/46 on the adequacy of the protection provided by the EU-U.S. Privacy Shield was adopted. Notwithstanding improvements (such as the oversight role of the new US Ombudsman), several persistent shortcomings have been pointed out by the national supervisory authorities and the European Parliament, among others, and legal challenges against the new decision can be foreseen. In fact, two actions for annulment of Commission Implementing Decision 2016/1250, essentially based on its incompatibility with Articles 7, 8 and 47 CFREU, have already been brought before the EU General Court: these are *La Quadrature du Net and Others v Commission* (Case T-738/16) and *Digital Rights Ireland v Commission* (Case T-670/16).

Elements of judicial dialogue:

The CJEU referred several times to *Schrems I* in relation to the questions in the box, notably:

- in *Tele2* (C-203/15 & C-698/15), where the Court referred to the proportionality test implemented in *Schrems* to assess the admissibility of derogations from data protection;

-in *Wirtschaftsakademie* (C-210/16), for the ruling on the independence of Member State data protection authorities in relation to each other.

New perspectives based on the GDPR:

The GDPR includes one chapter (Chapter V) dedicated to the "transfer of personal data to third countries or international organisations", which strongly reinforces the control and guarantees, as compared to what existed under previous EU legislation.

While the general principles laid down by Article 44 are in line with the former principles, the guidelines to the Commission, with the view of adopting a decision on adequacy (Article 45) are very detailed.

Where there is no decision on adequacy, transfers are subjected to "appropriate safeguards" described in Article 46. A decisive role is given, in this context, to self-regulation: approved codes of conduct pursuant to Article 40; approved certification mechanisms pursuant to Article 42; binding corporate rules in accordance with Article 47, etc. Having recourse to self-regulation, duly monitored by Member States' supervisory authorities, is a very interesting means of giving EU legislation an extraterritorial reach without frontally violating the principles of sovereignty.

The GDPR also calls for international cooperation for the dat protection (Article 50). It should be noted that the GDPR also includes a blocking provision, according to which "any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter" (Article 48).

Recital 104 states that the third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where personal data are processed in one or several specific sectors. In particular, the third country should ensure effective independent data protection supervision and should provide for cooperation mechanisms with the Member States' data protection authorities, and the data subjects should be provided with effective and enforceable rights and effective administrative and judicial redress.

Article 45 (2) specifies: When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

(a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation, both general and sectoral, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organisation which are complied with in that country or international organisation, case-law, as well as effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred;

(b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

(c) the international commitments the third country or international organisation concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

1.4. Further developments in CJEU case-law: Facebook Ireland Ltd, Maximillian Schrems (C-311/18), 16 July 2020

In the Judgment of 16 July 2020 (*Facebook Ireland Ltd, Maximillian Schrems*, C-311/18) the CJEU added further component to the standpoint expressed in the previous case law (especially in ***Schrems I***). Amongst other issues, the Court dealt with the territorial scope of application of the GDPR rules to data transfers between EU Members and non-EU states. As was found out, under Article 2(1) and (2) GDPR, the EU data protection standard applies to transfers of data, carried out for commercial purposes, even if one of the parties is established in a non-Member State. This pertains also to situations when at the moment when transfer occurs, 'that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.'

The CJEU found that under Article 46 (1) and (2)(c) GDPR the subjects of data transferred outside of the EU must receive proper safeguards, rights and remedies that are required by the GDPR, equal to the protection enjoyed under the EU law.

Furthermore, the CJEU stated that according to Article 58(2)(f) and (j) of Regulation 2016/679, unless there is a valid European Commission adequacy decision, the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses adopted by the Commission, if, in the view of that supervisory authority and in light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 of that regulation and by the CFR, cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.

Furthermore, the CJEU declared the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield invalid.

The High Court (Ireland) focused on judicial protection and stated that:

- EU citizens do not have the same remedies as US citizens in respect of the processing of personal data by the US authorities, since the Fourth Amendment to the Constitution of the United States, which constitutes, under United States law, the most important cause of action available to challenge unlawful surveillance, does not apply to EU citizens.
- there are substantial obstacles in respect of the causes of action open to EU citizens, in particular that of *locus standi*, which it considers to be excessively difficult to satisfy.

- the NSA's activities based on E.O. 12333 are not subject to judicial oversight and are not justiciable.
- the Privacy Shield Ombudsperson is not a tribunal within the meaning of Article 47 of the Charter, US law does not afford EU citizens a level of protection essentially equivalent to that guaranteed by the fundamental right enshrined in that article.

In this regard, the CJEU considers:

- that the first paragraph of Article 47 requires everyone whose rights and freedoms guaranteed by the law of the Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. According to the second paragraph of that article, everyone is entitled to a hearing by an independent and impartial tribunal.

- the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to them, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as established in Article 47 of the Charter (*Schrems I*)

- the existence of effective redress in the third country concerned is of particular importance in the context of the transfer of personal data to that third country, since, as is apparent from recital 116 of the GDPR, data subjects may find that the administrative and judicial authorities of the Member States have insufficient powers and means to take effective action in relation to data subjects' complaints based on allegedly unlawful processing, in that third country, of their data thus transferred, which is capable of compelling them to resort to the national authorities and courts of that third country.

- the Commission's finding in the Privacy Shield Decision that the United States ensures a level of protection essentially equivalent to that guaranteed in Article 47 of the Charter has been called into question on the ground, *inter alia*, that the introduction of a Privacy Shield Ombudsperson cannot remedy the deficiencies which the Commission itself found in connection with the judicial protection of persons whose personal data is transferred to that third country.

- The lack of any redress mechanism when U.S. intelligence authorities are concerned is a *lacuna* in judicial protection. Therefore United States law does not ensure a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter.

- data subjects must have the possibility of bringing legal action before an independent and impartial court in order to have access to their personal data, or to obtain the rectification or erasure of such data. The Ombudsperson Mechanism in the United States cannot be deemed to ensure a level of protection essentially equivalent to that guaranteed by Article 47 of the Charter as long as the ombudsman directly reports to the Secretary of State who has appointed them.

The CJEU concludes that Article 1 of the Privacy Shield Decision is incompatible with Article 45(1) of the GDPR, read in light of Articles 7, 8 and 47 of the Charter, and is therefore invalid.

Impact on national case law in Member States different from the state of the court referring the preliminary question to the CJEU:

After *Schrems II*, an association (Noyb) has filled **101 Complaints filed concerning companies in 30 EU and EEA member states** that still transfer data about each visitor to Google and Facebook in the US, in violation of the GDPR.

After receiving complaints, Data Protection Authorities cooperated and analysed the conditions under which the data collected through Google Analytics is transferred to the United States.

In a decision of the 12 January 2022, the Austrian Data Protection Authority ("Datenschutzbehörde" or "DSB") decided on a model case by noyb that the continuous use of Google Analytics violates the GDPR.

In a decision of the 10 February 2022, the French CNIL considered that the transfers are illegal and orders a French website manager to comply with the GDPR and, if necessary, to stop using this service under the current conditions.

1.5. Guidelines emerging from the analysis

1. While assessing the adequacy of data protection provided by third-state legal systems, EU courts need to take into consideration the substantive provisions of the GDPR in light of the CFREU. The existence of an adequacy decision is not sufficient to authorise the transfer to the third country concerned by that decision that can be challenged

2. The right to be forgotten (de-referencing) is effective against every version of search engine that are in use in EU Member States. The search engines that function outside of the EU territorial domain, where necessary, should use measures which effectively prevent (or at 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.

3. In cross-border cases, the issue of applicable law is not addressed in the GDPR. Domestic data protection authorities and domestic courts may apply their domestic law. The consistency of the data protection in the EU is then not ensured. Judges could refer to the CJEU whether they should leave their national law unapplied to ensure either better data protection or greater legal certainty.

4. The competence of national authorities is limited by the one-stop shop mechanism set up by the GDPR. This is not the case for some kind of data protection rules (directive e-privacy). This is also not the case for the jurisdiction of the court to which the data subject's request is referred or before which a collective action is brought. Consequently, while establishing jurisdiction in data protection cases, courts should not pay decisive attention to the domicile of a party against whom the supervisory proceedings are carried out. Instead, it should focus on the habitual residence of the data subject.

5. The courts of each Member State in which disparaging comments are or were accessible have jurisdiction to hear the case, but the compensation sought is limited to the damage suffered within the Member State of the court seised. For the rectification of incorrect information and the removal of disparaging comments affecting their reputation, only the courts competent to rule on the entirety of the damage have jurisdiction. These courts are those of the Member State in which the publisher of that content is established or before the courts of the Member State in which the plaintiff's centre of interests is based.

2. Impact of the Charter on the material scope of data protection[1]

2.1. Introduction

Until the coming into force of the GDPR in May 2018, the material scope of EU data protection was defined by **Article 3(1) of Directive 95/45**, pursuant to which "this Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system". Article 3(2) limited the material scope of the protection by expressly excluding its application to the processing of personal data realised: (first indent) "in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on EU and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law"; or (second indent) "by a natural person in the course of a purely personal or household activity".

Article 2 of the GDPR titled "Material scope" reads:

(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) This Regulation does not apply to the processing of personal data:

(a) in the course of an activity which falls outside the scope of Union law;

(b) by the Member States when carrying out activities which fall within the scope of Chapter 2 of Title V of the TEU;

(c) by a natural person in the course of a purely personal or household activity;

(d) 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.

(3) For the processing of personal data by the Union institutions, bodies, offices and agencies, Regulation (EC) No 45/2001 applies. Regulation (EC) No 45/2001 and other Union legal acts applicable to such processing of personal data shall be adapted to the principles and rules of this Regulation in accordance with Article 98.

(4) This Regulation shall be without prejudice to the application of Directive 2000/31/EC, in particular of the liability rules of intermediary service providers in Articles 12 to 15 of that Directive.

This Chapter analyses how, based on the Charter and/or of the principles of effectiveness and proportionality, the CJEU has interpreted Article 3 of Directive 95/45 and Article 2 of the GDPR to define the general scope of the protection.

[1] We thank Andrea M. Garofalo (University of Trento) for his contribution in editing this chapter and enriching it with special regard to German legislation and caselaw.

Main questions addressed

1. What is "personal data" in the perspective of the Charter? How does the CJEU's case-law define the array of personal data? What elements go beyond this scope?

2. What is "processing" of personal data? What types of operations constitute "processing" in the meaning of the EU data protection law and in light of Article 47 CFREU and the principle of effective protection?

3. a) In light of the principle of effectiveness of data protection, how should the concept of "controller" of the processing of personal data be interpreted under EU Data protection? Can the Charter and the principle of effective protection influence this concept?

b) In light of the principle of effectiveness of data protection, what are the circumstances under which an operator, who is not the data processor, should be considered as having "joint control" over the data processing?

4. In light of the principle of effectiveness of data protection, how should the concept of "data subject" be interpreted within the meaning of EU law on data protection?

2.1.1. Question 1: Definition of the concept of "personal data"

1) What is "personal data" in the perspective of the Charter? How does the CJEU case-law define the array of personal data? What elements are beyond this scope?

Within the cluster of cases, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

➢ Judgment of the Court (Second Chamber), 19 October 2016, *Patrick Breyer v. Bundesrepublik Deutschland*, Case C-582/14 (Breyer)

Cluster of relevant CJEU cases

➢ Judgment of the Court, 6 November 2003, *Bodil Lindqvist*, Case C-101/01 (**Lindqvist**)

➢ Judgment of the Court (Grand Chamber), 16 December 2008, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy*, Case C-73/07 (**Satamedia**)

➢ Judgment of the Court (Grand Chamber), 9 November 2010, *Volker und Markus Schecke GbR & Hartmut Eifert v Land Hessen*, Joined cases C-92/09 & C-93/09 (**Volker**)

➢ Judgment of the Court (Third Chamber), 24 November 2011, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Case C-70/10 (**Scarlet Extended**)

➢ Judgment of the Court (Third Chamber), 30 May 2013, W*orten – Equipamentos para o Lar SA v Autoridade para as Condições de Trabalho* (ACT), Case C-342/12, (**Worten**)

➢ 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*, Case C-131/12 (**Google Spain**)

➢ Judgment of the Court (Second Chamber), 19 October 2016, *Patrick Breyer v. Bundesrepublik Deutschland*, Case C-582/14 (**Breyer**)

➢ Judgment of the Court (Second Chamber), 20 December 2017, *Nowak v Data Protection Commissioner*, Case C-434/16 (**Nowak**)

➢ Judgment of the Court (Second Chamber), 14 February 2019, *Sergejs Buivids*, Case C-345/17 (**Buivids**)

➢ Judgement of the Court (Grand Chamber), 24 September 2019, *GC, AF, BH et ED v CNIL*, Case C-136/17 (**CNIL**)

➢ Judgement of the Court (Third Chamber), 11 December 2019, *TK v Asociația de Proprietari bloc M5A-ScaraA*, Case C-708/18 (**TK**)

➢ Judgement of the Court (Grand Chamber), 6 October 2020, *La Quadrature du Net and Others v Premier ministre and Others*, Joined Cases C-511/18, C-512-18 and C-520/18 (**La Quadrature du Net**)

➢ Judgement of the Court (Fifth Chamber), 17 Juni 2021, *Mircom International Content Management & Consulting (M.I.C.M.) Limited v Telenet BVBA*, Case C-597/19 (**Mircom**)

Relevant legal sources

Directive 95/46 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

Recital 26, Article 2 [Definitions], Article 3 [Scope]

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)

Recital (26); Recital (34); Recital (35); Article 2 - Material scope; Article 4 - Definitions

National Level

The Bundesdatenschutzgesetz (German Federal Data Protection Law) of 20 December 1990 (BGBl. 1990 I, p. 2954):

Paragraph 3(1) (now repealed[2]): "personal data are individual indications concerning the personal or factual circumstances of an identified or identifiable natural person (data subject)".

Telemediengesetz (German Law on telemedia) of 26 February 2007 (BGBl. 2007 I, p. 179, 'TMG'):

[2] See now the (new) *Bundesdatenschutzgesetz* (German Federal Data Protection Law) of 30 June 2017 (BGBl. 2017 I, p. 2097), and especially its paragraph 46, n. 1: ""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 person".

Paragraph 12 (now repealed[3]):

"(1) A service provider may collect and use personal data to make telemedia available only in so far as this law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.

(2) Where personal data have been supplied in order for telemedia to be made available, a service provider may use them for other purposes only in so far as this law or another legislative provision expressly relating to telemedia so permits or the user has consented to it.

(3) Except as otherwise provided, the provisions concerning the protection of personal data which are applicable in the case in question shall apply even if the data are not processed automatically.'

Paragraph 15 (now repealed[4]):

---

[3] See now the (new) *Telekommunikation-Telemedien-Datenschutz-Gesetz* (Telecommunications Telemedia Data Protection Act - TTDSG) of 23 June 2021 (BGBl, 2021 I, p. 1982), and especially its §3, "Vertraulichkeit der Kommunikation – Fernmeldegeheimnis": "(1) Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche.
(2) Zur Wahrung des Fernmeldegeheimnisses sind verpflichtet
1. Anbieter von öffentlich zugänglichen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
2. Anbieter von ganz oder teilweise geschäftsmäßig angebotenen Telekommunikationsdiensten sowie natürliche und juristische Personen, die an der Erbringung solcher Dienste mitwirken,
3. Betreiber öffentlicher Telekommunikationsnetze und
4. Betreiber von Telekommunikationsanlagen, mit denen geschäftsmäßig Telekommunikationsdienste erbracht werden.
Die Pflicht zur Geheimhaltung besteht auch nach dem Ende der Tätigkeit fort, durch die sie begründet worden ist.
(3) Den nach Absatz 2 Satz 1 Verpflichteten ist es untersagt, sich oder anderen über das für die Erbringung der Telekommunikationsdienste oder für den Betrieb ihrer Telekommunikationsnetze oder ihrer Telekommunikationsanlagen einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder von den näheren Umständen der Telekommunikation zu verschaffen. Sie dürfen Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis unterliegen, nur für den in Satz 1 genannten Zweck verwenden. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit dieses Gesetz oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht. Die Anzeigepflicht nach §138 des Strafgesetzbuches hat Vorrang"

[4] See now the (new) *Telekommunikation-Telemedien-Datenschutz-Gesetz* (Telecommunications Telemedia Data Protection Act - TTDSG) of 23 June 2021 (BGBl, 2021 I, p. 1982), and especially its §9, "Verarbeitung von Verkehrsdaten": "(1) Nach § 3 Absatz 2 Satz 1 Verpflichtete dürfen folgende Verkehrsdaten nur verarbeiten, soweit dies zum Aufbau und zur Aufrechterhaltung der Telekommunikation, zur Entgeltabrechnung oder zum Aufbau weiterer Verbindungen erforderlich ist:
1. die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei 61arden Anschlüssen auch die Standortdaten,
2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,
3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,
4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen und
5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.
Im Übrigen sind Verkehrsdaten von den nach § 3 Absatz 2 Satz 1 Verpflichteten nach Beendigung der Verbindung unverzüglich zu löschen. Eine über Satz 1 hinausgehende Verarbeitung der Verkehrsdaten ist unzulässig. Die Pflicht zur Verarbeitung von Verkehrsdaten aufgrund von anderen Rechtsvorschriften bleibt unberührt.
(2) Teilnehmerbezogene Verkehrsdaten nach Absatz 1 dürfen vom Anbieter des Telekommunikationsdienstes zum Zweck der Vermarktung von Telekommunikationsdiensten, zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Maß und im dazu erforderlichen Zeitraum nur verwendet 61arden, wenn der Endnutzer in diese Verwendung gemäß der Verordnung (EU) 2016/679 eingewilligt hat. Die

‘(1) A service provider may collect and use the personal data of a user only to the extent necessary in order to facilitate, and charge for, the use of telemedia (data concerning use). Data concerning use include, in particular:

1. particulars for the identification of the user,

2. information about the beginning, end and extent of the particular use, and

3. information about the telemedia used by the user.

(2) A service provider may combine the data concerning use of a user relating to the use of different telemedia to the extent that this is necessary for purposes of charging the user.

…

(4) A service provider may use data concerning use after the end of the use to the extent that they are required for purposes of charging the user (invoicing data). The service provider may block the data in order to comply with existing limits on storage periods laid down by law, statutes or contract”.

The case(s)

In Breyer, a German resident had accessed several information websites operated by German federal institutions. To prevent attacks and make it possible to prosecute “pirates”, most of those websites store information including the name of the web page, the terms of the search, the time of access, the quantity of data transferred, an indication of whether access was successful, and the IP address of the computer from which access was sought on all access operations in log files.

IP addresses are series of digits assigned to networked computers to facilitate their communication. When a website is accessed, the IP address of the computer seeking access is communicated to the server on which the website consulted is stored. That connection is necessary so that the data accessed maybe transferred to the correct recipient. Internet service providers allocate to the computers of internet users either a “static” IP address or a “dynamic” IP address, that is to say an IP address that changes each time there is a new connection.

Mr. Breyer brought an action before the German administrative courts seeking an order restraining the Federal Republic of Germany from storing, or arranging for third parties to store, the IP address of his host system collected after consultation of the above mentioned websites. The action was dismissed, and Mr. Breyer lodged an appeal.

The Court of Appeal ordered the Federal Republic of Germany to refrain from storing or arranging for third parties to store, at the end of each consultation period, the IP address of Mr. Breyer’s host system, where that address was stored together with the date of the consultation period to which it related and where Mr. Breyer had revealed his identity during that use, including in the form of an electronic address mentioning his identity, except in so far as that storage was not necessary in order to restore the dissemination of those media in the event of a fault occurring. The Court of Appeal considered that when combined with such information, a dynamic IP constitutes personal data, because the operator of the website is able to identify the user by linking his name to his computer’s IP address. For the Court, in other circumstances, that is when Mr. Breyer does not reveal his identity during a consultation period, the IP address is not personal data, even in combination with the date of the consultation period to which

---

Daten anderer Endnutzer sind unverzüglich zu anonymisieren. Eine zielnummernbezogene Verwendung der Verkehrsdaten zu den in Satz 1 genannten Zwecken ist nur zulässig, wenn der Endnutzer gemäß der Verordnung (EU) 2016/679 informiert wurde und er eingewilligt hat. Hierbei sind die Daten anderer Endnutzer unverzüglich zu anonymisieren. Außerdem ist der Endnutzer darauf hinzuweisen, dass er die Einwilligung nach den Sätzen 1 und 3 jederzeit widerrufen kann”.

it relates, because the user of the websites concerned is not identifiable by the Member State. The appeal was thus only partially upheld.

Mr. Breyer and the Federal Republic of Germany brought an appeal on a point of law before the Bundesgerichtshof (Federal Court of Justice, Germany). The BGH questioned the outcome, on the basis of an academic debate concerning the issue whether an "objective" or "relative" criterion should be used to decide if a person is identifiable. In substance, the question is whether the person is identifiable where the information, which when read together permit his identification, is stored by different operators, one being the online media services provider (the Federal Republic of Germany) and the other being Mr. Breyer's internet service provider. The BGH decided to refer it to the CJEU.

This question of whether the data processed are "personal data" within the meaning of Article 2 of the Directive, and consequently be protected as such, had been raised in other cases. It involved, in particular:

-in *Scarlet Extended* and *Mircom*, IP addresses when they allow the user to be precisely identified;

-in *Lindqvist*, information concerning the health of the data subject, formulated in a very vague manner (limited to the statement that an individual had injured her foot and was on half-time work on medical grounds);

-in *Google Spain*, *Satamedia* and *CNIL*, information that had already been lawfully published by third parties;

-in *Worten*, a record of working time which indicated, in relation to each worker, the times when working hours began and ended, as well as the corresponding breaks and intervals,

-in *Volker*, information concerning the beneficiary of agricultural funds,

-In *Nowak*, the written answers submitted by a candidate in a professional examination and any examiner's comments with respect to those answers,

-in *Buivids*, the video of police officers in a police station while a statement is being made;

-in *La Quadrature du Net*, traffic and location data automatically analysed for antiterrorism aims, if they allow the data subject to be identified, even though only at a later stage.

It is in Breyer that the reasoning of the Court is for the first time substantially developed, which makes this case the reference point, although it is usefully complemented by *Nowak*.

Preliminary question(s) referred to the Court

In *Breyer*, the question put to the Court, in relation to the concept of "personal data", is the following:

Must Article 2(a) of Directive 95/46 be interpreted as meaning that an internet protocol address (IP address) which an (online media) service provider stores when his website is accessed already constitutes personal data for the service provider if a third party (an access provider) has the additional knowledge required in order to identify the data subject?

In all other referred cases, the Court had to decide, at one point, on whether the disputed data were "personal data" within the meaning of EU law.

Reasoning of the Court

Whereas in previous cases the Court did not greatly expand its reasoning on the concept of personal data, the question is extensively and carefully dealt with in *Breyer*, where it was more complex.

Although not expressly referring to the Charter nor to the principle of effectiveness, the reasoning of the Court implicitly relies on such principle as it endorses a precautionary approach. The decision of the Court requires the inclusion within the meaning of "personal data" not only of information which actually permit the identification of a person, but also each piece of information which, even though not allowing such identification in itself, could allow such identification if combined with other pieces of information, even if these other pieces are in the hands of different operators and if the combination of the pieces of information may occur only in exceptional circumstances (such as cyber-attacks).

The Court firstly recalls that, "personal data" "mean any information relating to an identified or identifiable natural person ("data subject")", and that 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."

Referring to *Scarlet Extended*, the Court stresses that IP addresses of internet users, when collected by internet service providers, are protected personal data because they allow users to be precisely identified. But the situation in the case at hand is different, firstly because the online media services provider registers IP addresses of the users of its website, without having the additional data necessary in order to identify those users, secondly because the IP addresses are "dynamic" ones, and change for each connection.

The Court then examines carefully the situation where a dynamic IP address is registered by an online media service provider, while additional data making it possible to identify the user is detained by a third party, the internet service provider. Such examination is to be made in light of recital 26 of Directive 95/46, which states that, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person. **For the Court, the wording "any other person" suggests that, for information to be treated as "personal data" within the meaning of Article 2(a) of that Directive, it is not required that all the information enabling the identification of the data subject must be in the hands of one person**. **The issue is not only whether the combined data are actually in the same hands, but whether there is a reasonable possibility that the controller will be in a position to collect such combined information**. For the Court, that would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant. In light of this statement, the Court observes that, in the case at hand, even if German law does not allow the internet service provider to directly transmit the additional data necessary for the identification of the data subject to the online media services provider, although, it seems subject to verification by the referring court, that, in particular in the event of cyber-attacks, legal channels exist so that the online media services provider is able to contact the competent authority, so that the latter can take the steps necessary to obtain that information from the internet service provider and bring criminal proceedings. Thus, it appears that the online media services provider has the means that may likely reasonably be used in order to identify the data subject, with the assistance of other persons. In the case at hand, an IP address is to be considered as personal data.

Such a broad definition of "personal data" is in line with the Court's previous case law. In particular, in *Lindqvist*, the Court judges that a "wide interpretation" should be given to the expression "data concerning health" used in Article 8(1) of the Directive, so as to include information concerning all aspects, both physical and mental, of the health of an individual. Thus, a mere reference to the fact that an individual has injured their foot and is on half-time work on medical grounds constitutes personal data within the meaning of the Directive. In *Satamedia* and *Google Spain*, the Court uses arguments (described above under question 1) to conclude that operations related to information that has already been lawfully published by third parties are "processing of personal data".

Conclusion of the Court

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

Impact on the follow-up case

In its judgment of 17 May 2017, BGH Az VI ZR 135/13, the German Federal Court (Bundesgerichtshof) ruled that:

A dynamic IP address that is stored by an online media service provider when a person accesses a website that that provider makes generally accessible must be considered personal data. The provider is allowed to collect and use personal data of a user of online media services, such as the IP address, even after the end of the page navigation, provided it is necessary for the general operation of the website. This, however, implies a balancing with the interests and fundamental rights and freedoms of users.

In the present case, this balancing could not be made conclusively on the basis of the Court of Appeal's findings. Therefore, the case was referred to the Berlin Regional Court.

Elements of judicial dialogue - Horizontal (within the CJEU):

In *Lindqvist, Ryneš*, *Buivids* and *TK*, the Court decides that the image of a person recorded by a camera constitutes "personal data" inasmuch as it makes it possible to identify the person concerned.

In *Nowak*, the CJEU analyses whether the written answers submitted by a candidate at a professional examination, and any examiner's comments with respect to those answers, constitute personal data. It refers to Breyer to recall that there is no requirement that all the information enabling the identification of the data subject must remain in the hands of one person. To determine whether the written answers provided by a candidate at a professional examination and any comments made by an examiner with respect to those answers constitute information relating to that candidate, the Court observes that the scope of application of Directive 95/46 is broad and the personal data covered is varied. It is not, in particular, restricted to information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it "relates" to the data subject.

The written answers submitted by a candidate at a professional examination constitute information that is linked to them as a person, since:

1) it reflects the extent of the candidate's knowledge and competence in a given field and, in some cases, their intellect as well as, eventually, information as to their handwriting;

2) the purpose of collecting those answers is to evaluate the candidate's professional abilities and their suitability to practice the profession concerned;

3) the use of that information, a consequence of that use being the candidate's success or failure in the examination concerned, is liable to have an effect on their rights and interests, in that it may determine or influence the chance of entering the profession aspired to or of obtaining the post sought, for example.

The comments of an examiner with respect to the candidate's answers also constitute information relating to that candidate and to the examiner as they reflect the opinion or the assessment of the examiner of the individual performance of the candidate in the examination.

For the Court, it is clear that an examination candidate has, *inter alia*, a legitimate interest, based on the protection of their private life, in being able to object to the processing of the answers submitted by them in that examination and of the examiner's comments with respect to those answers outside the examination procedure and, in particular, to their being sent to third parties, or published, without his permission. He also has the right to ask for the answers and comments to be erased or deleted, after a certain period of time.

In several decisions, the CJEU has stated that the fact that information is provided as part of a professional activity does not mean that it cannot be characterised as a set of personal data, since the concepts of "personal data" and of "data relating to private life" are not to be confused (*Österreichischer Rundfunk and Others,* C-465/00, C-138/01 and C-139/01, *Commission v. Bavarian Lager*, C-28/08 P, 70; *Worten*, C-342/12, *ClientEarth*, C-615/13 P, *Manni*, C- 698/15).

Impact on national case law in Member States different from the state of the court referring the preliminary question to the CJEU

France

Cour de cassation (1re civ., 3 nov. 2016, no 15-22.595, publié au Bulletin): IP addresses are personal data.

2.1.2. Question 2: Definition of the concept of "processing" of personal data

2. What is "processing" of personal data? What types of operations constitute "processing" in the meaning of the EU data protection law and in light of Article 47 CFREU and the principle of effective protection?

Cluster of CJEU cases particularly relevant with respect to question 2

Within the cluster of cases, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts on the question under consideration:

➢ Judgment of the Court, 6 November 2003, *Bodil Lindqvist*, Case C-101/01 (Lindqvist)

Cluster of cases

➢ Judgment of the Court, 6 November 2003, *Bodil Lindqvist*, Case C-101/01 (**Lindqvist**)

➢ Judgment of the Court (Grand Chamber), 16 December 2008, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy, Satamedia Oy*, Case C-73/07 (**Satamedia**)

➢ 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*, Case C-131/12 (**Google Spain**)

➢ Judgment of the Court (Fourth Chamber), 11 December 2014, *František Ryneš v. Úřad pro ochranu osobních údajů*, Case C-212/13 (**Ryneš**)

➢ Judgment of the Court (Third Chamber), 1 October 2015, *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, Case C-230/14 (**Weltimmo**)

➢ Judgment of the Court, (Grand Chamber), 6 October 2015, *Schrems v. Data Protection Commissioner*, Case C-362/14 (**Schrems I**)

➢ Judgment of the Court (Grand Chamber), 10 July 2018, *Tietosuojavaltuutettu / Jehovan todistajat — uskonnollinen yhdyskunta*, Case C-25/17 **(Jehovan**)

➢ Judgment of the Court (Second Chamber), 14 February 2019, *Sergejs Buivids*, Case C-345/17 (**Buivids**)

➢ Judgment of the Court (Second Chamber), 29 July 2019, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*, Case C-40/17 (**Fashion ID**)

➢ Judgement of the Court, 24 September 2019, *GC, AF, BH et ED v CNIL*, Case C-136/17 (**CNIL**)

➢ Judgement of the Court, 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, Case C-311/18 (**Schrems II**)

Relevant legal sources

Directive 95/46 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

Article 2 - Definitions; Article 3 - Scope

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)

Recital (15); Article 2 - Material scope; Article 4 - Definitions

National Level

Personuppgiftslag (SFS1998:204) (Swedish law on personal data, the "PUL") [in *Lindvisqt*]

The case(s)

Mrs. Lindqvist was charged with breach of the Swedish legislation on the protection of personal data for publishing personal data (such as names, phone numbers, jobs and hobbies, and in one case health information) of a number of people working with her on a voluntary basis in a parish of the Swedish Protestant Church on her internet website. She had not informed her colleagues of the existence of those pages or obtained their consent, nor did she notify the Datainspektionen (Swedish supervisory authority for the protection of electronically transmitted data) of her activity. She removed the pages in question as soon as she became aware that they were not appreciated by some of her colleagues.

Prosecution was brought for breach of the Swedish law on personal data (the "PUL") on the grounds that she had:

- processed personal data by automatic means without giving prior written notification to the Datainspektionen (Paragraph 36 of the PUL);

- processed sensitive personal data (concerning an injured foot and half-time working on medical grounds) without authorisation (Paragraph 13 of the PUL);

- transferred processed personal data to a third country without authorisation (Paragraph 33 of the PUL).

Mrs. Lindqvist accepted the facts but disputed that she was guilty of an offence. Mrs. Lindqvist was fined by the Eksjö tingsrätt (District Court) (Sweden) and appealed against that sentence to the referring Court. As it had doubts as to the interpretation of Directive 95/46, the Göta hovrätt decided to maintain proceedings and refer several questions to the Court for a preliminary ruling, including one on the scope of the Directive and the meaning of the concept of "processing data".

In all other referred cases, a data controller alleged that its activity could not be regarded as "processing of data" within the meaning of EU legislation. For instance, in the referred cases, the activities at issue were:

- in *Weltimmo*, the operation of loading personal data on an internet page, in *Satamedia* and *Google Spain*, the processing of personal data without alteration, or the processing of personal data exclusively concerning material that had already been published in unaltered form in the media;

- in *Google Spain* and *CNIL*, the activity of a search engine as a provider of content, which consisted in finding information including personal data, 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;

- in *Schrems I* and *Schrems II*, the operation consisting in having personal data transferred from a Member State to a third country;

- in *Ryneš*, the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual in his family home for the purposes of protecting the property, health and life of the home owners, but which also monitored a public space;

- in *Jehovan*, the collection of personal data by members of a religious community in the course of door-to-door preaching and the subsequent processing of that data;

- in *Buivids*, the recording and publication of a video on a video website, on which users can send, watch and share videos (*youtube*);

- in *Fashion ID*, the embedding on a third party's website of a social plugin ("*like*" button) causing the browser of the website's visitor to request content from the provider of that plugin and, to that end, the transmission to that provider of the personal data of the visitor.

Preliminary question(s) referred to the Court:

In all referred cases, the Court was asked, in substance, the same general question: What types of operations constitute "processing" in the meaning of the EU data protection law, in the perspective of the principle of effective protection and/or Article 47 CFR?

Reasoning of the Court

Although not expressly referring to Article 47 of the Charter or to the principle of effectiveness, the Court relies implicitly on the principle of effective protection to promote a broad conception of "processing" data. The Court endorses a two-step reasoning. Firstly, it focuses on the "positive" material scope of the Directive in light of Article 3 (1) to adopt **a broad conception of the general scope of the**

Directive. Secondly, le Court justifies **a strict interpretation of the exceptions** to the application of the Directive laid down by Article 3(2).

Broad conception of the general scope of the Directive defined in Article 3(1)

In *Google Spain* and *Satamedia*, the Court endorses a wide conception of the general scope of the Directive, stressing that not only does the wording of Article 2(b) of the Directive require the inclusion of the activities in question within the meaning of "processing of data", but also that "a general derogation from the application of Directive 95/46 in such a case [i.e. where the processing of personal data is made without alteration or exclusively concerns material that has already been published in unaltered form in the media] would largely deprive the Directive of its effect". This ruling is in line with the view taken by the Court in *Lindqvist*, according to which the Court, asked whether it is permissible for Member States to provide for greater protection for personal data or a broader scope than is required under Directive 95/46 (question 7), underlines that nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included within the scope thereof (provided that no other provision of Community law precludes it).

However, in *Lindqvist*, the Court mitigates the consequences of the principle of effectiveness and contains the scope of the Directive within reasonable limits, implicitly referring to the principle of proportionality. Even if Member States may extend the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included within the scope thereof, measures taken by Member States to ensure the protection of personal data should be consistent with the Directive's objective of maintaining a balance between the free movement of personal data and the protection of private life. Moreover, the interpretation of the concept of "processing of data" is also subject to the principle of proportionality: "If Article 25 of Directive 95/46 were interpreted to mean that there is "transfer [of data] to a third country" every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the Directive would thus necessarily become a regime of general application, with regard to operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet".

Strict interpretation of the exceptions to the application of the Directive laid down by Article 3(2)

In *Lindqvist*, *Satamedia*, *Ryneš* and *Jehovan*, the Court favours a strict interpretation of the exceptions to the application of the Directive as defined in Article 3(2) of the Directive. The reasoning is particularly developed in *Lindqvist*. Having decided that the loading of personal data on an internet page constitutes "processing" within the meaning of the Directive, the court considers whether it can be covered by one of the exceptions to the application of the Directive.

Concerning the first subparagraph of Article 3(2) of Directive 95/46, first, the Court observes that it would not be appropriate to interpret the expression "activity which falls outside the scope of Community law" as having a scope requiring to be determined in each individual case, by assessing whether the specific activity at issue directly affects freedom of movement between Member States. Such an approach would make the limits of the field of application of the Directive particularly unsure and uncertain, which would be contrary to its essential objective of approximating the laws, regulations and administrative provisions of the Member States in order to eliminate obstacles to the functioning of the internal market. It should thus be considered that the first subparagraph of Article 3(2) of Directive 95/46 is intended to define the scope of the exception provided for therein, with the result that that exception applies only to

the activities which are expressly listed there or which can be classified in the same category. Charitable or religious activities such as those carried out by Mrs. Lindqvist cannot be considered equivalent to the activities listed in the first subparagraph of Article 3(2) of Directive 95/46 and are thus not covered by that exception.

Concerning the second subparagraph of Article 3(2) of Directive 95/46, the Court stresses that the 12th Recital in the preamble to that Directive, which concerns that exception, cites, as examples of the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, correspondence and the holding of records of addresses. That exception must therefore be interpreted as relating only to activities which are carried out in the course of the private or family life of individuals, which is clearly not the case with the processing of personal data consisting of publication on the internet so that those data are made accessible to an indefinite number of people.

Conclusion of the court

1) The act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions and hobbies, constitutes "the processing of personal data wholly or partly by automatic means" within the meaning of Article 3(1) of Directive 95/46.

2) Such processing of personal data is not covered by any of the exceptions in Article 3(2) of Directive 95/46.

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

Elements of judicial dialogue

- *Horizontal dialogue:*

In *Jehovan* (C25/17), the CJEU analyses the meaning of the concept of a "filing system" referred to in Article 2 (c) Directive 95/46, to decide whether a set of personal data collected in the course of door-to-door preaching, consisting of names and addresses as well as other information concerning persons contacted, is covered by that definition. The Court observes that the Directive covers both automatic processing of data and manual processing of such data, so that the scope of the protection it confers on data subjects does not depend on the techniques used and avoids the risk of that protection being circumvented. For the Court, there is no specific requirement as to the form of the "file"; the only criterion is that the set of personal data must be structured for the purpose of enabling personal data to be easily retrieved. Therefore, the Court concludes that the concept of a "filing system" covers: "a set of personal data collected in the course of door-to-door preaching, consisting of the names and addresses and other information concerning the persons contacted, if those data are structured according to specific criteria which, in practice, enable them to be easily retrieved for subsequent use. In order for such a set of data to fall within that concept, it is not necessary that they include data sheets, specific lists or other search methods".

The Court was also asked whether the collection of personal data by members of a religious community in the course of door-to-door preaching and the subsequent processing of such data constituted the processing of personal data carried out for the purposes of the activities referred to in Article 3(2), first subparagraph, of the Directive or the processing of personal data carried out by a natural person in the course of a purely personal or household activity within the meaning of Article 3(2), second subparagraph.

Referring to *Lindqvist, Google Spain, Satamedia* and *Rynes*, the Court decided that it was not the case: although the door-to-door preaching activities of the member of a religious community is protected by Article 10(1) of the Charter as an expression of the faith of those preachers, that fact does not confer an exclusively personal or household character on that activity, within the meaning of Article 3(2), second indent, of Directive 95/46.

In *Buivids*, the Court refers to *Ryneš* and *Lindqvist* to decide that the recording of a video which is stored on a continuous recording device (digital photo camera) and the operation of loading personal data onto an internet page and placing information on an internet page constitute "processing".

In *Fashion ID* (C-40/17), the Cours refers to Article 2 (b) of the Directive, defining what is "processing", and stresses that, "it is apparent from that definition that the processing of personal data may consist in one or a number of operations, each of which relates to one of the different stages that the processing of personal data may involve" (§72).

Although it leaves it to the national courts to decide whether *Fashion ID* processes data in the meaning of EU law, the Court furthers its analysis by stating that:

"75 … by embedding on its website the Facebook "Like" button, Fashion ID appears to have made it possible for Facebook Ireland to obtain personal data of visitors to its website … and that such a possibility is triggered as soon as the visitor consults that website, regardless of whether or not the visitor is a member of the social network Facebook, has clicked on the Facebook 'Like' button or is aware of such an operation". As a consequence, Fashion ID should be considered — together with Facebook Ireland — as jointly capable of determining the purpose and means of data processing. At the same time, however, Fashion ID is not capable of determining the purpose and means of processing data after it is transferred to Facebook Ireland. By placing a Facebook plugin (the "Like" button) on its website, Fashion ID purposefully allowed Facebook Ireland to collect data of its customers.

"76 … In view of that information, it should be pointed out that the operations involving the processing in respect of which Fashion ID is capable of determining, jointly with Facebook Ireland, the purposes and means are, for the purposes of the definition of the concept of "processing of personal data" in Article 2(b) of Directive 95/46, the collection and disclosure by transmission of the personal data of visitors to its website. By contrast, in the light of that information, it seems, at the outset, impossible that Fashion ID determines the purposes and means of subsequent operations involving the processing of personal data carried out by Facebook Ireland after their transmission to the latter, meaning that Fashion ID cannot be considered to be a controller in respect of those operations within the meaning of Article 2(d).

"77 … With regard to the means used for the purposes of the collection and of certain personal data of visitors to its website, it is apparent from paragraph 75 above that Fashion ID appears to have embedded on its website the Facebook "Like" button made to website operators by Facebook Ireland while fully aware of the fact that it serves as a tool for the collection and disclosure by transmission of the personal data of visitors to that website, regardless of whether or not the visitors are members of the social network Facebook.

78 Moreover, by embedding that social plugin on its website, Fashion ID exerts a decisive influence over the collection and transmission of the personal data of visitors to that website to the provider of that plugin, Facebook Ireland, which would not have occurred without that plugin".

2.1.3. Question 3: Definition of the concept of "controller"

3.a) In light of the principle of effectiveness of data protection, how should the concept of "controller" of the processing of personal data be interpreted under EU Data protection? Can the Charter and the principle of effective protection influence this concept? 3.b) In light of the principle of effectiveness of data protection, what are the circumstances under which an operator, who is not the data processor, should be considered as having "joint control" over data processing?

Cluster of relevant CJEU cases

➢ 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*, Case C-131/12 (**Google Spain**)

➢ Judgment of the Court (Grand Chamber), 5 June 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH & Facebook Ireland Limited*, Case C-210/16 (**Wirtschaftsakademie**)

➢ Judgment of the Court (Grand Chamber), 10 July 2018, *Tietosuojavaltuutettu / Jehovan todistajat — uskonnollinen yhdyskunta*, Case C-25/17 (**Jehovan**)

➢ Judgment of the Court (Second Chamber), 29 July 2019, *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*, Case C-40/17 (**Fashion ID**)

➢ Judgement of the Court (Grand Chamber), 24 September 2029, *GC, AF, BH et ED v CNIL*, Case C-136/17 (**CNIL**)

➢ Judgment of the Court (Third Chamber), 9 July 2020, *VQ v Land Hesse*, Case C-272/19 (**Hesse**)

2.1.4. Question 3a: the concept of controllership

3.a. In light of the principle of effectiveness of data protection, how should the concept of "controller" of the processing of personal data be interpreted under EU Data protection? Can the Charter and the principle of effective protection influence this concept?

Within the cluster of cases listed above, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

➢ 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)

Relevant legal sources

Directive 95/46 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

Article 2 - Definitions; Article 3

Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Recital (18); Recital (20); Article 2 - Material scope; Article 4 - Definitions

National Level

Spanish Organic Law n°15/1999, 13 December 1999, on the protection of personal data (transposing Directive95/46)

The case(s)

A Spanish national resident in Spain lodged a complaint against a Spanish publisher and against Google Spain and Google Inc., with the AEPD (Spanish data protection supervisory authority), seeking an order requiring them to remove or conceal the personal data relating to him, and published many years earlier, which were now irrelevant and detrimental to him. The complaint directed against Google Spain and Google Inc., was upheld. The AEPD considered that operators of search engines are subject to data protection legislation given that they carry out data processing for which they are responsible and act as intermediaries in the information society. The AEPD took the view that it has the power to require the withdrawal of data and the prohibition of access to certain data by the operators of search engines when it considers that the locating and dissemination of the data are liable to compromise the fundamental right to data protection and the dignity of persons in the broad sense, and this would also encompass the mere wish of the person concerned that such data not be known to third parties.

Google Spain and Google Inc., brought separate actions appealing against that decision before the Audiencia Nacional (National High Court). Google Spain and Google Inc., contended that the activity of a search engine as a provider of content that consists in finding information published or placed on the internet by third parties could not be classified as "processing of personal data" (see on this topic Question 2 above). They also contended that should that activity be classified as "processing of personal data", the operator of a search engine cannot be regarded as a "controller" in respect of that processing since it has no knowledge of that data and does not exercise control over the data.

The Audiencia Nacional joined the actions and decided to maintain the proceedings and to refer several questions to the Court for a preliminary ruling regarding the interpretation of Directive 95/46, and more specifically the meaning of the concept of "controller".

Preliminary question referred to the Court

In ***Google Spain***, the referring court sought to ascertain, if the activity of a search engine as a provider of content which consists 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 were to be classified as "processing of personal data" within the meaning of that provision when that information contains personal data, whether Article 2(d) of Directive 95/46 is to be interpreted as meaning that the operator of a search engine must be regarded as the 'controller' in respect of that processing of the personal data, within the meaning of that provision.

See also below at: "Elements of judicial dialogue".

Other cases refer to different types of operators:

In ***Wirtschaftsakademie*** (C-210/16), the administrator of a fan page hosted on a social network, enabling the collection and processing of certain data of visitors to that page;

In ***Jehovan*** (C-25/17), a religious community acting jointly with its members who engage in preaching, with regard to the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community, also taking into account the fact that the community has (or does not have) access to that data or had given (or did not give) its members written guidelines or instructions in relation to that processing;

In ***Fashion ID*** (C-40/17), (1) the person embedding a programming code in their website which causes the user's browser to request content from a third party ("like" button) and, to this end, transmits personal data to the third party, but who are themselves unable to manage this data processing operation; and (2) the operator of a website who has embedded the content of a third party and thus creates the cause for the processing of personal data by the third party.

In ***CNIL*** (C-139/17), as in *Google Spain*, the operator of a search engine;

In ***Land Hesse*** (C-272/19), a Petitions Committee of the parliament of a Federated State of a Member State d

Reasoning of the Court

The Court clearly builds on the principle of effectiveness to promote a broad definition of the concept of "controller" within the meaning of the Directive, in order for the operator of a search engine to be included in this definition. Analysing the concrete role played by the operator of a search engine, firstly, the Court observes that it determines the purposes and means of its activity, secondly that such activity can be distinguished from, and is additional to, that carried out by publishers of websites (loading of data on the internet). The Court also stresses that the activity of search engines plays a decisive role in the dissemination of personal data, making them available to internet users who otherwise would not have found that data. It concludes that, additionally compared to that of web publishers, the activity of a search engine thus significantly affects the fundamental rights to privacy and to the protection of personal data. Therefore, it "would be contrary, not only to the clear wording of Article 2(d) of the Directive but also to its objective which is to ensure, through a broad definition of the concept of "controller", effective and complete protection of data subjects – to exclude the operator of a search engine from that definition on the ground that it does not exercise control over the personal data published on the web pages of third parties" (§34). Finally, the Court finds that the fact that publishers of websites have the option of indicating to search engine operators that they wish information published on their site to be excluded from the search engines' indexes, is irrelevant, since the operator of the search engine is still in the position to define the purposes and means of the processing.

Conclusion of the Court

Articles 2(b) and (d) of Directive 95/46 are to be interpreted as meaning that, first, 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 the "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).

Impact on the follow-up case

The major impact of Google Spain is mainly related to the part of the decision creating a right to be de-listed. This impact is fully analysed in Chapter [see the part "Impact on national case law in the Member State different from the state of the court referring the preliminary question to the CJEU" below].

Elements of judicial dialogue

The cluster of cases discussed above clearly illustrates an interesting issue of **horizontal** dialogue within the CJEU, combined with **vertical** dialogue, where domestic courts attempted to further develop CJEU doctrine, by referring subsequent preliminary questions.

As was said above, in the initial ***Google Spain*** case, the referring court sought to ascertain if the activity of a search engine as a provider of content, which consists 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 were to be classified as "processing of personal data" within the meaning of that provision when that information contains personal data, whether Article 2(d) of Directive 95/46 is to be interpreted as meaning that the operator of a search engine must be regarded as the "controller" in respect of that processing of the personal data, within the meaning of that provision.

The subsequent cases refer to different types of operators who collect and process personal data:

1) in ***Wirtschaftsakademie*** (C-210/16), the question pertained to the administrator of a fan page hosted on a social network, enabling the collection and processing of certain data of visitors to that page;

2) in ***Jehovan*** (C-25/17), the referring Court addressed a religious community acting jointly with its members who engage in preaching, with regard to the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community. The preliminary question aimed to establish, in particular, whether it is a relevant/necessary factor to consider whether the community has access to that data — or whether the religious community had given its members written guidelines or instructions in relation to that processing. The answer of the Court was in the sense that these factors are irrelevant;

3) in ***Fashion ID*** (C-40/17), the preliminary reference addressed the issue whether: (1) the person embedding a programming code in their website, which causes the user's browser to request content from a third party ("like" button) and, to this end, transmits personal data to the third party, but who are themselves unable to manage this data processing operation; and (2) the operator of a website who has embedded the content of a third party and thus creates the cause for the processing of personal data by the third party;

4) in ***CNIL*** (C-139/17), as in earlier *Google Spain* judgment, the question addressed an operator of a search engine;

5) in ***Land Hesse*** (C-272/19) the Court stated that, in so far as a Petitions Committee of the parliament of a Federated State of a Member State determines, alone or with others, the purposes and means of the processing of personal data, that committee must be categorised as a "controller", within the meaning of the GDPR, and consequently the processing of personal data carried out by that committee falls within the scope of that Regulation.

Impact on national case law in Member States different from the state of the court referring the preliminary question to the CJEU

The Netherlands

The CJEU's decision in Google Spain has directly influenced two decisions (ECLI:NL:RBAMS:2018:1644 and ECLI:NL:RBAMS:2015:9515) from Rechtbank Amsterdam (Court of Amsterdam). Both cases concern the removal of a URL from Google Search. The Court of Amsterdam directly cites Google Spain in deciding that Google is a data controller.

2.1.5. Question 3b: joint controllership

3.b. In light of the principle of effectiveness of data protection, what are the circumstances under which an operator, who is not the data processor, should be considered as having "joint control" over the data processing?

Within the cluster of cases listed above, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

Judgment of the Court (Grand Chamber), 5 June 2018, *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH & Facebook Ireland Limited*, Case C-210/16 (Wirtschaftsakademie)

Relevant legal sources

Directive 95/46 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

Article 2 - Definitions; Article 3

Regulation (Eu) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Article 4 - Definitions

National Level

Paragraph 3(3)(4) and Paragraph 12(1) of the TMG

Paragraph 3(7) of the old BDSG and Paragraph 63 of the new BDSG

The case

Wirtschaftsakademie offers educational services by means of a fan page hosted on Facebook. Fan pages are user accounts that can be set up on Facebook by individuals or businesses to post any kind of communication in the media and opinion market. Administrators of fan pages can obtain anonymous statistical information on visitors to the fan pages via a function called "Facebook Insights" which Facebook makes available to them free of charge under non-negotiable conditions of use. That information is collected by means of evidence files ("cookies"), each containing a unique user code, which are active for two years and are stored by Facebook on the hard disk of the computer or on other media

of visitors to fan pages. The user code, which can be matched with the connection data of users registered on Facebook, is collected and processed when the fan pages are opened.

Wirtschaftsakademie was ordered by the ULD, a German supervisory authority, to deactivate the fan page on pain of a penalty payment, on the ground that neither Wirtschaftsakademie nor Facebook informed visitors of the fan page that Facebook, by means of cookies, collected personal data concerning them and then processed the data. Wirtschaftsakademie brought a complaint against that decision, arguing essentially that it was not responsible under data protection law for the processing of the data by Facebook or the cookies which Facebook installed.

By decision of 16 December 2011, the ULD dismissed the complaint, finding that Wirtschaftsakademie as a service provider was liable under Paragraph 3(3)(4) and Paragraph 12(1) of the TMG in conjunction with Paragraph 3(7) of the BDSG. The ULD stated that, by setting up its fan page, Wirtschaftsakademie had made an active and deliberate contribution to the collection by Facebook of personal data. Wirtschaftsakademie brought an action against that decision in the Verwaltungsgericht (Administrative Court, Germany), submitting that the processing of personal data by Facebook could not be attributed to it.

By judgment of 9 October 2013, the Verwaltungsgericht (Administrative Court) annulled the contested decision, essentially on the ground that, since the administrator of a fan page on Facebook is not a responsible entity within the meaning of Paragraph 3(7) of the BDSG, Wirtschaftsakademie could not be the addressee of a measure taken under Paragraph 38(5) of the BDSG. The Oberverwaltungsgericht (Higher Administrative Court, Germany) dismissed the ULD's appeal against that judgment as unfounded.

The ULD appealed on a point of law to the Bundesverwaltungsgericht (Federal Administrative Court, Germany).

The Bundesverwaltungsgericht (Federal Administrative Court) took the view that Wirtschaftsakademie cannot itself be regarded as responsible for the data processing within the meaning of Paragraph 3(7) of the BDSG or Article 2(d) of Directive 95/46. It nevertheless considered that the concept of controller should in principle be interpreted broadly, in the interests of effective protection of the right of privacy, as the Court had held in its recent case-law on the point. It further entertained doubts as to the powers of the ULD with respect to Facebook Germany in the present case, given that it was Facebook Ireland that was responsible, at EU level, for the collection and processing of personal data within the Facebook group. Finally, it was uncertain as to the effect, for the purpose of the exercise of the ULD's powers of intervention, of the assessments made by the supervisory authority to which Facebook Ireland is subject concerning the lawfulness of the processing of personal data at issue.

In those circumstances, the Bundesverwaltungsgericht (Federal Administrative Court) decided to maintain the proceedings and to refer the following questions to the Court for a preliminary ruling.

Preliminary question referred to the Court

Should Article 2(d), Article 17(2), Article 24 and the second indent of Article 28(3) of Directive 95/46 be interpreted as allowing an entity to be held liable in its capacity as administrator of a fan page on a social network where the rules on the protection of personal data are infringed, because it has chosen to make use of that social network to distribute the information it offers, even it is does not itself process the data?

Reasoning of the Court

The CJEU develops its reasoning, stressing the objective of offering an **effective and complete protection of personal data**. The Court points out that pursuant to Article 2 (d) of Directive 95/46, a controller is a body "which alone or jointly with others determines the purposes and means of the processing of personal data". Quoting *Google Spain*, it recalls that the concept of "controller" is to be defined broadly, in line with the objective of the effective and complete protection of personal data.

Stressing that since Article 2(d) of Directive 95/46 expressly relates to the entity which "alone or jointly with others" determines the purposes and means of the processing of personal data, the concept of "controller" does not necessarily refer to a single entity and may concern several actors taking part in that processing, with each of them then being subject to the applicable data protection provisions.

The Court then considers that the existence of joint responsibility does not necessarily imply equal responsibilities on the part of the various operators engaged in the processing. They may be involved at different stages and to different degrees, and they might not have equal access to the personal data. The relevant test is *whether the operator contributes to the processing, by taking part in the determination of the purposes and means of processing the personal data*. Consequently, **a party may be a controller, even if the data processing is essentially carried out by another party.**

The administrator of a fan page hosted on Facebook, such as Wirtschaftsakademie, by creating such a page, gives Facebook the opportunity to place cookies on the computer or other device of a person visiting its fan page. It must be regarded as taking part, by its definition of parameters depending in particular on its target audience and the objectives of managing and promoting its activities, in the determination of the purposes and means of processing the personal data of the visitors to its fan page. The administrator must therefore be categorised as a controller responsible for that processing within the EU, jointly with Facebook Ireland, within the meaning of Article 2(d) of Directive 95/46.

For the Court, the recognition of joint responsibility of the operator of the social network and the administrator of a fan page hosted on that network in relation to the processing of the personal data of visitors to that page contributes to ensuring a more complete protection of the rights of persons visiting a fan page, in accordance with the requirements of Directive 95/46 (§42).

Since the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data, the level of responsibility of each of them must be assessed with regard to all the relevant circumstances of the particular case.

Conclusion of the Court

Article 2(d) 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 must be interpreted as meaning that the concept of 'controller' within the meaning of that provision encompasses the administrator of a fan page hosted on a social network.

Impact of the follow-up case

In the Judgment of 11 September 2019, BVerwG 6 C 15.185 the German Federal Administrative Court (Bundesverwaltungsgericht) found that:

The operator of a fan page on the social network Facebook, is the data controller for the data processing operations that take place when this page is entered within the meaning of Section 3(7) of the German

5 https://www.bverwg.de/de/110919U6C15.18.0

Data Protection Act (Bundesdatenschutzgesetz - BDSG) and thus a potential addressee of an order pursuant to section 38(5) BDSG.

In the case of several parties jointly responsible for data processing, the exercise of the powers of intervention under Section 38 (5) BDSG requires the exercise of discretion with regard to the selection of the addressee.

Also in the area of data protection, the requirement of effective and efficient dissuasive prevention can justify the operation of the controller whose obligation can be affirmed without further ado and who has effective means at his disposal to stop the infringement.

Insights from independent authorities: EDPB Guidelines 07/2020 on the concepts of controller and processor in the GDPR of 2 September 2020

The concept of controller and joint controllership under GDPR have been thoroughly analysed by the European Commission in its *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* of 2 September 2020[6]:

(1) The commission underlined that the GDPR does not limit the array of entities that can act as **data controllers**. In particular, the concept in question is not limited to individuals and may also encompass organizations, companies and other collective entities.
(2) The key element of the controller concept is the ability of this person/entity to actually steer the process of processing data.
(3) The control in question should relate to "purposes and means of data processing". This substrate, as the European Commission observes, provides the substantial part of the controller concept. "Purposes" and "means" address the issues of "why" and "how" the data is processed. The controller should be able to determine both elements — even if they do not process the data by themselves (i.e., when there are separate data processors). In such a case, as the Commission elucidates, it is necessary to distinguish which means are essential and which are non-essential for the particular instance of data processing. The person/entity who is in charge of the former should be considered to act as the data controller.
(4) The person/entity who determines the purpose of data processing is always a data controller in the aforementioned sense.
(5) The concept of processing of personal data — used in the definition of controller in Article 4(7) GDPR – should be read in accordance with the general understanding of this concept under Article 4(2) GDPR.
(6) The **joint controllership** exists in the instances where data is processed with the involvement of several persons/entities, and where more than one of them complies with the definition of the data controller in the aforementioned sense. In other words, joint controllership requires that more than one person/entity are involved together ("jointly") in determining both the purpose and the means of data processing.
(7) Cooperation between the entities may either take up a form of a common decision or of a converging decision (where a few decisions are taken independently, but each of them is necessary for the particular process of data processing).
(8) The joint controllership should be established after examination of the factual circumstances of each particular case, not merely by adopting formal criteria of distinguishing. EDPB's Guidelines in that regard are particularly useful.

[6] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf

Impact on national case law in Member States different from the state of the court referring the preliminary question to the CJEU

The Netherlands

In ECLI:NL:RVS:2019:3331, The Raad van State (Council of State) directly referred to the CJEU's reasoning in *Fashion ID* (C-40/17) and *Wirtschaftsakademie* (C-210/16) in deciding that, whilst the Mayor and Municipal executive (College) was jointly responsible for wrongly posting the applicant's data, joint responsibility does not mean that both parties have the same responsibility, as the parties may be involved in different stages of the data processing. Thus, a court must consider all the relevant circumstances of the case (*Wirtschaftsakademie* C-210/16, followed). The Council of State then refers to Fashion ID (C-40/17), finding that that parties only have the same responsibility under Article 2(d) of Directive 95/46 if they jointly determine the purpose of the processing of the data. As the College lacked the requisite control over the forum, the Council of State found that the College was not liable for providing a list of names of those that had seen the forum post. Instead, the applicant should have submitted a request for the list to the party that controlled the forum.

Elements of judicial dialogue

Several requests for preliminary rulings have been referred to the Court since Google Spain, concerning the concept of "joint control" within the meaning of the Directive.

In ***Jehovan*** (C-25/17), the question referred to the Court is whether Article 2(d) of Directive 95/46, read in light of Article 10(1) of the Charter, must be interpreted as meaning that a religious community may be regarded as a controller, jointly with its members who engage in preaching, with regard to the processing of personal data carried out by the latter in the context of door-to-door preaching organised, coordinated and encouraged by that community, and whether it was necessary for that purpose for the community to have access to that data, or whether it must be established that the religious community had given its members written guidelines or instructions in relation to that processing.

Relying on *Google Spain* and *Wirtschaftsakademie*, the Court recalls that a natural or legal person who exerts influence over the processing of personal data, for his 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. The collection of personal data relating to persons contacted and their subsequent processing help to achieve the objective of the Jehovah's Witnesses Community, which is to spread its faith and are, therefore, carried out by members who engage in preaching for the purposes of that community. Furthermore, not only does the Jehovah's Witnesses Community have knowledge, on a general level, of the fact that such processing is carried out in order to spread its faith, but that community organises and coordinates the preaching activities of its members, in particular, by allocating areas of activity between the various members who engage in preaching. Such circumstances lead to the conclusion that the Jehovah's Witnesses Community encourages its members who engage in preaching to carry out data processing in the context of their preaching activity. The Jehovah's Witnesses Community, by organising, coordinating and encouraging the preaching activities of its members intended to spread its faith, participates, jointly with its members who engage in preaching, in determining the purposes and means of processing of personal data of the persons contacted, which is, however, for the referring court to verify with regard to all of the circumstances of the case (§71-73).

In ***Fashion ID*** (C-40/17), the question referred to the Court is (1) whether the person embedding a programming code in their website which causes the user's browser to request content from a third party ("like" button) and, to this end, transmits personal data to the third party, is a "controller" within the meaning of the Directive, if that person are themselves unable to influence this data processing operation; and (2) whether the operator of a website who has embedded the content of a third party and thus creates

the cause for the processing of personal data by the third party is a "controller" within the meaning of the Directive.

Building on *Google Spain*, *Wirtschaftsakademie* and *Jehovan*, the Court finds that where several operators jointly determine the purposes and means of the processing of personal data, they participate in that processing as controllers. By contrast, and without prejudice to any civil liability provided for in national law in this respect, that natural or legal person cannot be considered to be a controller, within the meaning of that provision, in the context of operations that precede or are subsequent in the overall chain of processing for which that person does not determine either the purposes or the means. By embedding the social plugin on its website, Fashion ID exerts a decisive influence over the collection and transmission of the personal data of visitors to that website to the provider of that plugin, Facebook Ireland, which would not have occurred without that plugin. It must be concluded that Facebook Ireland and Fashion ID jointly determine the means at the origin of the operations involving the collection and disclosure by transmission of the personal data of visitors to Fashion ID's website, and jointly determine the purposes of the operations involving the collection and disclosure by transmission of the personal data at issue in the main proceedings.

The decisions of the Court in *Wirtschaftsakademie*, *Jehovan* and *Fashion ID* contribute to the broad interpretation of the concept of "controller". The distinction between "processor" and "controller" laid down in the GDPR only confirms the relevance of the CJEU's understanding of the concept of "controller" and "joint controller".

2.1.6. Question 4: Definition of the concept of "data subject"

4. In light of the principle of effectiveness of data protection, how should the concept of "data subject" be interpreted within the meaning of EU law on data protection?

The CJEU has not directly addressed the question in the box. However, it is considered in passing by the Court in some decisions.

For instance, in *Volker* (Judgment of the Court (Grand Chamber), 9 November 2010, *Volker und Markus Schecke GbR & Hartmut Eifert v Land Hessen*, Joined Cases C-92/09 & C-93/09), the Court identifies the beneficiaries of the protection of personal data enshrined in Article 8 of the Charter: "it must be considered that the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual" (§52).

However, the question stated in the box is rather related to the question of precisely who is the holder of the rights laid down by EU legislation with regard to data protection? That issue raises problems, particularly, when the person exercising the right is not the same person whose data has been unlawfully published or processed. The GDPR includes recitals dealing with the issue of the identification of data subjects. National case law emphasises that questions may arise in relation to this issue.

The Charter and the principle of effectiveness and/or proportionality might therefore play a significant role.

Relevant legal sources

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)

Recital (14); Recital (27); Recital (38); Article 2 - Material scope

National caselaw

French Conseil d'Etat, 6 June 2017, No. 399446

Relevant national legal sources

Loi Informatique et Libertés n° 78-17, 6 January 1978 (French Data Protection Law): Article 2 and Article 39

Loi n° 2002-303, relative aux droits des malades et à la qualité du système de santé, 4 March 2002 (French law on the rights of patients)

The case

The claimant lodged a complaint with the Commission Nationale Informatique et Libertés (CNIL), the French data protection authority, alleging that he had not been provided proper access to data concerning his mother by her insurance company, which were needed for the purpose of evaluating damage she had suffered. The mother had died in the course of the proceedings and the President of the CNIL consequently decided to close the case, on the basis that the right of access to personal data is a personal right that is not transmitted to the data subject's heir. The claimant requested the French Conseil d'Etat to annul this decision.

Reasoning of the French Conseil d'Etat

On the basis of Article 2 of the French Loi Informatique et Libertés (No. 78-17, 6 January 1978), which defines the "data subject", and Article 39 of that law, which defines the conditions in which the right to access may be exercised, the French Court observes that the right to access is offered only with regard to personal data related to the person exercising the right. Successors and assignees of the person to whom personal data is related, such as heirs, cannot be automatically assimilated to such person.

However, when a person who suffers damage dies, his right to compensation is transmitted to his heirs, who replace him in pending legal actions brought to seek compensation for the damage suffered. Therefore, heirs should be classified as "persons to whom personal data is related" for the purpose of exercising the deceased's right to access, insofar as the data to which access is sought is necessary for the purpose of pursuing the action brought to obtain compensation.

The French Conseil d'Etat concluded that the decision of the French data protection authority was invalid.

To be compared with **Conseil d'Etat, 8 June 2016, Appeal no. 386525**, in which the Conseil d'Etat refused to recognise that a person's heirs were "persons to whom personal data is related" and thus dismissed their appeal against the decision of the French CNIL, which had refused to order that the phone records of the deceased be disclosed to them.

2.2. Guidelines emerging from the analysis

1) Data must be deemed as personal when the person, to whom the data refers to, is identifiable. Identifiability must be assessed through a relative criterion, taking into account whether there is a

reasonable possibility that the controller will be in a position to collect other pieces of information which allow to identify that person (Breyer, Case C-582/14).

2) While examining the legality of collecting and processing data that was collected through a dynamic IP address (registered by a social media provider) it is necessary to establish, whether the provider may identify the data subject with use of additional data that the internet service provider has at their disposal. If this condition is satisfied, the data collected through such IP address should be considered to constitute personal data (Breyer, Case C-582/14).

3) The concept of personal data processing should always be referred to within the particular factual circumstances. It can be understood, for instance, as the practice of public identification of private individuals by putting their contact details or information on employment or hobbies on a publicly available website (Lindqvist, Case C-101/01).

4) Processing of personal data may also be constituted — depending on the circumstances — by aggregation, indexing and storing information published on the internet by third parties (which may be proper e.g. for the online search engines) (Google Spain, Case C-131/12).

5) While establishing whether particular persons/entities act as controllers or as joint controllers of personal data, a court must establish whether such actor(s) exercise(s) effective control over purposes and means of processing data. In this investigation, courts must build on the actual facts of the case, without adopting all-embracing abstract and formal criteria (Fashion ID, Case C-40/17).

3. The exceptions to the protection of data, relating to activities outside of the scope of EU Law, in particular public security, state security, defence, and criminal matters

3.1. The general scope of exceptions under GDPR

Article 23 of the GDPR gives Member States the option to enact rules that restrict application of the data protection measures, if this is justified by goals legitimised by social or public reasons. The possible limitations may pertain to instruments enacted in Articles 12–22 (in connection with Article 5) and 34. Under Article 23, the domestic restrictions are compliant with EU law as long as they meet three cumulative criteria. (1) First of all, the restriction cannot infringe the essence of fundamental rights and freedoms that are protected under the GDPR rules restricted by a Member State. (2) Secondly, the imposed limitations should be necessary and proportionate to safeguard the intended aims. (3) Thirdly, the restrictions should serve one of the purposes listed in number by Article 23 (a)–(j) [on the content of this list, see below quotes from the applicable EU law].

At the same time, each legislative measures imposed by Member States should provide specific provisions with respect to: the purpose or categories of processing personal data; the categories of personal data being processed; the scope of restrictions to the GDPR; the measures that allow to prevent abuse, unlawful access or transfer of data; the specification of a relevant controller or categories thereof; the period for which the data is stored, as well as the relevant measures that apply in this regard; the risks to the rights and freedoms of data subjects; the indication of data subjects' right to be informed about the restriction (as long as such information may not be prejudicial to the purpose of the restriction).

Before the GDPR came into force, the similar exceptions were contained also in the 95/46/EC directive. Under the first subparagraph of Article 3 (2) the directive stated that the protection of personal data offered by the Directive shall not apply to the processing of personal data made "in the course of an activity which falls outside the scope of Community law", "and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law".

The more precise procedural steps applicable in the case of retention of data for security purposes have also been indicated in the Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (the so-called "Data Detention Directive"). It has remained in force after introduction of the GDPR and provides an additional point of reference in interpretation of its Article 23. The issue of data retention has been further addressed in ***Privacy International*** **(C-623/17) and in** ***La Quadrature du Net*** (C-511/18; C-512/18; C-520/18).

What is particularly noteworthy, is the fact that the issue of restrictions to data protection instruments of GDPR is not merely the matter of legislation at an EU and a domestic level, but, in many ways, remains connected with the fundamental rights guaranteed in the CFR. The general sense of this relation has been reflected in the opening part of Article 23 of the GDPR, which indicates that restricting measures imposed by Member States cannot infringe the essence of fundamental rights and freedoms that are protected by the GDPR. In other words, while Article 23 of the GDPR provides the general premises for restricting the protection of data, fundamental rights serve as the ultimate legitimisation to these restrictions. Consequently, the public aims enumerated in Article 23 GDPR need to be balanced with the

right of individuals to data protection, and must not allow any type of infringement of such a right merely on the vague grounds of "public security", "other important objectives of general public interest", etc.

Main questions addressed

1. In light of the principles of effectiveness and proportionality, to which extent may data subjects' rights to the protection of private life and personal data (Articles 7 & 8 of the Charter) be limited by Member States for the purpose of protecting public security, defence or State security?

2. In light of the Charter, Article 47 and the principle of proportionality, how does case law understand the exception to data protection related to state security?

3. In light of the Charter, Article 47 and the principle of proportionality, what is the understanding of the "safety" exception? How should the case law balance the right of data subjects and the collective interests related to safety and crime protection?

3.1.1. Question 1: The extension of the protection of data in the field of State security matters

In light of the principles of effectiveness and proportionality, to which extent may data subjects' rights to the protection of private life and personal data (Articles 7 & 8 of the Charter) be limited by Member States for the purpose of protecting public security, defence or State security?

Within the following cluster of cases, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

➢ Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases C-293/12 and C-594/12 (***Digital Rights Ireland***)

Cluster of relevant CJEU cases

➢ Judgment of the Court (Fourth Chamber), 17 October 2013, *Michael Schwarz* v. *Stadt Bochum*, C-291/12 (***Schwarz***)

➢ Judgment of the Court (Grand Chamber) of 8 April 2014, *Digital Rights Ireland Ltd* v *Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others*, Joined Cases C-293/12 and C-594/12 (***Digital Rights Ireland***)

➢ Judgment of the Court (Fourth Chamber), 16 April 2015, *W.P. Willems* v. *Burgemeester van Nuth,* and alii, Joined Cases C-446/12 to C-449/12 (***Willems***)

➢ Judgment of the Court (Grand Chamber), 21 December 2016, *Tele2 Sverige AB* v. *Post-och telestyrelsen* (C-203/15) and *Secretary of State for the Home Department,* (C-698/15), Joined cases (***Tele2***).

➢ Judgment of the Court (Second Chamber), 27 September 2017, *Puškár v. Finančné riaditeľstvo Slovenskej Republiky, Kriminálny úrad finančnej správy,* Case C-73/16 (***Puškár***)

➢ Opinion of the Court (Grand Chamber) of 26 July 2017, *Accord PNR UE-Canada*, Avis C-1/15 (***Accord PNR***)

➢ Judgment of the Court (Grand Chamber) of 8 April 2014, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs* and alii, Case C-623/17 (***Privacy International***)

➢ Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others v Premier ministre and Others*, Joint Cases C-511/18, C-512/18 and C-520/18 (***La Quadrature du Net***)

Relevant legal sources:

EU Level

European Convention on Human Rights:

Article 8 (right to the protection of private life)

Charter of Fundamental Rights of the EU:

Article 7 (right to protection of private life), article 8 (right to protection of personal data), article 52 (scope of guaranteed rights)

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 (GDPR)

Article 23 – Restrictions

Directive 95/46 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

Article 3 (2), Article 13(1)

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), as amended by Directive 2009/136

Article 1, Article 4 (1) and (2), Article 5 (1) and (3), Article 6 (1), Article 15 (1)

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

Recital 16, 21, 22

Article 1 to 9, 11 and 13

National Level

Irish law: Part 7 of the Criminal Justice (Terrorist Offences) Act 2005, which empowers Irish authorities to require providers of telecommunications services to retain telecommunications data for a period specified by law in order to prevent, detect, investigate and prosecute crime and safeguard the security of the State.

Austrian law: 2003 Law on Telecommunications (Telekommunikationsgesetz 2003), concerning the obligation to retain data and transposing Directive 2006/24 into Austrian law.

The case(s):

Digital Rights Ireland Ltd., the owner of a mobile phone registered on 3 June 2006, brought an action claiming that the Irish authorities had unlawfully processed, retained and exercised control over data related to its communications on 11 August 2006. First, it challenged the legality of several national measures that empowered Irish authorities to require providers of telecommunications services to retain telecommunications data for a period specified by law in order to prevent, detect, investigate and prosecute crime and safeguard the security of the State (in particular Part 7 of the Criminal Justice (Terrorist Offences) Act 2005). Second, it questioned the validity of Directive 2006/24 in light of the Charter and/or the European Convention for the Protection of Human Rights and Fundamental Freedoms. *Kärntner Landesregierung*, Mr Michael Seitlinger and 11,130 applicants brought actions before the Verfassungsgerichtshof (Austrian Constitutional Court), seeking the annulment of the provisions of the 2003 Law on Telecommunications (Telekommunikationsgesetz 2003) concerning the obligation to retain data and transposing Directive 2006/24 into Austrian law. The claimants took the view that such provisions constituted, *inter alia*, an infringement of Article 8 of the Charter.

In both cases, the national courts considered that they were not able to resolve the questions raised relating to national law unless the validity of Directive 2006/24 had first been examined and decided to maintain proceedings and to refer a question to the Court for a preliminary ruling.

Preliminary ruling referred to the Court:

Is Directive 2006/24, inasmuch as it obliges Member States to impose the retention of personal data by telecommunications services for national security motives, compatible with the right to privacy laid down in Article 7 CFREU (and Article 8 ECHR) and with the right to the protection of personal data laid down in Article 8 of the Charter?

Reasoning of the Court:

Firstly, the Court states that Directive 2006/24 derogates from the system of protection of the right to privacy established by Directives 95/46 and 2002/58. More particularly, the obligation (Article 3 of the Directive) on providers of publicly available electronic communications services or of public communications networks to retain certain data for the purpose of making them accessible, if necessary, to the competent national authorities, in itself, constitutes an interference with the rights guaranteed under Articles 7 and 8 of the Charter, since that 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. So does the access of the competent national authorities (Articles 4 and 8 of the Directive) to the data. **This interference, because it is wide-ranging, must be considered to be particularly serious.**

Secondly, the Court examines whether such interference may be justified in light of article 52(1) of the Charter, which provides that any limitation on the exercise of the rights and freedoms laid down by the Charter must be provided for by law, respect their essence and, be subject to the principle of **proportionality**, limitations may be made to those rights and freedoms 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.

The Court judges that, even if the interference is serious, it does not affect the essence of the fundamental rights protected by the Charter. It recognises that the interference satisfies an objective of general interest, since the material objective of Directive 2006/24 is to contribute to the fight against serious crime and thus, ultimately, to public security. The Court then engages in ***the evaluation of the interference in light of the principle of proportionality***. Recalling that the principle of proportionality requires that acts of the EU institutions be appropriate for attaining the legitimate

objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve those objectives, and that where interferences with fundamental rights are at issue, the extent of the EU legislature's discretion may prove to be limited, depending on a number of factors, in particular, including the area concerned, the nature of the right at issue guaranteed by the Charter, the nature and seriousness of the interference and the object pursued by the interference, the Court concludes that the EU legislature's discretion in the case at hand is reduced, with the result that review of that discretion should be strict.

Engaging in this review, the Court, after finding that data is a valuable tool for the objective pursued so that retention of such data may be seen as an appropriate measure for attaining that objective, states that given the importance of the fundamental rights at stake, EU legislation must lay down clear and precise rules governing the scope and application of the measure and impose minimum safeguards so that the persons whose data has been retained have sufficient guarantees to effectively protect their personal data against the risk of abuse and against any unlawful access and use of that data. With this in mind, the Court observes, as to the necessity of the measure, that: 1) the Directive applies to all means of electronic communication, the use of which is very widespread and of growing importance in people's everyday lives – of all subscribers and users, that is of the entire European population (no limits concerning the targeted data subjects); 2) whilst seeking to contribute to the fight against serious crime, the Directive does not require any relationship between the data whose retention is provided for and a threat to public security and, in particular, is not restricted to a retention of data in relation to targeted data (no limit concerning the targeted data); 3) there are no substantive or procedural conditions relating to the access of the competent national authorities to the data or to its subsequent use (no limit concerning access to data); 4) there is no reasonable time limitation on the retention period (no limit concerning the retention period). In light of this analysis, **the Court concludes that Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter.**

Finally, the Court adds that the directive does not require the data in question to be retained within the EU, with the result that control by an independent authority, explicitly required by Article 8(3) of the Charter, of compliance with the requirements of protection and security, as referred to in the two previous paragraphs, cannot be found to be guaranteed.

For the Court, by adopting Directive 2006/24, **the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in light of Articles 7, 8 and 52(1) of the Charter.** Although the decision mentions the principle of proportionality alone, it implicitly implements **the principle of effectiveness** since it is driven by the concern to guarantee an effective protection of personal data and private life; apart from this, the decision uses the expression "effective protection of the data" twice (§54, §66).

Conclusion of the Court:

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC is invalid.

Impact on the follow-up case:

In Austria, on 27 June 2014, in light of the CJEU's decision, the Austrian Constitutional Court declared national data retention laws void, finding that data retention, as implemented under Austrian law, represented a massive interference with the right to privacy and the right to data protection.

In Ireland, prior to the judgment in *Digital Rights Ireland*, the Communications (Retention of Data) Act, 2011 was enacted to give effect to Directive 2006/24 and, *inter alia*, to repeal Part 7 of the Criminal Justice (Terrorist Offences) Act, 2005. Digital Rights Ireland's claim was hence amended to reflect these statutory changes. After the judgment delivered by the CJEU in 2014 that declared the Directive 2006/24 invalid, Digital Rights Ireland sought an order to the CJEU, referring the following question: "whether, in light of the Provisions of the Charter of Fundamental Rights and Freedoms and the findings of the Court of Justice (sic) in Digital Rights Ireland v. Ireland a domestic legislative measure which requires indiscriminate retention of telecommunications data for a period longer than is required for the legitimate commercial purposes of the telecommunications providers, is valid". However, on 19 July 2017 the Irish High Court dismissed the application for a reference to the Court of Justice. Indeed, the Court deemed such a request not necessary to adjudicate upon the matter at that stage of the proceedings, when the facts of the case had not yet been clarified: "[i]t may be that the trial judge, when he or she has heard the relevant evidence in these proceedings, may decide that a reference to the CJEU is required to clarify the issue or issues in the case".[7]

In the EU, the invalidated directive has not been replaced.[8]

Following *Digital Rights Ireland*, several providers of electronic communications services across Europe decided that they would cease to retain electronic communications data, covered by national laws implementing the invalidated directive, and that they would erase data retained before the annulment of the directive. Such a position raised disputes in Member States, and new requests for a preliminary ruling from the Court.

The ***Tele2*** case is an example: Tele2, a provider of electronic communication services established in Sweden, decided that it would no longer retain electronic communications data, following the annulment of the directive by the Court. However, a special *rapporteur* appointed by the Swedish government concluded that Swedish legislation on the retention of data was not incompatible either with EU law or the European Convention for the Protection of Human Rights and Fundamental Freedoms. Tele2, which was ordered to continue retaining data, brought an action against the injunction. The Kammarrätten in Stockholm (Administrative Court of Appeal of Stockholm, Sweden) found it necessary for the CJEU to give clarification of its ruling in *Digital Rights Ireland*, since Article 15(1) of Directive 2002/58 introduces a derogation from the general rule that data is to be erased when no longer needed, insofar as it permits Member States, where justified on one of the specified grounds, to restrict that obligation to erase or render anonymous, or even to make provision for the retention of data. Accordingly, in certain situations, EU law allows for the retention of electronic communications data.

The question referred to the Court was whether, given the invalidity of Directive 2006/24, article 15(1) of Directive 2002/58, read in the light of articles 7 and 8 and Article 52(1) of the Charter, must be interpreted as precluding national legislation such as that at issue in the main proceedings that provides, for the purpose of fighting crime, for general and indiscriminate retention of all traffic and location data of all subscribers and registered users with respect to all means of electronic communications.

The Court, after proceeding with assessment quite similar to the one endorsed in *Digital Ireland*, based **on the principle of proportionality**, concludes that Article 15(1) of Directive 2002/58, read in light of Articles 7, 8 and 11 and Article 52(1) of the CFREU, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention

[7] These parts are extracted and/or based at least partially on the database template drafted by Isabella Oldani.
[8] These parts are extracted and/or based at least partially on the database template drafted by Isabella Oldani

of all traffic and location data of all subscribers and registered users relating to all means of electronic communication.

The Court also concludes that article 15(1) of Directive 2002/58, read in light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation governing the protection and security of traffic and location data and, in particular, access by the competent national authorities to the retained data, where the objective pursued by that access, in the context of fighting crime, is not restricted solely to fighting serious crime, where access is not subject to prior review by a court or an independent administrative authority, and where there is no requirement that the data concerned should be retained within the EU.

Elements of judicial dialogue:

The balance between the data subjects' rights to privacy and protection of data, and the general interest in ensuring public security, is at the heart of numerous CJEU decisions.

In the earlier ruling of the Court in ***Schwarz***, on the question whether Regulation No 2252/2004, which created the obligation to take the fingerprints of persons applying for passports, should be declared invalid because it infringes Articles 7 and 8 of the CFREU of the EU ('the Charter'), the Court answers that the infringement, although effective, is justified in light of Article 52 of the Charter. The regulation is pursuing an objective of general interest, i.e., preventing falsification of passports and hindering their fraudulent use. And the measure is proportionate, since no other identification system (iris ID) would be less infringing of the fundamental rights guaranteed by the Charter.

The decision in *Schwarz* has been complemented by the decision of the Court in *Willem*: Regulation No 2252/2004 as amended by Regulation No 444/2009, which is not applicable to identity cards issued by a Member States to its nationals, regardless of the period of validity and the possibility of using them for the purposes of travel outside that State, does not require Member States to guarantee, in their legislation, that biometric data collected and stored in accordance with that regulation will not be collected, processed and used for purposes other than the issue of the passport or travel document, since that is not a matter that falls within the scope of that regulation.

In ***Puskar***, the Court rules that the collection of tax and combating tax fraud must be regarded as tasks carried out in the public interest within the meaning of Article 7 of Directive 95/46. However, since "the protection of the fundamental right to respect for private life at the European Union level requires that derogations from the protection of personal data and its limitations be carried out within the limits of what is strictly necessary", the derogation from such a protection has to be proportionate to the objective pursued.

In ***La Quadrature du Net*** (C-511/18; C-512/18; C-520/18), the Court stated that Article 15(1) of Directive 2002/58/EC, read in light of Articles 7, 8 and 11 and Article 52(1) CFR, must be interpreted:

1. **as precluding** legislative measures which establishes the preventive measure of the general and indiscriminate retention of traffic and location data for the purposes of Article 15(1) Directive 2002/58 (as a restriction which constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system).
2. **As not precluding** legislative measures that:

i) allow, for the purposes of safeguarding national security, recourse to an instruction requiring providers of electronic communications services to retain, generally and indiscriminately, traffic and location data in situations where

- the Member State concerned is confronted with a serious threat to national security that is shown to be genuine and present or foreseeable, and

- the decision imposing such an instruction is subject to **effective review**, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that one of those situations exists and

that the conditions and safeguards which must be laid down are observed, and that instruction may be given only for a period that is limited in time to what is strictly necessary, but which may be extended if that threat persists;

ii) provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the targeted retention of traffic and location data which is limited, on the basis of objective and non-discriminatory factors, according to the categories of persons concerned or using a geographical criterion, for a period that is limited in time to what is strictly necessary, but which may be extended;

iii) provide, for the purposes of safeguarding national security, combating serious crime and preventing serious threats to public security, for the general and indiscriminate retention of IP addresses assigned to the source of an Internet connection for a period that is limited in time to what is strictly necessary;

iv) provide, for the purposes of safeguarding national security, combating crime and safeguarding public security, for the general and indiscriminate retention of data relating to the civil identity of users of electronic communications systems;

v) allow, for the purposes of combating serious crime and, *a fortiori*, safeguarding national security, recourse to an instruction requiring providers of electronic communications services, by means of a decision of the competent authority that is subject to **effective judicial review**, to undertake, for a specified period of time, the expedited retention of traffic and location data in the possession of those service providers,

provided that those measures ensure, by means of clear and precise rules, that the retention of data at issue is subject to compliance with the applicable substantive and procedural conditions and that the persons concerned have effective safeguards against the risks of abuse.

3. as not precluding national rules which requires providers of electronic communications services to have recourse, first, to the automated analysis and real-time collection, *inter alia*, of traffic and location data and, second, to the real-time collection of technical data concerning the location of the terminal equipment used, where:
i) recourse to automated analysis is limited to situations in which a Member State is facing a serious threat to national security which is shown to be genuine and present or foreseeable, and where recourse to such analysis may be the subject of **an effective review**, either by a court or by an independent administrative body whose decision is binding, the aim of that review being to verify that a situation justifying that measure exists and that the conditions and safeguards that must be laid down are observed; and where

ii) recourse to the real-time collection of traffic and location data is limited to persons in respect of whom there is a valid reason to suspect that they are involved in one way or another in terrorist activities and is subject to a prior review carried out either by a court or by an independent administrative body whose decision is binding in order to ensure that such real-time collection is authorised only within the limits of what is strictly necessary. In cases of duly justified urgency, the review must take place within a short time.

Furthermore, the Court states that Article 23(1) GDPR, allows Member States to restrict, for the purposes of the objectives that it provides for and by means of legislative measures, the scope of the obligations and rights that are referred to therein 'when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and **proportionate measure** in a democratic society to safeguard' the objective pursued. Then, the Court considered that any legislative measure adopted on that basis must, in particular, comply with the specific requirements set out in Article 23(2) of that regulation. Accordingly, the Court stated that Article 23(1) and (2) GDPR cannot be interpreted as being capable of conferring on Member States the power to undermine respect for private life, disregarding Article 7 of the Charter, or any of the other guarantees enshrined therein. Furthermore, the Court affirmed that **the power conferred on Member States by Article 23(1) of Regulation 2016/679 may be exercised only in accordance with the requirement of proportionality**, according to which derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary. In light of the above, the CJEU stated that Article 23(1) of Regulation 2016/679, read in light of Articles 7, 8 and 11 and Article 52(1) of the Charter, must be interpreted as precluding national legislation which requires that providers of access to online public communication services and hosting service providers retain, generally and indiscriminately, *inter alia*, personal data relating to those services.

Impact on national case law in Member States different from the state of the court referring the preliminary question to the CJEU:

As a result of *Digital Rights Ireland*, several national data retention laws have been held invalid by national courts. By way of example, on 11 March 2015, the District Court of The Hague suspended the 2009 Telecommunications Data Retention Act (TDRA), which was drafted on the basis of the EU Data Retention Directive. By the same token, Digital Rights Ireland largely inspired the decision of the Belgian Constitutional Court on 11 June 2015, to annul the Belgian data retention law. The Constitutional Courts of Slovakia, Slovenia, Romania and Bulgaria also annulled their respective national data retention provisions.

France

***Conseil d'Etat*, 5 May 2017, No. 396669**

The decision deals with the claim of a data subject relating to his right of access to data related to him, data which was allegedly held by several State services dedicated to the protection of the territory (namely "*Direction de la protection et de la sécurité de la défense* (DPSD)", now "*Direction du renseignement et de la sécurité de la défense* (DRSD)", and "*service du renseignement territorial*"). The French supervisory authority answered the claimant by stating that all relevant verifications had been conducted, and that the procedure was over, without giving further information.

The French *Conseil d'Etat* observes that a specific body has been created to ensure the verification of such sensitive registers. The role of this body is to verify if data related to the claimant is included in the registers, on the basis of the elements communicated to it in a non-adversarial manner, and if so, whether such an inclusion is justified, relevant and proportionate in regard to the purposes of the registers. If the body finds that the data is not registered, or that the data is lawfully included in the register, then the judge must dismiss the claim. On the contrary, if the body finds that the data has been unlawfully included in the register, or that the data registered is inaccurate, incomplete, equivocal, or outdated, it shall inform the claimant, without mentioning information protected by national defence secrecy. The unlawful processing of data, which may be found by the court, if necessary, on its own motion, implies that the data must be deleted or rectified.

The French *Conseil d'Etat* concludes that in the case at hand, the verification revealed that the claimant's data was unlawfully included in the said registers. It orders that the data be erased.

Italy

The Italian Criminal Court of Cassation in its decision of 13 February 2020, n. 5741 stated that the Italian legislation in the sector is not contrary to the fundamental principles of the European Convention on the right to privacy, since the Italian legislation contains the statement of the purpose of repression of crimes, the temporal delimitation of the storage activity, the preventive intervention of the judicial authorities, functional to the effective control of the strict need for access to data, as well as compliance with the principle of proportionality. According to the Italian Court of Cassation, the Italian regulations on the storage of traffic data is not in contrast with Digital rights Ireland and Tele2, since that legislation provides for the retention of data for a limited period of 24 months, subordinates the possibility of collection of those data only for the purpose of ascertaining and prosecuting crimes, provides that the use of that data is subject to the acquisition order issued by the Public Prosecutor, (i.e. a judicial body that acts in the context of a preliminary investigation). Accordingly, the Court stated, that Italian legislation does not provide for the power of the public authorities to indiscriminately access sensitive data but limits it to cases of investigations for offences carried out within a given period of time of 24 months (increased to 72 only for offences of particular social alarm) and makes it subject to authorisation from a judicial body.

This judgement is coherent with previous case law of the Italian Criminal Court of Cassation (Judgement of 23 August 2019, n. 36380; 19 July 2018, n. 33851).

Netherlands

In the judgment of 5 February 2020 (C-09-550982) the District Court of the Hague established that infringement to the right to privacy, guaranteed in Article 8 ECHR, instigated by a public authority in order to prevent fraud, was not proportionate to the aim of combatting fraud in social security payments. The judgment concerned the Dutch Risk Indication System (SyRI), designed for the purpose of combatting and preventing fraud in labour laws, social security and tax. As the Court found in its motives, under Article 8 ECHR the Netherlands as a Member State must carefully balance the benefits of new technologies with the right to privacy. The Court considers that SyRI does not strike this balance and is therefore incompatible with Article 8(2) ECHR, as it not necessary in a democratic society or proportional. Apart from the ECHR, the Court also referred to Articles 7 and 8 CFREU, as well as to the GDPR, as parallel sources of the right to privacy. The exact architecture of the system was not revealed during the proceedings – in particular, it was not certain whether it is based on deep learning and profiling schemes. As the Court found, this may infringe individuals' interests by creating biases that would be non-transparent due to system's secrecy. Furthermore, the amount of data collected by the system is not compliant with the principle of data minimisation.

3.1.2. Question 2: The role of effective judicial protection and proportionality in establishing the state security exception.

2. In light of the Charter, Article 47 and the principle of proportionality, how does the case law understand the exception to data protection related to state security?

Within the cluster of cases, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

Judgment of the Court (Second Chamber), 27 September 2017, *Puškár v. Finančné riaditeľstvo Slovenskej Republiky, Kriminálny úrad finančnej správy,* Case C-73/16 (***Puškár***)

The case(s):

Mr Puškár claimed of the Supreme Court of the Slovak Republic that his name be removed from a list of the persons who act as "fronts" in the role of company directors in the Slovak Republic. The list was administered by the Slovak Finance Directorate. Although the list could only circulate among administrative offices, Mr. Puškár maintained that such list (containing the Identity Number and Tax Identification Number of each mentioned individual) constituted a violation of his rights and thus asked for the removal of his name and of any reference to him from the list and from other similar lists, as well as from the finance authority's IT system. As was established in the domestic proceedings, the list was protected by relevant technical and organisational measures from "unauthorised disclosure or access" in the sense of Article 17(1) of Directive 95/46. Mr Puškár, however, failed to evidence that he obtained the list with the consent of the administrative authority that administered this data. The Supreme Court dismissed the claim, pointing out that Mr Puškár did not exhaust the measures available under the domestic law.

The Supreme Court dismissed Mr. Puškár's case (along with two other claimants who made the same application), pointing out that he did not exhaust all the measures available to him under domestic law. The decision was challenged by Mr. Puškár before the Constitutional Court of the Slovak Republic.

While deciding on the appeal, the Constitutional Court focused mainly on the jurisprudence of Article 6(1) ECHR in connection with Article 46 of the Slovak Constitution. In particular, it addressed the obligation of the courts to justify their decision taking all the relevant facts and legal arguments into account. The Court deemed this obligation to be the necessary precondition for the parties to exercise their right to an effective remedy. This conclusion has been drawn from Article 46 (1) of the Slovak Constitution, read in connection with Article 6 (1) ECHR, as interpreted in the ECtHR jurisprudence (*Garcia Ruiz v. Spain*; *Van de Hurk v. the Netherlands*; *Ruiz Torija v. Spain*; *Georgiadis v. Greece*; *Suominen v. Finland*; *Vetrenko v. Moldova*; *Wagner and J.M.W.L. v. Luxembourg*; *Pronina v. Ukraine*; *Krasulya v. Russia*; *Hiro Balani v. Spain*).

By making this assertion, the Constitutional Court affirmed that in order to comply with the requirements of Article 46 of the Constitution (along with Article 6 ECHR) the analysis of the Supreme Court should have taken into consideration all circumstances of the case that are relevant for the level of personal data protection (as guaranteed by the Constitution), as well as for the level of privacy protection (as guaranteed by the ECHR). Resting upon this initial observation, the Constitutional Court concluded — after having analysed and compared the national and ECtHR jurisprudence — that the Supreme Court had failed to take into account the factual and legal arguments of the case. Moreover, due to the Constitutional Court's conclusions, the Supreme Court was obliged to provide a decision with regard to conditions that have been met.

The Constitutional Court then affirmed that the Supreme Court had infringed the applicant's fundamental rights, namely the right to an effective remedy and a fair trial, the right to privacy and the right to protection of personal data. Thus, the Constitutional Court referred the case back to the Supreme Court. During the re-hearing of the case, the Supreme Court came to the conclusion that the Constitutional Court had not taken into account case-law of the CJEU relevant for the matters discussed in the case. For these reasons, the Court submitted preliminary questions to the CJEU.

Preliminary questions

The Slovak Supreme Court presented four questions; for the purpose of this analysis, only the second question will be addressed in detail in this section:

Can the right to respect for private and family life, home and communications, in Article 7 of the Charter, and the right to the protection of personal data in Article 8 be interpreted to the effect that where there is an alleged violation of the right to the protection of personal data, which, with respect to the EU, is implemented primarily through Directive 95/46, and under which, in particular

– the Member States must protect the right to privacy with respect to the processing of personal data (Article [1](1)), and

– the Member States are authorised to process personal data where this is necessary for the implementation of a task performed in the public interest (Article 7(e)) or is necessary for the purpose of a legitimate interests that is performed by the responsible authority or by the third party or parties to whom the data are disclosed, and

– a Member State is exceptionally authorised to limit obligations and rights (Article 13(1)(e) and (f)), where such a restriction is necessary to safeguard an important economic or financial interest of a Member State or of the EU, including monetary, budgetary and taxation matters,

are interpreted in such a way as not to allow a Member State to create, without the consent of the person concerned, a list of personal data for the purposes of tax administration, so that the fact that personal data is made available to a public authority for the purpose of combating tax fraud in itself constitutes a risk?

Reasoning of the Court:

In analysis of the second question, the Court had to establish, whether the 95/46/EC Directive, as well as Articles 7 and 8 of the CFREU preclude processing of personal data by the authorities of a Member State for the purpose of collecting tax and copying with tax frauds — even, if data subjects do not agree on such processing. Despite position of the claimant, the Court found that this issue is not clearly irrelevant for the case decided before the Slovak Court and hence, it constitutes a valid ground for a preliminary question.

Regarding the substance of the question, the CJEU observed that processing of personal data should not only satisfy the requirements set in the 95/46 Directive but should also be compliant with Articles 7 and 8 of the CFR. Since setting the contested list of company directors was a form of data processing, it should be in line with the general standards of using data set in Article 7 of the 95/46 directive. In the circumstances of the case, it requires particular attention to Article 7(e), according to which processing of personal data may be justified, if "it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed".

Further, the Court concluded that the way of setting the list in question does not seem to comply with these standards. Notwithstanding the fact that collecting taxes and combatting tax fraud is carried out in public interest, it should be determined, whether the way, how the data was used, was necessary for these tasks. In making this assessment it should be taken into account, in particular, what was the specific purpose of establishing the list, what are the legal effects that pertain to the person and the public nature of the list, as well as whether the list has a public nature. This assessment should meet the criteria of proportionality — by using personal data solely in a way that allows to choose the least restrictive measure.

Inclusion of a person on the list may harm her rights, by undermining her reputation and causing difficulties in relations with fiscal administration. In this respect it may, in particular, contradict the

presumption of innocence of such person and undermine freedom of her business activity (freedom of enterprise). For these reasons, as the Court concluded, "an infringement of this kind can be **proportionate** only if there are sufficient grounds to suspect the person concerned of purportedly acting as a company director of the legal persons associated with him and accordingly undermines the public interest in the collection of taxes and combating tax fraud." According to the CJEU, this assessment should be carried out by the domestic court, taking into consideration all the relevant circumstances of the case.

Conclusion of the Court:

The Court declared that the assessment of lawfulness of processing personal data in question should be carried out by the domestic authorities. The 95/46 Directive, which provides the basis for this assessment, does not preclude processing of personal data by the competent domestic bodies for the aims related to collecting taxes and copying tax fraud. The consent of data subjects is not required in such situation, providing that (1) processing of data is carried out in public interest, that (2) it remains necessary for the intended purpose, and that (3) there is sufficient indication allowing to assume that "the data subjects are rightly included in that list" and "that all of the conditions for the lawfulness of that processing of personal data imposed by Directive 95/46 be satisfied".

Elements of judicial dialogue:

The CJEU decision was triggered by a preliminary question of the Slovak Supreme Court that wanted to established, amongst other issues, whether processing of personal data for the purposes related to tax administration. The CJEU acknowledges that the contrast between the national courts may affect the results of the decision in a specific case; thus, it addresses the problem of coordination between administrative and judicial enforcement systems in detail.

It is important to note that the conclusion of the CJEU is based on the jurisprudence of the same court in other areas of law, namely public procurement (e.g. *SC Star Storage*, C-439/14 and C-488/14), migration and asylum law (e.g. decisions in *Tall*, C-239/14 and *Sacko*, C-348/16), and in particular electronic communication (e.g. *Alassini*, C-317/08 to C-320/08) and consumer protection (e.g. *Menini, C-75/16*).

From a different standpoint, the judicial dialogue between European and national courts at the same time addresses the horizontal aspect, with the decision of the CJEU able to provide a uniform interpretative perspective so to avoid further conflicts.

3.1.3. Question 3: The role of effective judicial protection and proportionality in establishing the state security exception

3. In light of the Charter, Article 47 and the principle of proportionality, what is the understanding of the "safety" exception? How should the case law balance right of data subjects and the collective interests related to safety and crime protection?

Within the following cluster of cases, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

➢ Judgment of the Court (First Chamber), 3 October 2019, *Staatssecretaris van Justitie en Veiligheid*

v A, B, P, C-70/18 (***Staatssecretaris***)

Cluster of relevant CJEU cases

➢ Judgment of the Court (First Chamber), 3 October 2019, *Staatssecretaris van Justitie en Veiligheid* v A, B, P, C-70/18 (***Staatssecretaris***)

➢ Judgment of the Court (Second Chamber) of 14 February 2019, *Sergejs Buivids*, C-345/17 (***Buivids***)

➢ Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others v Premier ministre and Others*, Joint Cases C-511/18, C-512/18 and C-520/18 (***La Quadrature du Net***)

➢ Case *B.* v. *Latvijas Republikas Saeima*, C-439/19 (***Latvijas Republikas Saeima***) [pending]

The case(s):

The preliminary question, submitted by the Dutch court, pertained to Article 7 of Decision Nom 2/76 of 20 December 1976 adopted by the Association Council set up by the Agreement establishing an Association between the European Economic Community and Turkey, signed in Ankara on 12 September 1963 by the Republic of Turkey, on the one hand, and by the Member States of the European Economic Community (EEC) and the Community, on the other, and concluded, approved and confirmed on behalf of the Community by Council Decision 64/732/EEC of 23 December 1963 (OJ 1973 C 113, p. 1; 'the Association Agreement'), and of Article 13 of Decision No 1/80 of the Association Council of 19 September 1980 on the development of the Association. The questions were asked upon two proceeding between the Dutch State Secretary for Justice and Security, which addressed obligation to of Turkish citizens A, B and P to cooperate in collecting their biometric data by the Dutch authority. The purpose of this collection was to grant them a temporary residence permit in the Netherlands, as prescribed by the two international agreements mentioned above.

All the individuals involved in the cases challenged administrative decisions to collect their biometric data. After dismissal of the complaints by the administrative authority, the District Court in the Hague found them justified. First of all, it indicated that the requirement of data collection constituted a 'new restriction' in the sense of Article 7 of Decision No 2/76 and Article 13 of Decision No 1/80. Secondly. It pointed out that the requirement was disproportionate regarding its aim, *i.e.,* prevention and combatting identity and document fraud. Upon these grounds the Court declared the administrative decisions in question invalid.

Preliminary questions

While deciding on an appeal of the District Court judgment, the Dutch Council of State referred four preliminary questions to the CJEU. For the sake of further analysis, the first of these questions will be discussed at length. The domestic court inquired the CJEU on clarifying whether Article 7 of Decision No 2/76 1 and Article 13 of Decision No 1/80 allow Member States to store and process biometric data of third-country nationals (including Turkish nationals) in a system that constitutes a filing system in the meaning of Article 2(a) and (b) of 95/46/EC Directive. By a preliminary question the Dutch court seeks to establish, in particular, whether such storage and processing can be justified by the fact that national rules do not go further than is necessary to achieve the legitimate objective, pursued by that rule, of preventing and combating identity fraud and document fraud.

Reasoning of the Court:

In analysis of the question, the Court observed that both Article 7 of Decision No 2/76 and Article 13 of Decision No 1/80 in general prohibit Member States from imposing additional measures that would limit freedom of movement for employees who are Turkish nationals. By requiring Turkish nationals to share their biometric data with Dutch authorities, the Netherlands introduced additional restriction, which was generally prohibited by the Decision No 1/80.

At the same time, however, the Court found that the measures introduced by the Dutch government can be justified on the grounds of overriding public interest reasons. According to the CJEU, collection and processing of personal biometric data is justifiable, in the circumstances of the case, by the public security reasons in the EU Member State. Collection of biometric data (fingerprints) supports the control of legality of entering the territory of EU Member States by third-state nationals. Furthermore, the biometric data allows to identify the third-country national and help preventing identity and document fraud.

The Court also ascertained that the measures introduced in the Dutch law meet the criterion of **proportionality**. In making this assessment the Court referred to Articles 7 and 8 CFREU in particular, which declare protection for a person's private life, including privacy in the context of processing personal data. The Court found that the data collected by the Dutch government is limited to only 10 fingerprints and a facial image. As such, it does not include any details of intimate nature nor causes physical or mental discomfort for individuals subjected to the screening procedure. A similar standard for data collection, as the Court further observed, has been introduced also by the EU itself, for instance in the context of 767/2008 Regulation. The measures adopted by the Netherlands are also justifiable in terms of their personal scope, since there would be no reasonable way to limit their application to selected third-country nationals. Moreover, the access to the data is limited only to authorised public officials of the Member State and is legally allowed only to the extent necessary to establish or verify identity of third-party nationals. Finally, the domestic law mandates that the personal data is erased after five years from one of the specified events, namely: after an application for a residence permit is rejected, the person left the country after the end of her legal stay or the period of an entry ban or a declaration of undesirability expired. The biometric data is destroyed also after naturalisation of a third-country national in the Netherlands.

With this in mind, the Court concluded that the measures adopted by the Netherlands constitute a limit to privacy that is adequate to the justified public policy aims that the Member State pursues through collecting and processing data.

Conclusion of the Court:

The Court concluded that the Dutch rules on collecting and processing biometric data of third-country nationals who apply for a residence permit, constitutes a new restriction to free movement of persons, in the sense of Decision No 1/80. At the same time, however, this restriction can be justified by the public policy aims, namely combatting identity and document fraud.

Elements of judicial dialogue:

The ***Staatssecretaris*** decision belongs to a long line of CJEU decisions that tackle the rights of non-EU foreigners in the proceedings before domestic EU bodies. The discussed judgment subscribes itself into the existing case law and hence, into the standard of protection awarded to foreigners seeking entry or asylum in the territory of one of the EU Member States. First of all, the *Staatssecretaris* decision builds on the previous cases concerning protection of privacy of third-country individuals, in particular the *Schwarz*

(C-291/12), as well as *Volker und Markus Schecke and Eifer* (C 92/09 and C 93/09) cases, along with the *Accord PRN* (1/15) opinion. Secondly, the judgment also addressed the issue of adequacy of measures imposed by public authorities upon individuals, referring to the relevant part of the *Accord PRN* (1/15) opinion. From this vantage point, the preliminary reference in *Staatssecretaris* engaged itself in a dialogue with this existing body of case law. The case aims to establish a standard of protection for third-country individuals with regard to collection, retaining and processing their data, accrued in the course of relocation proceedings.

Furthermore, a relevant case is *La Quadrature du Net* (C-511/18; C-512/18; C-520/18), where the CJEU considered that the possibility of an effective judicial review is an element to be considered in assessing the legitimacy of a national measure taker pursuant to Article 15 Directive 2002/58 (See the § *Elements of judicial dialogue* in Question 1).

3.2. Guidelines emerging from the analysis

The adequacy test performed by domestic courts

While assessing whether domestic authorities process data lawfully, a domestic court should establish whether the applied means are adequate to the public interest in retaining and processing the data.The adequacy can be established only as long as: (1) processing of data is carried out in the public interest, that (2) it remains necessary for the intended purpose, and that (3) there is sufficient indication allowing to assume that "the data subjects are rightly included in that list" and "that all of the conditions for the lawfulness of that processing of personal data imposed by Directive 95/46 be satisfied".

Protection awarded by the EU data protection rules applies also to third-country individuals who are subjected to administrative proceedings before the domestic authorities in EU Member States. The general adequacy test applies in these situations adequately.

4. Impact of the Charter on the assessment of the legitimacy of data processing

4.1. Introduction. The lawful basis for processing and Article 8 CFREU between Directive 95/46 and Regulation UE 2016/679

Article 8(2) CFREU states that personal 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 (…)".
The wording of this article makes it clear that the
fundamental right to data protection requires for personal data to be processed only if there is a specific lawful basis for doing so. The general framework of the lawful basis for processing is laid down by Regulation EU 2016/679, and before its entry into force by Directive 1995/46. Those two legal acts are quite different, but their basic approach is similar and reflects Article 8(2) CFR. For this reason, the CJEU's judgments related to interpreted Article 7 of Directive 95/46 are to be taken into account in interpreting and applying Article 6 Regulation EU 2016/679 (GDPR).
Article 7 of Directive 95/46 provided:
Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent; or
(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; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) 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 in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).
Article 6 GDPR, entitled "Lawfulness of processing" provides:
"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 official authority vested in the controller;
(e) 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 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".

In interpreting the legal bases for processing, the right to data protection (Article 8 CFR) and the right to a private life (Article 7 CFR) come into play. Furthermore, other fundamental rights should be taken into account, such as the right to an effective remedy and to a fair trial (Article 47 CFR), or the freedom of information (see Chapter 5). Moreover, the relevance of fundamental rights of third parties (other than the data subject and the data controller) raises the question whether in some cases third parties can successfully request access to personal data.

Main questions addressed in this chapter:

1. How is the interpretation of the concept of "legitimate interest" as a lawful basis for processing (Article 6, par. 1, let. f) influenced, in light of Article 47, Article 7 and Article 8, CFR, by the effective protection of data subjects?

2. In light of the principle of effectiveness and of Article 8 CFR, is data subject's consent valid if data processing is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent?

3. In light of the principle of effectiveness and proportionality, can an individual, relying on the right to an effective remedy (Article 47 CFR) for the protection of a fundamental right (e.g., the right to intellectual property), require that a data controller gives her access to that personal data which are necessary for exercising that fundamental right?

4.1.1. Question 1: The legitimate interest as a lawful basis for processing[9]

Within the following cluster of cases, the main case that is to be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

➢ Judgment of the Court (Third Chamber). 11 December 2019, *TK v Asociația de Proprietari bloc M5A-ScaraA*, Case C-708/18 (***Asociația de Proprietari***)

Relevant CJEU cases

➢ Judgment of the Court (Third Chamber), 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), Federación de Comercio Electrónico y Marketing Directo (FECEMD)* v. *Administración del Estado*, Joined cases C-468/10 and C-469/10 (***ASNEF and FECEMD***)

➢ Judgment of the court (Second Chamber), 19 October 2016, *Patrick Breyer* v. *Bundesrepublik Deutschland, Case C-582/14* (***Breyer***)

➢ Judgment of the Court (Second Chamber), 4 May 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde* v. *Rīgas pašvaldības SIA 'Rīgas satiksme'*, Case C-13/16 (***Rīgas satiksme***).

➢ Judgment of the Court (Third Chamber). 11 December 2019, *TK v Asociația de Proprietari bloc M5A-ScaraA*, Case C-708/18 (***Asociația de Proprietari***)

➢ Judgement of the Court, 17 June 2021, *M.I.C.M. Mircom International Content Management & Consulting Limited v Telenet BVBA*, Case C-597/19, (***M.I.C.M.***)

➢ Request for a preliminary ruling from the Administrativen sad Blagoevgrad (Bulgaria) lodged on 23 March 2021 — *VS v Inspektor v Inspektorata kam Visshia sadeben savet*, Case C-180/21 [pending]

➢ Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged

[9] Drafted by C. Angiolini

on 22 April 2021 — *Facebook Inc. and Others v Bundeskartellamt*, Case C-252/21; **Facebook Inc. and Others** [pending]

➢ Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) lodged on 2 February 2022 — *AB v Land Hesse* (C-64/22)

➢ Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) lodged on 11 January 2022 — UF v Land Hesse (Case C-26/22)

Main question addressed

4. How does the interpretation of the concept of "legitimate interest" as a lawful basis for processing (Article 6, par. 1, lett. f) is influenced, in light of Article 47, Article 7, Article 8, and Article 52 CFR, by the effective protection of data subjects?

Relevant legal sources

EU Level

Directive 95/46

Article 1 (1) Object of the Directive: "(…)Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".

Article 7 of the Directive

See §1.1.

The case

TK lives in an apartment which he owns. At the request of certain co-owners of the building where the apartment is located, the association of co-owners adopted a decision approving the installation of video surveillance cameras in that building. Then, three video surveillance cameras were installed in the common parts of the building. TK objected to that video surveillance system being installed, on the ground that it constituted an infringement of the right to respect for private life.

He brought an action before the referring court requesting that the association of co-owners be ordered to remove the three cameras and to take them out of operation definitively.

TK argued that the video surveillance system at issue infringed EU primary and secondary law, in particular the right to respect for private life. The association of co-owners stated that the decision to install a video surveillance system had been taken up in order to monitor who entered and left the building as effectively as possible, since the lift had been vandalised on many occasions and there had been burglaries and thefts in several apartments and in common parts. The association also stated that other measures which it had taken previously, namely the installation of an intercom/magnetic card entry system, had not prevented repeat offences of the same nature being committed. In addition, the association of co-owners sent TK several memoranda which show that the system's hard drive had been erased and disconnected, that it had been taken out of operation and that the images recorded had been deleted and that the video surveillance cameras had been uninstalled. However, TK stated that the three video surveillance cameras were still in place before the referring court.

Preliminary questions referred to the Court

The referring court considered that within national law the processing of personal data were admissible only with the consent of the data subject, with several exceptions (Article 5 law No 677/2001, implementing Directive 95/46 CE). One of those exceptions allowed the processing of personal data

where it is required in order to protect the data subject's life, physical integrity or health or those of a threatened third party.
The referring court relied on Article 52(1) of the Charter, and more specifically on the principle according to which there must be proportionality between the aim pursued by the interference with the rights and freedoms of citizens and the means used. Accordingly, the regional court of Bucharest referred the following questions to the CJEU for a preliminary ruling:
'(1) Are Articles 8 and 52 of the Charter and Article 7(f) of Directive 95/46 to be interpreted as precluding provisions of national law such as those at issue in the main proceedings, namely Article 5(2) of [Law No 677/2001], and Article 6 of [Decision No 52/2012 of the ANSPDCP], in accordance with which video surveillance may be used to ensure the safety and protection of individuals, property and valuables and for the pursuit of legitimate interests, without the data subject's consent?
(2) Are Articles 8 and 52 of the Charter to be interpreted as meaning that the limitation of rights and freedoms which results from video surveillance is in accordance with the principle of proportionality, satisfies the requirement of being 'necessary' and 'meets objectives of general interest or the need to protect the rights and freedoms of others', where the controller is able to take other measures to protect the legitimate interest in question?
(3) Is Article 7(f) of Directive 95/46 to be interpreted as meaning that the 'legitimate interests' of the controller must be proven, present and effective at the time of the data processing?
(4) Is Article 6(1)(e) of Directive 95/46 to be interpreted as meaning that data processing (video surveillance) is excessive or inappropriate where the controller is able to take other measures to protect the legitimate interest in question?'

Reasoning of the Court

With regard to the lawful basis of the legitimate interest (Article 7, lett. f) Directive 95/46), the CJEU affirmed that that provision laid down three cumulative conditions in order for the processing of personal data to be lawful:
1) **the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed**. In the present case, the CJEU stated that this condition is fulfilled, because the objective which the controller essentially seeks to achieve when they install a video surveillance system, namely protecting the property, health and life of the co-owners of a building, is likely to be characterised as a 'legitimate interest', within the meaning of Article 7(f) of Directive 95/46. The CJEU affirmed that **the interest is to be considered present and effective** because the referring court notes that thefts, burglaries and acts of vandalism had occurred before the video surveillance system was installed and that was despite the previous installation, in the entrance to the building, of a security system comprising an intercom/magnetic card entry.
2) **the need to process personal data for the purposes of the legitimate interests pursued**. In that regard, the CJEU recalled its previous case law (*Rīgas satiksme*, C-13/16, §30) where it was pointed out that derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.
The CJEU stated that the referring court must ascertain that the legitimate data processing interests pursued by the video surveillance **cannot reasonably be as effectively achieved by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 of the Charter.**
Within the CJEU reasoning, the **proportionality** principle is at stake: the proportionality of the data processing by a video surveillance device must be assessed by taking into account the specific methods of installing and operating that device, which must limit the effect thereof on the rights and freedoms of data subjects while ensuring the effectiveness of the video surveillance system at issue. Furthermore, the

CJEU mentioned the **data minimisation principle**, according to which personal data must be 'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed' (Art. 5 (1)(c) GDPR. Before the entry into force of the GDPR, Article 6(1)(c) Directive 95/46 established such a principle).

3) **the fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interest pursued.** The CJEU, recalling its previous case law (*ASNEF and FECEMD*, joined cases C-468/10 and C-469/10) stated that **the assessment** relating to the existence of fundamental rights and freedoms of the data subject which override the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, **necessitates a balancing of the opposing rights and interests concerned which depends on the individual circumstances of the particular case in question, where account must be taken of the significance of the data subject's rights arising from Articles 7 and 8 of the Charter.**

Relying on those arguments, the CJEU stated that Articles 8 and 52 of the Charter must not, in the present case, "be applied in isolation".

The CJEU stated that the criterion of the seriousness of the infringement of the data subject's rights and freedoms is an essential component of the weighing or balancing exercise on a case-by-case basis, required by Article 7(f) of Directive 95/46. In this respect, the CJEU recalled its previous case law (*Rīgas satiksme*, C 13/16, §28), affirming that in the assessment concerning the seriousness of the infringement of the data subject's fundamental rights resulting from that processing the following elements could be considered:

a) the availability of personal data at issue in public sources. The CJEU, relying on *ASNEF and FECEMD* (joined cases C-468/10 and 469/10), noted that there is a more serious infringement of the data subject's rights enshrined in Articles 7 and 8 of the Charter in case of processing of data from non-public sources, because that information relating to the data subject's private life will thereafter be known by the data controller and, as the case may be, by the third party or parties to whom the data are disclosed.

b) **the nature of the personal data** at issue, in particular of its potentially **sensitive nature,**

c) the **nature and specific methods of processing**

d) the **number of persons having access to data and the methods of accessing them**.

e) The **data subject's reasonable expectations** that his or her personal data will not be processed when, in the circumstance of the case, that person cannot reasonably expect further processing of those data.

The CJEU considered **those factors must be balanced against the importance of the legitimate interests pursued** in the instant case. In the present case by the video surveillance system at issue, inasmuch as it seeks essentially to ensure that the property, health and life of those co-owners are protected.

Conclusion of the Court

The Court concluded that Article 6(1)(c) and Article 7(f) of Directive 95/46/EC, read in light of Articles 7 and 8 of the CFREU, must be interpreted as not precluding national provisions which authorise the installation of a video surveillance system, installed in the common parts of a residential building, for the purposes of pursuing legitimate interests of ensuring the safety and protection of individuals and property, without the consent of the data subjects, if the processing of personal data carried out by means of the video surveillance system at issue fulfils the conditions laid down in Article 7(f), which it is for the referring court to determine.

Elements of judicial dialogue

- Horizontal judicial dialogue (within the CJEU):

- In ***ASNEF and FECEMD***, (C-468/10 and C-469/10), the CJEU stated that Article 7 of Directive 95/46 sets out an exhaustive and restrictive list of cases in which the processing of personal data can be regarded as being lawful, and that Member States cannot add new principles relating to the lawfulness of the processing of personal data or impose additional requirements that have the effect of amending the scope of one of the six principles laid down in that article. **Therefore, Article 7(f) of Directive 1995/46 precludes Member States from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case**. Thus, Member States cannot definitively prescribe, for certain categories of personal data, the result of the balancing of the opposing rights and interests, without allowing for a different result depending on the particular circumstances of an individual case.
- The CJEU in ***Breyer*** (C-582/2014) recalled *ASNEF and FECEMD*, (C-468/10 and C-469/10), and stated that Article 7(f) of dir 95/46 precludes Member States from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case.
- the CJEU in ***Rīgas satiksme***, (C-13/16, §30) stated that with regard to the condition relating to the **necessity of processing personal** data where the lawful basis for processing is the legitimate interest, **derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary**. Article 52 CDFUE is not expressly recalled, but the CJEU seems to implicitly rely on this provision, which states that "*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*". However, in that case the CJEU affirmed also that the result of **balancing** the opposing rights and interests at issue, depends in principle on the **specific circumstances of the particular case.**
- In ***Fashion ID*** (C-40/17) the CJEU, recalling *Rīgas satiksme*, (C-13/16, §30) stated that Article 7(f) of Directive 95/46 lays down three cumulative conditions for the processing of personal data to be lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; **second, the need to process personal data for the purposes of the legitimate interests pursued**; and third, the condition that the fundamental rights and freedoms of the data subject whose data require protection do not take precedence.
- in ***M.I.C.M*** (C-597/19) the Court, relying on recalling *Rīgas satiksme*, (C-13/16), affirmed that Article 6 (1) (f) Regulation EU 20165/679 lays down three cumulative conditions so that the processing of personal data is lawful, namely: first, the pursuit of a legitimate interest by the data controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the interests or freedoms and fundamental rights of the person concerned by the data protection do not take precedence.

With regard to the first condition, the Court stated that the interest of the controller or of a third party in obtaining the personal information of a person who allegedly damaged their property in order to sue that person for damages can be qualified as a legitimate interest. The Court affirmed that this interpretation is supported by Article 9(2)(e) and (f) of Regulation 2016/679, according to which the prohibition on the processing of certain types of personal data is not to apply, in particular, where the processing concerns personal data which is clearly rendered public by the person concerned or is necessary for the establishment, exercise or defence of legal claims.

As to the condition relating to the necessity of processing personal data for the purposes of the legitimate interests pursued, the Court, relying on its previous case law (*Rīgas satiksme*, C-13/16, §30) considered that derogations and limitations in relation to the protection of personal data must apply

only in so far as they are strictly necessary. Furthermore, the Court stated that the processing should be considered necessary where the identification of the owner of the internet connection is possible only on the basis of the IP address and the information provided by the Internet service provider. Moreover, the Court considered that the condition of balancing the opposing rights and interests at issue depends in principle on the specific circumstances of the particular case.

- In *VS v Inspektor* the referring Court asked the CJEU whether the expression 'legitimate interests' in Article 6(1)(f) of Regulation 2016/679 includes the disclosure, in whole or in part, of information concerning a person which has been collected in a public prosecution investigation file opened in relation to that person for the purposes of the prevention, investigation, detection or prosecution of criminal offences, in the case where that disclosure is carried out for the purposes of the defence of the controller as a party to civil proceedings.

- In *Facebook Inc. and Others v Bundeskartellamt,* (Case C-252/21), the referring court asked to the CJEU whether the undertaking, such as Facebook Ireland, which operates a digital social network funded by advertising and offers personalised content and advertising, network security, product improvement and continuous, seamless use of all of its group products in its terms of service, justify collecting data for these purposes from other group services and third-party websites and apps via integrated interfaces or via cookies or similar storage technologies placed on the internet user's computer or mobile device, linking those data with the user's Facebook.com account and using them, on the ground of necessity for the performance of the contract under Article 6(1)(b) of the GDPR or on the ground of the pursuit of legitimate interests under Article 6(1)(f) of the GDPR. Moreover, the referring court asked whether a list of interests may be considered legitimate under Article 6(1)(f) (i) the fact of users being underage, *vis-à-vis* the personalisation of content and advertising, product improvement, network security, and non-marketing communications with the user; ii) the provision of measurements, analytics, and other business services to enable advertisers, developers and other partners to evaluate and improve their services; iii) the provision of marketing communications to the user to enable the undertaking to improve its products and engage in direct marketing; iv) research and innovation for social good, to further the state of the art or the academic understanding of important social issues and to affect society and the world in a positive way; v) the sharing of information with law enforcement agencies and responding to legal requests in order to prevent, detect and prosecute criminal offences, unlawful use, breaches of the terms of service and policies and other harmful behaviour).

- In the pending cases *AB v Land Hesse* (C-64/22) and *UF v. Land Hessen* (C-26/22) the referring judge asked two questions related to the application of the legitimate interest as a legal basis for processing. In particular, the national court asked whether

o in so far as Article 6(1)(f) GDPR may be the sole legal basis for the storage of data at private credit information agencies with regard to data also stored in public registers, a credit information agency is already to be regarded as pursuing a legitimate interest where it imports data from the public register without a specific reason so that those data are then available in the event of a request

o It is permissible for codes of conduct which have been approved by the supervisory authorities in accordance with Article 40 GDPR, and which provide for time limits for review and erasure that exceed the retention periods for public registers, to suspend the balancing of interests prescribed under point (f) of Article 6(1) of the GDPR

The opinions of supervisory authorities

The Article 29 Working Party (WP29) adopted on 9 April 2014 the *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*. Although this opinion was not recalled by the CJEU in *Asociația de Proprietari* (C-708/18), it is important because it highlights that Directive 95/46 and now the GDPR provide several balancing tests in which the **proportionality principle** is involved. According to the WP 29, in applying the balancing test related to the comparison between the legitimate interest and the impact on the data subjects, the measures that the controller plans to adopt to comply with the Directive 95/46, such as the proportionality of processing must be taken into account.
Furthermore, the *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, adopted by the WP29 on 27 February 2014 shows the importance of the judicial dialogue between the ECtHR and the CJEU in the interpretation of data protection rules, and particularly with regard to the application of the proportionality principle (*Z v Finland*, Appl. No. 22009/93, 25 February 1997; *S & Marper v United Kingdom*, Appl. No. 30562/04 and 30566/04, 04 December 2008).

Impact on national case law in Member States other than the one of the court referring the preliminary question to the CJEU

Italy

In Italy, on several occasions Courts have interpreted the concept of "legitimate interest"; a group of cases concerns the possibility for heirs to access the personal data of the deceased that are processed by a data controller. In particular, the question arises in relation to personal data relating to the deceased that are necessary for heirs to exercise a right in court. In this regard, in its decision of 3 November 2020, the Tribunal of Marsala affirmed that the right to judicial defence is a legitimate interest under the GDPR, also considering that even Article 9 letter f - which also allows the processing of sensitive personal data in the absence of consent of the data controller allows the processing where it is "necessary for establishing, exercising or defending a right in court or whenever judicial authorities exercise their judicial function".

In the same manner, the Tribunal of Milan, in its decision of 10 November 2021, affirmed the prevalence of the right of access to justice and of exercising the rights before a Court on the rights and interests of the data subjects, interpreting the legal basis of legitimate interest in light of other provisions of the GDPR. In particular, the Court took into account the exception to the prohibition of processing provided for in Article 9 GDPR, also mentioned by the Tribunal of Marsala.

In this regard, the Court of Cassation, in its decision no. 39531 of 13 December 2021, although not expressly mentioning the legitimate interest as a legal basis for processing, affirmed that, "the interest in the confidentiality of personal data must yield, in the face of the protection of other legally relevant interests, and by the system configured as prevailing in the necessary balancing act, including the interest, if genuine, to the exercise of the right of defence in court."

Furthermore, the Tribunal of Milan, in its decision of 10 February 2021, considered that the parents of a deceased son can access the cloud account of the son, as they are entitled because of family reasons deserving of protection.

Moreover, concerning the protection of property as a legitimate interest, the Court of Cassino, in its decision of 26 June 2019, relying on *Ryneš* (C-212/13) stated that the protection of property may be a legitimate interest that justifies the processing. In particular, in the present case, a video surveillance system had been installed because of the passage on the property of third parties and some damage suffered. The Court stated that the processing is considered lawful if, according to the court, in the

specific case, there is a legitimate interest of the data controller in the protection of health, their own life, or that of their family, and private property.

4.1.2. Question 2: Consent of the data subject as a legitimate basis for processing

Relevant CJEU case

Within the following cluster of cases, the main case that is to be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

➢ Judgment of the Court (Grand Chamber) of 1 October 2019, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH, Case C-673/17, ("**Planet49**")

Cluster of cases

➢ Judgement of the Court the Oberlandesgericht Düsseldorf (Germany), lodged on 26 January 2017, *Fashion ID Gmbh & Co.KG* v. *Verbraucherzentrale NRW EV*, Case C-40/17 (***Fashion ID***)

➢ Judgment of the Court (Grand Chamber) of 1 October 2019, Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband eV v Planet49 GmbH, Case C-673/17, ("**Planet49**")

➢ Judgement of 11 November 2020*, Orange Romania SA v Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal*, Case C-61/19 ("***Orange Romania***")

➢ Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 20 July 2021 — **Maximilian Schrems v Facebook Ireland Ltd**, Case C-446/21 [pending]

➢ Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged on 22 April 2021 — **Facebook Inc. and Others v Bundeskartellamt** (Case C-252/21) [pending]

Main question addressed

In light of the principle of effectiveness and of Article 8 CFR, is data subject's consent valid if data processing is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent?

Relevant legal sources

EU Level
Directive 2002/58
Recital (17) ; (24); Article 1 "Scope and aim"; Article 2, Definitions; Article 5(3) Confidentiality of the communications
Directive 95/46
Article 1 "Object of the Directive"; Article 2, "Definitions"; Article 7;
Regulation 2016/679 (GDPR)
Recital 32; Article 4 (11), definition of consent; Article 6 "Lawfulness of processing"; Article 7(4) "Conditions for consent"; Article 94 "Repeal of Directive 95/46/EC".

The case

On 24 September 2013, Planet49 organised a promotional lottery on the website www.dein- macbook.de. Internet users wishing to take part in that lottery were required to enter their postcodes, which redirected them to a web page where they were required to enter their names and addresses.

Beneath the input fields for the address were two bodies of explanatory text accompanied by checkboxes. The first body of text with a checkbox without a preselected tick ('the first checkbox') read:
'I agree to certain sponsors and cooperation partners providing me with information by post or by telephone or by email/SMS about offers from their respective commercial sectors. I can determine these myself here; otherwise, the selection is made by the organiser. I can revoke this consent at any time. Further information about this can be found here.'
The second set of text with a checkbox containing a preselected tick ('the second checkbox') read:
'I agree to the web analytics service Remintrex being used for me. This has the consequence that, following registration for the lottery, the lottery organiser, [Planet49], sets cookies, which enables Planet49 to evaluate my surfing and use behaviour on websites of advertising partners and thus enables advertising by Remintrex that is based on my interests. I can delete the cookies at any time. You can read more about this here.'
Participation in the lottery was possible only if at least the first checkbox was ticked.
A consumer association (on the role of consumer associations in data protection see chapter 9) asserted that the declarations of consent requested by Planet49 through the first and second checkboxes did not satisfy the legal requirements and on this basis brought an action before the national court for an injunction.
The first instance court upheld the action in part. *Planet49* brought an appeal on points of fact and law; the appeal court stated that the Federation's plea for an injunction was unfounded because, first, the user would realise that they could deselect the tick in that checkbox and, second, the text was set out with sufficient clarity from a typographical point of view and provided information about the manner of the use of cookies without it being necessary to disclose the identity of third parties able to access the information collected.

Preliminary questions referred to the Court

The Federal Court of Justice of Germany, before which the consumer association brought an appeal, referred to the CJEU the following question, concerning the interpretation of Article 5(3) and Article 2(f) of Directive 2002/58, read in conjunction with Article 2(h) of Directive 95/46 and Article 6(1)(a) of Regulation 2016/679 and referred a question to the CJEU:
'(1) (a) Does it constitute a valid consent within the meaning of Article 5(3) and Article 2(f) of Directive [2002/58], read in conjunction with Article 2(h) of Directive [95/46], if the storage of information, or access to information already stored in the user's terminal equipment, is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent?
(…)
(c) In the circumstances referred to in Question 1(a), does a valid consent within the meaning of Article 6(1)(a) of Regulation [2016/679] exist?
(…)"

Reasoning of the Court

The Court decided the case both on the basis of Directive 95/46 and Regulation UE 2016/679.
The CJEU interpreted the wording "given his or her consent" of Article 5 Directive 2002/58 in light of Directive 95/46, which defined "the data subject's consent" as being "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". The CJEU also considered that Article 7(a) of Directive 95/46 stated that the data subject's consent must be "unambiguously" given.
Therefore, the CJEU stated that **the requirement of an "indication" of the data subject's wishes clearly points to active, rather than passive, behaviour**.

The CJEU stated that this interpretation of Article 5(3) of Directive 2002/58 is confirmed by the GDPR, because of the wording of Article 4(11) thereof, which defines the "data subject's consent" as a "freely given, specific, informed and unambiguous" indication of the data subject's wishes in the form of a statement or of "clear affirmative action" signifying agreement to the processing of the personal data relating to them.
The CJEU considered that active consent is thus now expressly laid down in **Regulation 2016/679**. It should be noted in that regard that, according to **recital 32** thereof, giving consent could include ticking a box when visiting an internet website. On the other hand, that recital expressly precludes 'silence, pre-ticked boxes or inactivity' from constituting consent.
The CJEU did not expressly rely on the general principles of EU law and only mentioned fundamental rights. Nevertheless, the CJEU's decision could be read in light of the **principle of effectiveness**, read in conjunction with Article 8 CFR, the latter being interpreted as aimed at balancing the asymmetry of powers between the data subject and the data controller. Data subject's consent is an important lawful basis for processing, considering that through consent the data subject authorises the processing beyond the processing which is permitted by the law. Therefore, in order to grant the effectiveness of Article 8(2) CFREU it is crucial to interpret EU law fostering data subjects' awareness, with the aim of granting the possibility of a free choice of the data subject.

Conclusion of the Court

Article 2(f) and of Article 5(3) of Directive 2002/58/EC, read in conjunction with Article 2(h) of Directive 95/46/EC and Article 4(11) and Article 6(1)(a) of Regulation (EU) 2016/679 (GDPR), must be interpreted as meaning that the **consent** referred to in those provisions **is not validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent**.

Elements of judicial dialogue

- **Horizontal dialogue (within the CJEU)**

In *Fashion ID* (C-40/17), the **efficient protection of the data subject's rights** is at the core of the CJEU's reasoning with regard to consent as a legitimate basis for processing (in other language versions of the judgement, such as the Italian one, the wording directly uses to "effective" protection). In the case there were two data controllers for the processing of personal data through a social plug-in installed on a website: the operator of the website and the provider of the social plugin. The CJEU considered, relying on Article 2(h) and 7(a) of Detective 95/46 that data subject's consent must be given prior to the collection and disclosure by transmission of the data subject's data. Then, the CJEU stated that it is for the operator of the website, rather than for the provider of the social plugin, to obtain the data subject's consent, since it is the fact that the visitor consults that website that triggers the processing of the personal data.
The CJEU affirmed that it would not be in line with efficient and timely protection of the data subject's rights if the consent were given only to the joint controller that is involved later, namely the provider of that plugin. However, the consent that must be given to the operator relates only to the operation or set of operations involving the processing of personal data in respect of which the operator actually determines the purposes and means.
In ***Orange Romania*** **(C-61/19),** a Romanian court asked what conditions must be fulfilled for an indication of wishes to be regarded as specific and informed and as freely given for the purposes of Article 2(h) of Directive 95/46/EC. The Court stated that according to Article 2(h) and Article 7(a) of Directive 95/46/EC and Article 4(11) and Article 6(1)(a) Regulation EU 2016/679 it is for the data controller to demonstrate that the data subject has given his or her valid consent to the processing of his

or her personal data. Furthermore, the Court interpreted the requirements for a valid consent (specific, informed, freely given, manifested with an active behaviour) in order to grant the data subject the possibility to make an **effective choice** concerning the processing of personal data concerning them.
According to the Court a contract for the provision of telecommunications services which contains a clause stating that the data subject has been informed of, and has consented to, the collection and storage of a copy of his or her identity document for identification purposes is not such as to demonstrate that that person has validly given his or her consent, as provided for in those provisions, to that collection and storage, where:
iii) the box referring to that clause has been ticked by the data controller before the contract was signed, or where (in that case there would be a lack of an unambiguous indication of the data subject's wishes by which they expressed by a statement or by a clear affirmative action)
ii) the terms of that contract are capable of misleading the data subject as to the possibility of concluding the contract in question even if they refuse to consent to the processing of their data, (in that case consent would not be free neither informed)
iii) the freedom to choose to object to that collection and storage is unduly affected by that controller, in requiring that the data subject, in order to refuse consent, must complete an additional form setting out that refusal (in that case consent would not be free consent is not free).

In the pending case **Schrems IV** (C-446/21), the referring court assessed the issue of the relationship between data subject consent as a legal basis for processing and the legal basis provided for by Article 6(1) (b) (the 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). In particular, the referring Court asked the CJEU if the lawfulness of contractual provisions in general terms of service for platform agreements which provides the processing of personal data with a view to aggregating and analysing it for the purposes of 111ersonalized advertising, must be assessed in accordance with the requirements of Article 6(1)(a) of the GDPR, read in conjunction with Article 7 thereof, which cannot be replaced by invoking Article 6(1)(b) thereof.

In the pending case **Facebook Inc. and Others** (C-252/21) the referring court asked the CJEU whether consent, within the meaning of Article 6(1)(a) and Article 9(2)(a) of the GDPR, can be given effectively and, in accordance with Article 4(11) of the GDPR in particular, freely, to a dominant undertaking such as Facebook Ireland.

The opinions of supervisory authorities

The Working Party Article 29 adopted on 28 November 2017 the *Guidelines on consent under Regulation 2016/679*, that were endorsed by the European Data Protection Board (EDPB) with the Endorsement 1/2018. Although in the English version of the Opinion the principle of effectiveness is not mentioned (in the Italian version is used with regard to an "effective choice" of the data subject)
The WP 29 affirmed that:
"consent can only be an appropriate **lawful basis if a data subject is offered control and is offered a genuine choice with regard to accepting or declining the terms offered or declining them without detriment**. When asking for consent, a controller has the duty to assess whether it will meet all the requirements to obtain valid consent. If obtained in full compliance with the GDPR, consent is a tool that gives data subjects control over whether or not personal data concerning them will be processed. If not, the data subject's control becomes illusory and consent will be an invalid basis for processing, rendering the processing activity unlawful".
Specific guidelines are provided in order to ensure that the given consent is specific, informed, free, and explicit.

Furthermore, on 4 May 2020, the EDPB adopted new guidelines (No 5) on consent. According to that guidelines "**Free and freely given consent" means that data subjects can make "real" choice and control.**

In particular, the EDPB stated that:
"If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment (…). The GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract".
Moreover, the EDPB highlighted that, by reason of the wording of Article 7(4) GDPR and of recital 43 thereof, where the data are not necessary for the performance of the contract, (including the provision of a service), and the performance of that contract is made conditional on the obtaining of these data on the basis of consent, the conditionality would not render the consent invalid only in highly exceptional cases.
Furthermore, the EDPB recalled that the burden of proof concerning the existence of a free consent lies on the controller and that this rule is a concretisation of the general principle of accountability. According to the EDPB, in order to prove that the consent is free and freely given, the controller could argue that his organisation offers data subjects genuine choice if they were able to choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by the same controller that does not involve consenting to data use for additional purposes on the other hand.
According to the EDPB, another important element for the assessment concerning the existence of a free consent are the granularity of consent (the possibility of consent or not separately to each purpose for processing and data processing operation).
Furthermore, the EDPB provided guidelines concerning the meaning of the "specific" and informed consent, based on "unambiguous indication of wishes". With regard to the latter requirement, the EDPB stated that:
"The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice. (…) A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data. The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example 'opt-out boxes')".

Impact on national case law in Member States other than the one of the court referring the preliminary question to the CJEU

Italy
Italian courts have not yet referred to *Planet49* (C-673/17). Nevertheless, it is interesting to look to Italian case law and administrative decisions concerning data subject's consent. An important group of decisions concerns the freedom of the consent.
In that regard, the Italian Data Protection Authority have adopted a restrictive position, considering that consent cannot be qualified as freely given when the providing of a service is subordinate to data subject's consent (GPDP, 1° October 2015, n. 4611905; GPDP, 11 June 2015, n. 4243173; GPDP, 18 December 2014, n. 3750400; GPDP, *Linee guida in materia di attività promozionale e contrasto allo spam,* 4 July 2013, n. 2542348; GPDP, 10 January 2019, n. 9080914) or when there is a pre-checked checkbox which the user must deselect to refuse his or her consent (GPDP, 1° October 2015, n. 4611905; GPDP, 5 March 2015, n. 4203055; GPDP, 11 June 2015, n. 4243173; GPDP, 18 December 2014, n. 3750400; GPDP, *Linee guida*

in materia di attività promozionale e contrasto allo spam, 4 luglio 2013, n. 2542348; GPDP, 22 February 2007, n. 1388590; GPDP, 12 October 2015, n. 1179604; GPDP, 3 November 2005, n. 1195215; GPDP, 15 July 2010, n. 1741998; GPDP, 10 January 2019, n. 9080914).

Furthermore, in the judgment of 2 July 2018, n. 17278, the Court of Cassation affirmed that the consent could considered freely given also in some cases in which a service is provided only if the data subject expresses the consent to processing. In this regard, the Court stated that in order to decide if the consent is freely given it is important to consider if the service is non-fungible and essential.

Moreover, a recent judgement of the Italian Court of Cassation (of 21 October 2019, No. 26778), concerning a contractual relationship between a client and a bank, is of particular interest. In that case, the client signed a clause according to which, in the absence of consent to the processing of sensitive data, the bank would not be able to carry out the operations and services requested. The Court of Cassation, in the above mentioned case, affirmed the voidness of the clause because it is considered contrary to imperative provisions of data protection law.

As to the meaning of "informed consent" the Court of Cassation, in its decision no. 14381 of 25 May 2021, stated that consent to processing is valid only if it is freely and specifically expressed with reference to a clearly identified processing operation; it follows that in the case of a web platform (with annexed computer archives) designed to process the reputation profiles of individual physical or legal persons, based on a calculation system based on an algorithm aimed at establishing reliability scores, the requirement of "informed consent" cannot be considered satisfied if the executive scheme of the algorithm and the elements of which it is composed remain unknown or cannot be known by the data subjects.

France

Various decisions of the French Data Protection Authorities (*Commission nationale de l'informatique et des libertés*; hereinafter: CNIL) are of particular interest. For example, the decision of 30 October 2018 2018-042, concerning the lawfulness of the data processing implemented by a company which uses technologies that allows personal data to be collected via multifunction mobiles and to carry out advertising campaigns on mobiles. This company uses technical tools which allow the company to collect data from users of multifunction mobile phones even when these applications are not running. The advertising ID of the MFPs and the geolocation data of the people are collected. This data is then cross-referenced with points of interest determined by partners (store chains) to display targeted advertising on people's devices from the places they have visited. The company also processes, for the purposes of profiling and advertising targeting, geolocation data that it receives via real-time auction offers initially transmitted for the purpose of enabling the company to purchase advertising space. The company indicates that it processes this data with the consent of the persons concerned. **The CNIL stated that there was lack of consent to the processing of geolocation data for the purposes of advertising targeting**. *Inter alia*, the CNIL stated that the information given to the user does not explain that their data will be used for this real-time auction system, nor that it will then be stored for the purpose of defining a commercial profile (For more information on the decision, see the FRICORE Database, at this link).

Another important decision of the CNIL is the one of 21 January 2019 2019-001. In that case, the CNIL was seized for two collective complaints submitted in accordance with Article 80 of the GDPR, from associations who criticised Google for not having a valid legal basis for processing the personal data of the users of its services, in particular for the purposes of advertising personalisation.

On the basis of the investigations carried out, the CNIL found Google's failure to have a legal basis for the personalisation processing of advertising. Google relies on users' consent to process their data for the purpose of personalising advertising. **However, the CNIL stated that that consent is not validly collected for two reasons. First, user consent is not sufficiently informed.** The information on such processing, diluted in several documents, does not allow the user to be aware of the extent of the

processing. **Second, the consent collected is not "specific" and "unambiguous".** On the breach of the obligation to have a legal basis for the processing implemented, the CNIL considers that the consent on which the company bases personalised advertising processing is not validly obtained as provided for in Article 6 of the GDPR. The CNIL pronounced a financial penalty of 50 million euros against the company Google LLC in application of the GDPR for lack of transparency, unsatisfactory information and lack of valid consent for the personalisation of advertising. (For more information on the decision, see the FRICORE Database, at this link).

4.1.3. Question 3: Fundamental rights and legitimate basis for processing

Within the following cluster of cases, the main case that is to be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

➢ Judgment of the Court (Grand Chamber), 29 January 2008, *Productores de Música de España (Promusicae)* v. *Telefónica de España SAU*, Case C-275/06 (***Promusicae***)

Cluster of relevant CJEU cases

➢ Judgment of the Court, 6 November 2003, *Bodil Lindqvist*, Case C-101/01 (***Lindqvist***)

➢ Judgment of the Court (Grand Chamber), 29 January 2008, *Productores de Música de España (Promusicae)* v. *Telefónica de España SAU*, Case C-275/06 (***Promusicae***)

➢ Judgment of the Court (Grand Chamber), 9 November 2010, Volker und Markus Schecke GbR & Hartmut Eifert v Land Hessen, Joined cases C-92/09 & C-93/09 (***Volker***)

➢ Judgment of the Court (Third Chamber), 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF), Federación de Comercio Electrónico y Marketing Directo (FECEMD)* v. *Administración del Estado*, Joined cases C-468/10 and C-469/10 (***ASNEF and FECEMD***)

➢ Judgment of the Court (Third Chamber), 24 November 2011, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Case C-70/10 (***Scarlet Extended***)

➢ 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***)

➢ Judgment of the Court (Fourth Chamber), 11 December 2014, *František Ryneš* v. *Úřad pro ochranu osobních údajů*, Case C-212/13 (***Ryneš***)

➢ Judgment of the court (Second Chamber), 19 October 2016, *Patrick Breyer* v. *Bundesrepublik Deutschland, Case C-582/14* (***Breyer***)

➢ Judgment of the Court (Second Chamber), 9 March 2017, *Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce* v *Manni*, Case C-398/15 (***Manni***)

➢ Judgment of the Court (Second Chamber), 4 May 2017, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde* v. *Rīgas pašvaldības SIA 'Rīgas satiksme'*, Case C-13/16 (***Rīgas satiksme***).

➢ Judgement of the Court the Oberlandesgericht Düsseldorf (Germany), lodged on 26 January 2017, *Fashion ID Gmbh & Co.KG* v. *Verbraucherzentrale NRW EV*, Case C-40/17 (***Fashion ID***)

➢ Judgment of the Court (Third Chamber) of 11 December 2019. TK v Asociația de Proprietari bloc M5A-ScaraA (***Asociația de Proprietari***), C-708/18

Main question addressed:

In light of the principle of effectiveness and proportionality, can an individual, relying on the right to an effective remedy (Article 47 CFR) for the protection of a fundamental right (e.g., the right to intellectual property), require that a data controller gives her access to that personal data which are necessary for exercising that fundamental right?

Relevant legal sources:

EU Level

Charter of Fundamental Fights of the EU

Article 7 (right to protection of private life), article 8 (right to protection of personal data), article 52 (scope of guaranteed rights, quoted above)

Directive 95/46 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

Article 7 – Criteria for making data processing legitimate; Article 8 (1) and (2) The processing of special categories of data; Article 13(1) Exemptions and restrictions

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

Recital 2; Article 5 (1) Confidentiality of the communications; *Article 6 (1) Traffic data*; *Article 15(1), Application of certain provisions of Directive 95/46/EC*

The case(s):

Promusicae is a non-profit-making organisation of producers and publishers of musical and audiovisual recordings. In 2005, it made an application to the *Juzgado de lo Mercantil No 5 de Madrid* (Commercial Court No 5, Madrid) for preliminary measures against Telefónica, a commercial company whose activities include the provision of internet access services. Promusicae contended that some of Telefónica's clients used a peer-to-peer programme to share access to phonograms in which the members of Promusicae held the exploitation rights and was seeking an injunction against Telefónica to disclose the identities and physical addresses of certain clients. Disclosure of this information was meant to enable Promusicae to bring civil proceedings against the persons concerned. By order of 21 December 2005 the *Juzgado de lo Mercantil No 5 de Madrid* ordered the preliminary measures requested by Promusicae.

Telefónica appealed against that order, contending that under the LSSI the communication of the data sought by Promusicae was authorised only in a criminal investigation or for the purpose of safeguarding public security and national defence, not in civil proceedings or as a preliminary measure relating to civil proceedings. Promusicae relied, notably, on articles 17(2) and 47 of the Charter protecting the right to intellectual property and the right to effective justice. The *Juzgado de lo Mercantil No 5 de Madrid* decided to stay the proceedings and refer a question to the Court for a preliminary ruling.

Preliminary ruling referred to the Court:

"Does Community law, specifically [the directives listed above] and Articles 17(2) and 47 of the Charter (…) permit Member States to limit to the context of a criminal investigation or to safeguard public security and national defence, thus excluding civil proceedings, the duty of operators of electronic communications networks and services, providers of access to telecommunications networks and providers of data storage services to retain and make available connection and traffic data generated by the communications established during the supply of an information society service?"

Reasoning of the Court:

On the question whether Directive 2002/58 precludes the Member States from laying down an obligation for operators of electronic communications networks to communicate personal data for the purpose of the protection of intellectual property rights, the Court answers in the negative.

After recalling that under the directive's provisions, Member States may adopt legislative measures to restrict the scope of the obligation to ensure the confidentiality of data traffic, where *such a 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 communications system, the Court observes that none of these exceptions appears to relate to situations that call for the bringing of civil proceedings. However, the Court considers that it is clear that Article 15(1) of Directive 2002/58 ends the list of the above exceptions with an express reference to Article 13(1) of Directive 95/46. That provision also authorises Member States to adopt legislative measures to restrict the obligation of confidentiality of personal data where that restriction is necessary *inter alia* for the protection of the rights and freedoms of others. As they do not specify the rights and freedoms concerned, those provisions of Article 15(1) of Directive 2002/58 must be interpreted as expressing the Community legislature's intention not to exclude from their scope the protection of the right to property or situations in which authors seek to obtain that protection in civil proceedings.

On the question whether EU law requires the Member States to lay down the disputed obligation, the Court briefly examines the impact of IP directives, on which it concludes that they do not impose such a requirement, before evaluating **the impact of fundamental rights enshrined in articles 17(2) and 47 of the Charter** more substantially.

Does an interpretation of the IP directives to the effect that Member States are not obliged, in order to ensure the effective protection of copyright, to lay down an obligation to communicate personal data in the context of civil proceedings, lead to an infringement of the fundamental right to property and the fundamental right to effective judicial protection?

To answer the question, the Court recalls that the fundamental right to property and the fundamental right to effective judicial protection constitute general principles of Community law. However, in the situation referred by the national court, another further fundamental right, namely the right that guarantees protection of personal data and hence of private life, is at stake, since Directive 2002/58 seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter, also protected under Article 8 ECHR). It is thus necessary to reconcile the requirements of the protection of those different (and in this case conflicting) fundamental rights. To achieve this reconciliation, *the Member States must, when transposing the directives, take care to rely on an interpretation of the directives that 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 that would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality*.

In other terms, the Court urges the Member States to transpose and implement directives so as to avoid any conflict of fundamental rights. If such conflict cannot be avoided, in the view of the Court, Member States should rely on general principles of the EU, **in particular the principle of proportionality**, to reach a balanced solution that will not unduly sacrifice **the effective protection of one fundamental right for the protection of another** (**principle of effectiveness**).

To define the relevant elements to put in the balance, the decision is to be read in light of the CJEU decisions in *Lindqvist*, *ASNEF* and *FECEMD, Google Spain* and *Rigas Satiksme*.

In ***Lindqvist***, the Court concludes that *when conducting that balancing process, a national court should take account, in accordance with the principle of proportionality, of all the circumstances of the case before it, in particular the*

duration of the breach of data protection and the importance, for the persons concerned, of the protection of the data disclosed.
In ***ASNEF and FECEMD***, the Court judges that in relation to the balancing of interests, it is possible to take into consideration the fact that the data in question already appears in public sources.
In ***Google Spain***, the Court states that the assessment *may depend on the nature of the information in question and its sensitivity for the data subject's private life and the fact that its initial publication had taken place 16 years previously, balanced with the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life* (See Chapters 5 and 8).
In ***Rigas Satiksme***, the Court considers that, while the age of the data subject may be one of the factors which should be taken into account in the context of that balance of interests, it does not appear to be justified to refuse to disclose to an injured party the personal data necessary for bringing an action for damages against the person who caused the harm, on the sole ground that that person was a minor.
The decision is also to be read in light of ***ASNEF and FECEMD*** and ***Breyer*** (see below), in which the Court judges that the Member States cannot add new principles relating to the lawfulness of the processing of personal data or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in Article 7 of Directive 95/46. Concerning in particular Article 7(f) of the Directive, only two cumulative conditions are set out for the lawfulness of the processing of data, which are: (1) that the processing of the personal data must be necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed; and, (2) that such interests must not be overridden by the fundamental rights and freedoms of the data subject. Thus, Member States are precluded from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case.

Conclusion of the Court:

Directives 2000/31, 2001/29, 2004/48 (IP) and 2002/58 (data protection) do not require Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings.
However, Community law requires that, the authorities and courts of Member States must make sure that they do not rely on an interpretation of data protection law which would be in conflict with fundamental rights or with the other general principles of Community law, such as the principle of proportionality.

Impact on the follow-up case:

The Commercial Court n° 5 of Madrid in its decision of 17 March 2008, mentioning the CJEU judgement, upheld Telefonica's opposition to Promusicae's request. Relying on national legislation applicable to the proceedings (*Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*, Article 12; *Ley de Protección de Datos de Carácter Personal*, Article 11; *Ley de Competencia Desleal*, Article 29), the Court stated that connection and traffic data generated by the communications established during the supply of an information society service may be used only in the course of criminal investigations or for safeguarding public security and national defence or other cases permitted by law. Data processing is not permitted by national law for bringing civil proceedings for unfair competition or infringement of intellectual property rights.

Elements of judicial dialogue:

- **Horizontal (within the CJEU):**

- In ***Scarlet Extended***, the Court builds on its analysis in *Promusicae* to decide whether it is possible for a national court to make an order, on the request of a management company representing authors of musical works, against an internet service provider for the installation of a filtering system

and for measures to be taken against its customers violating copyright. The Court reaches the conclusion that such an injunction would infringe the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other. But the decision is mainly motivated on the basis of freedom to conduct a business, not on the right to protection of data.

- In ***Ryneš***, the Court, after concluding that video surveillance covering even partial public space is not a 'purely personal or household activity' and thus falls under the regime of data protection (see Chapter 1, question 1), notes that EU law makes it possible to take account of legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself, as in the referred case. The court draws no direct conclusion from this finding; it simply answers the question asked (is the activity in question covered by one of the admitted derogations to data protection?). However, in light of *Promusicae*, it is clear that the Court is inviting national authorities to follow the methodology described above, in order to balance the right to data protection and privacy with the legitimate interest of the controller to protect his home and family.
- In ***Breyer*****,** the Court complements the reasoning in *Promusicae*, by answering the question whether Article 7(f) of Directive 95/46 precludes a provision in national law whereby a service provider may collect and use a user's personal data without his consent only to the extent necessary in order to facilitate, and charge for, the specific use of the tele-medium by the user concerned, and under which the purpose of ensuring the general operability of the tele-medium cannot justify use of the data beyond that of the particular use of the tele-medium.
- In ***Manni***, the Court observes that the purpose of the disclosure of personal data in the companies' register (provided for by Directive 68/151) is in particular to protect the interests of third parties in relation to joint stock companies and limited liability companies, since the only safeguards they offer to third parties are their assets, and to guarantee legal certainty in relation to dealings between companies and third parties in view of the intensification of trade between Member States following the creation of the internal market. The Court observes moreover that, for several reasons, it is absolutely necessary to access data concerning a company long after its dissolution. For this reason, Member States cannot guarantee the natural persons referred to in Directive 68/151 the right, as a matter of principle, a given length of time after the dissolution of the company concerned, to the erasure of personal data concerning them that have been entered in the register pursuant to the latter provision, or the blocking of that data from public access. Such situation does not result in disproportionate interference with the fundamental rights of the persons concerned, and particularly their right to respect for private life and their right to protection of personal data as guaranteed by Articles 7 and 8 of the Charter, because the disclosure concerns only a limited amount of data, because other legitimate interests are at stake, and because persons engaging in such activity are aware of these requirements. National courts must engage in a case-by-case analysis to decide if, exceptionally, it is justified, on compelling legitimate grounds relating to their particular situation, to limit, after a sufficiently long period has expired since the dissolution of the company concerned, access to personal data in that register relating to the natural person referred to in Directive 68/151, by third parties who can demonstrate a specific interest in consulting that data.
- In ***Rigas Satiksme*****,** the Court follows the same reasoning as in *Promusicae*, to which it expressly refers. Firstly, Article 7(f) of Directive 95/46 does not impose the obligation to disclose personal data to a third party in order to enable them to bring an action for damages before a civil court for harm caused by the person concerned by the protection of that data. However, Article 7(f) of that directive does not preclude such disclosure on the basis of national law, and national courts should decide whether disclosure is to be ordered after balancing the conflicting interests, following the methodology described above.
- In ***M.I.C.M*** (C-597/19) the Court, in what regards the balance of interests, considered that in order for processing, such as the registration of IP addresses of persons whose Internet connections have been used to upload pieces of files containing protected works on peer-to-peer networks, for the

purposes of filing a request for disclosure of the names and postal addresses of the holders of those IP addresses, can be regarded as lawful by satisfying the conditions laid down by Regulation 2016/679, it is necessary, in particular, to ascertain whether that processing satisfies the above mentioned provisions of Directive 2002/58, which embodies, for users of electronic communications, the fundamental rights to respect for private life and the protection of personal data. Accordingly, in its conclusions the Court stated that Point (f) of subparagraph 1 of Article 6(1) of Regulation (EU) 2016/679, read in conjunction with Article 15(1) of Directive 2002/58/EC (Directive on privacy and electronic communications), as does not preclude in principle, neither the systematic recording, by the holder of intellectual property rights as well as by a third party on his or her behalf, of IP addresses of users of peer-to-peer networks whose Internet connections have allegedly been used in infringing activities, nor the communication of the names and of the postal addresses of those users to that right-holder or to a third party in order to enable it to bring a claim for damages before a civil court for prejudice allegedly caused by those users, provided, however, that the initiatives and requests to that effect of that right-holder or of such a third party are justified, proportionate and not abusive and have their legal basis in a national legislative measure, within the meaning of Article 15(1) of Directive 2002/58, which limits the scope of the rules laid down in Articles 5 and 6 of that directive.

Impact on national case law in Member States different from the state of the court referring the preliminary question to the CJEU:

Italy

Promusicae had an impact on Italian judgements concerning similar cases. The Court of Rome (decision of 19 March 2008, No 26121), relying on *Promusicae* and on the principle of proportionality, affirmed that is for national judges to balance the protection of intellectual property and the right to data protection. Interpreting national rules applicable to the case (mainly Articles 4, 24, 132, 123 of the code concerning privacy and data protection, d.lgs. 196/2003, which was largely amended by reason of the GDPR), the court stated that the Italian legislator limited the exception to the general prohibition to retention of traffic data to criminal cases, and that this choice was compatible with European law, as interpreted by the CJEU. Accordingly, the Court of Rome rejected access requests to user data grounded on the protection of intellectual property. The same conclusion and a similar reasoning was adopted by the Court of Rome in its decisions of 22 November 2017 No 39349, and No 39355, where the conclusions of AG Kokott in *Promusicae* were mentioned.

4.2. Guidelines emerging from the analysis

The CJEU addressed the cases related to lawful basis for processing — namely the ones concerning the legitimate interest of the data controller or of a third party and the data subject's consent — in light of Article 8 CFREU and other fundamental rights.

Fundamental rights and legal basis for processing

With regard to the balance between the right to data protection on the one hand and on the other hand intellectual property rights and the right to conduct a business, within the scope of application of Directive 2002/58, according to the CJEU,

- the right to (intellectual) property (Article 17 CFR) and its enforceability (Article 47 CFR) do not require Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings (*Promusicae,* C-275/06).
- In light of the right to conduct a business and the right to data protection an injunction made against an internet service provider which requires it to install is precluded as a preventive measure for an unlimited period of time, a system for filtering all electronic communications passing via its services,

which applies indiscriminately to all its customers, exclusively at its expense, which is capable of identifying on that provider's network the movement of electronic files containing a musical, cinematographic or audio-visual work (*Scarlet Extended,* C-70/10)

- the systematic recording, by the holder of intellectual property rights as well as by a third party on their behalf, of IP addresses of users of peer-to-peer networks whose Internet connections have allegedly been used in infringing activities, and the communication of the names and of the postal addresses of those users to that right-holder or to a third party in order to enable it to bring a claim for damages before a civil court for prejudice allegedly caused by those users are not prohibited under Article 6(1)(f) GDPR, read in light of Directive 2002/58, where the initiatives and requests of that right-holder or of the third party are justified, proportionate and not abusive and have their legal basis in a national legislative measure, within the meaning of Article 15(1) of Directive 2002/58, which limits the scope of the rules laid down in Articles 5 and 6 of that directive (*M.I.C.M.,* C-597/19).

In that regard, the following question arises:

Within the framework of the GDPR, where the data controller can communicate personal data to a third party on the basis of its legitimate interest (e.g. the development of a specific medical device), a third party asks access to personal data and their access to personal data is essential for ensuring the protection of her fundamental right (e.g. right to health), could Article 47 CFREU play a role, granting the third party's access to data?

Legitimate interest as a legal basis for processing

In order to lawfully process personal data relying on the legal basis of the legitimate interest, three cumulative conditions should be met:

1) the pursuit of a present and effective legitimate interest by the data controller or by the third party or parties to whom the data are disclosed.

2) the need to process personal data for the purposes of the legitimate interests pursued. The necessity concept should be interpreted strictly (*Rīgas satiksme*, C-13/16, §30), and national courts should consider if the legitimate interest pursued through the processing cannot reasonably be as effectively achieved by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 CFR.

3) the fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interest pursued. The seriousness of the infringement of the data subject's rights and freedoms is an essential component of the balancing exercise on a case-by-case basis (*Rīgas satiksme*, C-13/16, §28). In that assessment the following elements could be considered (*Asociația de Proprietari* C-708/18):

a) the availability of personal data at issue in public sources.

b) the nature of the personal data at issue, in particular of its potentially sensitive nature, of the nature and specific methods of processing and of the number of persons having access to those data and the methods of accessing them.

c) The data subject's reasonable expectations.

The principle of **proportionality** is recalled in the CJEU case law, at least in two different ways: a) as an element of the evaluation of the necessity of the processing for the purposes of the legitimate, b) as a principle which has to be applied in case of limitation of the fundamental rights set forth in the Charter (Article 52 CFR). The relationship between the principle of proportionality of processing and Article 52 CFREU with regard to the proportionality of limitations to the exercise of the right to data protection could be object of future CJEU's judgements.

Data subject consent as a legal basis for processing

Data subject's consent is not validly constituted as a lawful basis for processing if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent (*Planet49*, C-673/17).

Moreover, in light of the effectiveness of Article 8 CFREU the regulation of data subject's consent should be interpret with the objective of ensuring a genuine choice of the data subject. In this respect, according to *Orange Romania* (C-61/19), under Regulation EU 2016/679 it is for the data controller to demonstrate that the data subject has given a valid consent to the processing.

5. Privacy vs. freedom of expression — the fundamental rights perspective

5.1. Introduction

The data protection framework in EU law does not directly address the problems concerning freedom of expression and other issues to public discourse. Nonetheless, both the 95/46 Directive, as well as GDPR, are involved in numerous interactions with "speech acts" understood in broad sense — as every manifestation of individual opinions and convictions, addressed to a defined or non-defined audience. The data protection rules may both enhance and (more frequently in practice) constrain the ways available for individuals to communicate their views.

For these reasons the rights to data protection (Article 8 CFR) and to private life (Article 7 CFR) may be in conflict with freedom of expression and freedom of information, framed as "freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers", both protected by Article 11CFR.

The issues discussed in this chapter are particularly important in an online context, especially with regard to social media platforms (such as Facebook and Twitter). They provide one of the most vibrant and intense fora for their member to voice social, political, cultural and other attitudes, providing a possibility to address audiences of unprecedented scope. At the same time, platforms of this kind are massive collectors of personal data and base their business model of aggregation, processing and trading vast pools of information about individual users. In this way the operation of platforms creates substantial concerns for both freedom of expression and data/privacy protection. Both domains are mutual flip sides and collide in numerous regards. Protection of speech liberty in many regards intervenes into the spheres relevant for privacy and data protection (such as including data into journalist materials and archiving information in a publicly-available databases). At the same time, data/privacy protection instruments may lead to removal of particular speech acts from the public sphere or to limit the array of the allowed means of expression.

The existing CJEU case law provides points of reference for better understanding of the interplay between freedom of speech and data/privacy concerns, as envisaged in the EU legal order. The following parts of this chapter attempt to unpack this approach and to provide more precise understanding of how the CJEU resolves the conundrum of values and rules involved in the privacy/data protection and liberty in expressing one's views. It must, however, be borne in mind that the sphere of these interactions still produces more vagueness than resolutions that are at stake in the European rules and case law. It creates a particularly meaningful task for domestic legal orders and the Member States' judiciary. They are included in the foreground of reconciling data protection and freedom of speech. In this task they should be guided by EU law (including the relevant Charter provisions), CJEU decisions, and constitutional traditions.

Main questions addressed:

1. a) What is the role of social media platforms (e.g., Facebook and Twitter) in balancing the freedom of expression with other fundamental rights? To what extent does Article 47 influence the scope and enforcement of their duties in that regard?

b) How does domestic case law approach the intersection of freedom of expression (freedom of speech) and privacy? How is this balance affected by the Charter and most particularly by Article 47, read together with Articles 7, 8, 11?

2. What is the role of public-purpose reveal of data (especially by journalists) on the general standard of privacy protection? To what extent does Article 47 influence the scope and enforcement of this standard?

Cluster of relevant CJEU cases

➢ Judgment of the Court (Grand Chamber) of 6 October 2015, *Maximillian Schrems v Data Protection Commissioner*, Case C-362/14 (***Schrems I***)

➢ Judgment of the Court (Third Chamber) of 3 October 2019, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, Case C-18/18 (***Glawischnig-Piesczek***)

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17 (***Google***)

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *GC, AF, BH, ED v. Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17 (***GC and others***)

➢ Judgment of the Court (Grand Chamber), 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, C-311/18 (***Facebook Ireland and Schrems***)

Relevant legal sources:

EU Level

Charter of Fundamental Rights of the EU:

Article 6 (right to security of the person), Article 7 (right to private life), Article 8 (right to the protection of data), Article 47 (right to an effective remedy and to a fair trial) and Article 52 (scope of guaranteed rights).

Directive 95/46 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 (*no longer in force*)

Article 3 – Scope; Article 7; Article 8 – The processing of special categories of data; Article 9 – Processing of personal data and freedom of expression; Article 12 - Right of access

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)

Article 17 – Right to erasure ('right to be forgotten'); Article 80 – Representation of data subjects

5.1.1. Question 1: Social media platforms and freedom of expression

a) What is the role of social media platforms (e.g., Facebook and Twitter) in balancing the freedom of expression with other fundamental rights? To what extent does Article 47 influence the scope and enforcement of their duties in that regard? *b)* How does domestic case law approach the intersection of freedom of expression (freedom of speech) and privacy? How is this balance affected by the Charter and most particularly by Article 47, read together with Articles 7, 8, 11?

Within the following cluster of cases, the main case that is to be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

➢ Judgment of the Court (Grand Chamber), 3 October 2019, *Eva Glawischnig-Piesczek v. Facebook Ireland Limited*, C-18/18 (***Glawischnig-Piesczek***)

Cluster of relevant CJEU cases

➢ Judgment of the Court, (Grand Chamber), 6 October 2015, *Schrems v. Data Protection Commissioner*, C-362/14 (***Schrems***)

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, C-507/17 (***Google***)

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *GC, AF, BH, ED v. Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17 (***GC and others***)

➢ Judgment of the Court (Grand Chamber), 3 October 2019, *Eva Glawischnig-Piesczek v. Facebook Ireland Limited*, C-18/18 (***Glawischnig-Piesczek***)

➢ Judgment of the Court (Grand Chamber), 16 July 2020, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, C-311/18 (***Facebook Ireland and Schrems***)

Relevant legal sources

EU Level

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market ('Directive on electronic commerce')

Article 14; Article 15(1); Article 18(1)

National level[10]

1) Paragraph 1330 of the *Allgemeines Bürgerliches Gesetzbuch* (General Civil Code)
2) Paragraph 78(1) of the *Urheberrechtsgesetz* (Law on copyright)
3) Paragraph 18(1) of the *E-Commerce-Gesetz* (Law on electronic commerce)

The case(s):

The question of obligations of service providers was approached by the Court in *Glawischnig-Piesczek* (C-18/18). The case concerned the responsibility of social media to control and remove illegal or defamatory material published within their outlets.

Eva Glawischnig-Piesczek, an Austrian politician, demanded Facebook Ireland to delete a comment that appeared under the article about her which was shared on a Facebook page and was accessible by any user. The Austrian court had already declared the comment defamatory, insulting and harmful to the reputation of Glawischnig-Piesczek.

After Facebook's refusal to remove the comment, Glawischnig-Piesczek complained before the Commercial Court in Vienna. The court, by interim order, obliged Facebook to stop publication of Glawischnig-Piesczek's photos if they were posted with text having an equivalent meaning of the comment in question. As a result, Facebook disabled access to the discussed content in Austria.

The Higher Regional Court in Vienna upheld the order and added that the restriction of publication concerns only the content notified to Facebook by Glawischnig-Piesczek, third parties or otherwise during the proceedings. The court has also recognized the excessively harmful and defamatory character of the published comment.

Both Facebook and Glawischnig-Piesczek lodged appeals before the Supreme Court of Austria. The court, deciding whether the injunction may also be extended to the identical or equivalent content, stated that **such an obligation** must be considered **proportionate** where the host provider was already aware of the harmful content on at least one occasion and, as a result, could foresee the risk of other infringements.

Preliminary questions referred to the Court:

In *Glawischnig-Piesczek* the Austrian Supreme Court referred the following questions to the CJEU for a preliminary ruling:

"1) Does Article 15(1) of Directive [2000/31] generally preclude any of the obligations listed below of a host provider which has not expeditiously removed illegal information, specifically not just this illegal information within the meaning of Article 14(1)(a) of [that] directive, but also other identically worded items of information:

worldwide;

in the relevant Member State;

of the relevant user worldwide;

of the relevant user in the relevant Member State?

[10] English translation as in C-18/18 *Glawischnig-Piesczek*.

2) In so far as Question 1 is answered in the negative: does this also apply in each case for information with an equivalent meaning?

3) Does this also apply for information with an equivalent meaning as soon as the operator has become aware of this circumstance?"

Reasoning of the Court:

The Court began its analysis by confirming the general prohibition enshrined in Article 15(1) of Directive 2000/31 to require host providers monitoring information which they transmit or store or to actively seek facts indicating an illegal activity. However, such a prohibition does not concern the monitoring obligations 'in a specific case'.

According to the Court, such a specific case may concern cases where the content stored by the host provider was declared illegal by the national court. Because of the risk of multiplication of such information between users of a social network, the court may require the host provider to block its access or remove it, including any identical content. This order does not entail a general obligation to monitor stored information nor actively search for illegal activity.

Subsequently, the Court approached the question of extending an injunction on the content that is equivalent to the information previously declared illegal. The Court defined 'information with an equivalent meaning' as 'information conveying a message the content of which remains essentially unchanged and therefore diverges very little from the content which gave rise to the finding of illegality'. In its view, the illegality of the content stems not from the use of certain terms, but from the fact that the conveyed message is declared illegal because of its defamatory character. Hence, in order to ensure the **effectiveness** of the order for an injunction, that injunction must be able to extend to the content essentially unchanged yet worded slightly differently. Otherwise, the order could be easily circumvented.

However, following the wording of Article 15(1) and Article 18(1) of Directive 2000/31 in conjunction with recital 41, the Court stressed that the obligation imposed on the host provider in order to protect a person's reputation and honour shall not be excessive. Consequently, the Court established general conditions to assess the equivalent nature of the information:

– it contains specific elements which are properly identified in the injunction (e.g. name of the person concerned by the infringement, the circumstances in which the infringement was determined, equivalent content to that which was declared illegal);

– differences in the wording do not require the host provider to carry out an independent assessment of the content.

According to the Court, such a solution allows for a sufficient balance between the protection of the targeted person and obligation imposed on the host provider. The order is then not general as it is limited only to monitor and search for information specifically detailed in the injunction and hence is attainable via automated search tools and technologies.

Finally, the Court approached the question of whether the order to block or remove the content declared illegal may have a global scope. Following Article 18(1) of Directive 2000/31, the Court observed that there is no provision in that regard for any limitation, including a territorial one, on the scope of the measures which the Member States are entitled to adopt. Hence, injunction measures may produce effects worldwide and it is up to national courts to decide so. However, in such cases the EU rules shall be consistent with the requirements of international law.

The Court did not directly approach the question of balance between fundamental rights of data protection and freedom of expression. In the context of Article 47 of the Charter, the AG Opinion warned that implementation of a removal obligation should not go beyond what is necessary to achieve the protection of the injured person. The AG pointed out that because of the lack of harmonisation among national laws, the national court must adopt an approach of self-limitation.

Conclusion of the Court:

In *Glawischnig-Piesczek* (C-18/18) the Court stated that national courts may order a host provider to remove or block access to information that is identical or equivalent to the content that was previously declared to be unlawful, regardless of who applied for its storage.

Subsequently, the Court specified that in cases of equivalent content an injunction shall be limited to the monitoring of and search for information that remains essentially unchanged compared with the content that was declared illegal. Moreover, the differences in the wording shall not require the host provider to carry out an independent assessment of the content.

Finally, according to the Court, the order to block or remove the content issued in the above mentioned circumstances may have a global scope. In such cases national courts shall act within the framework of the relevant international law.

Impact on the follow-up case:

The Supreme Court of Justice in Austria decided on the Glawischnig-Piesczek's case on 30 March 2020 (4 Ob 36/20b). Following the CJEU findings in *Glawischnig-Piesczek*, the Supreme Court held that the lower court had righteously ordered an injunction with a scope limited to Austria.

From the CJEU decision, the Supreme Court inferred that it is possible to issue an order to block or remove the illegal content if the essential correspondence appears at first glance or can be determined by technical measures such as content filtering. Moreover, the decisive criteria must be specified in the order in a sufficiently precise manner.

Subsequently, the Austrian court decided on the global effect of the order. Comparing the CJEU's findings in *Glawischnig-Piesczek* with similar decisions in the area of intellectual property law (C-170/12 *Pinckney*, C-192/04 *Lagardére*, C-194/16 *Bolagsupplysningen*) the Supreme Court held that orders based on Austrian IP law are limited to Austria given the established principle of territoriality. Where there are no clear restrictions of the territorial scope, the plaintiff should clarify whether they want to seek protection beyond Austria. Otherwise, it must be assumed that the scope is only domestic.

Elements of judicial dialogue:

Although the decision in *Glawischnig-Piesczek* (C-18/18) does not reference these cases directly, it seems to be in dialogue with *Google v. CNIL* and *GC and others v. CNIL*. These decisions were issued a week before the judgment in *Glawischnig-Piesczek* and discussed issues concerning possible conflicts between the freedom of expression and other fundamental rights. However, while in *Glawishnig-Piesczek* the Court interpreted provisions of Directive on electronic commerce, in *Google v. CNIL* and *GC and others v. CNIL* it approached Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

In ***Lindqvist***, Mrs Lindqvist contended that both Directive 95/46 and the Swedish law prohibiting processing of personal data of a sensitive nature were contrary to the general principle of freedom of expression enshrined in Community law, their scope being vague and too broad. The Court answers that at the stage of application at national level of the legislation implementing Directive 95/46, a balance must be found by national courts between the rights and interests involved through an interpretation of

national law in light of the **principle of proportionality**. For the Court, whilst it is true that the protection of private life requires the application of effective sanctions against people processing personal data in ways inconsistent with Directive 95/46, such sanctions must always respect the principle of proportionality. Since the scope of Directive 95/46 is very wide and the obligations of those who process personal data are many and significant, it is for the referring court to take account, in accordance with the principle of proportionality, of all the circumstances of the case before it, in particular the duration of the breach of the rules implementing Directive 95/46 and the importance, for the persons concerned, of the protection of the data disclosed.

In ***Google Spain*****,** the Court considers that the processing of personal data carried out by the operator of a search engine is liable to significantly affect the fundamental rights to privacy and to the protection of personal data when the search using that engine is carried out on the basis of an individual's name, since that processing enables any internet user to, through the list of results, obtain a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of their private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty. In light of the potential seriousness of that interference, the Court finds that it cannot be justified merely by the economic interest the operator of such an engine has in that processing. However, given the legitimate interest of internet users potentially interested in having access to information, a fair balance should be sought between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, the interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

In ***Google v. CNIL*** the Court refined the construction of the right to be forgotten established by ***Google Spain***. The case concerned an order issued by the French data protection authority on Google to globally remove references falling within the right to be forgotten request from its search engine. Google refused to do so and was fined 100 000 EUR. The French court made a preliminary reference to the CJEU, asking about the territorial scope of de-referencing and the use of geo-blocking technique in restricting access from places subject to the Directive 95/46. The Court stated that the search engine operator is obliged only to de-reference the versions of that search engine corresponding to all the Member States, using, when necessary, effectively preventive or discouraging technical measures.

In *Google v. CNIL* the Court stated that where a search engine operator grants a request for de-referencing, 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. However, in *Google v. CNIL* the Court approached directly the balance of fundamental rights; in *Glawischnig-Piesczek* the question was raised only within the AG opinion.

Similarly, in *GC and others v. CNIL* the Court approached obligations of search engine operators in the context of the right to be forgotten. The case concerned several claims of individuals demanding de-referencing of links revealing special categories of their data. The referencing court asked whether the prohibition imposed on other controllers of processing data caught by Article 8(1) and (5) of Directive 95/46, also applies to the operator of a search engine. The CJEU answered affirmatively and enshrined that where the operator of a search engine has received a request for de-referencing relating to a link to

a web page on which special categories of personal data are published, the operator must ascertain whether the inclusion of that link as a result following a search on the basis of the data subject's name is strictly necessary for protecting the freedom of information of internet users, protected by Article 11 of the Charter. The assessment must be carried out taking into account Articles 7 and 8 of the Charter, as well as the reasons of substantial public interest. Although the Court did not consider obligations of social media providers in *Schrems*, the case may also be relevant for the discussed mater. The Court stressed that protection of the fundamental right to respect for private life at EU level requires derogations and limitations in relation to the protection of personal data to apply only in so far as is strictly necessary. According to the Court, legislation not providing any possibility for an individual to pursue legal remedies in order to have access to personal data relating to them, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter.

The Court followed that reasoning in *Facebook Ireland and Schrems* (C-311/18) where it held that data transfers on the grounds of standard contractual clauses are based on the responsibility of the controller or his or her subcontractor established in the EU, and, in the alternative, of the competent supervisory authority. According to the Court, the controller or processor is obliged to verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection.

Moreover, *Glawischnig-Piesczek* is in dialogue with similar decisions issued on the grounds of intellectual property law. Although, the Court does not refer to them directly, they were either evoked by the Advocate General in his opinion or resonate within the judgment. For example, in Case C-360/10 *SABAM v. Netlog* the Court ruled that a social network cannot be obliged to install a general filtering system, covering all its users, in order to prevent the unlawful use of musical and audio-visual work. It stressed the obligation of the national authorities and courts to make a fair balance between the protection of copyright and the protection of the fundamental rights of individuals. In Case C-324/09 *L'Oréal and Others* the Court a host provider may be ordered to take measures to prevent the occurrence of any further infringements of the same nature by the same recipient. It may entail an order to remove illegal information that is yet unpublished.

Impact on national case law in Member States other than the state of the court referring the preliminary question to the CJEU

Poland

In Poland, there have not been any cases directly evoking *Glawischnig-Piesczek*. However, two pending cases concern the freedom of speech and duties of social media.

The president of the anti-defamation foundation "Reduta Dobrego Imienia" complained before the Polish court that in 2016 Facebook had suspended accounts spreading information about the rally organised by far-right groups on National Independence Day. The claimant argues that decisions were automatically made and users had not disposed of any effective redress. The proceedings started in 2019.

In a similar case, the NGO Panoptykon filed in 2019 a lawsuit against Facebook before the Polish court for removing in 2018 fan pages and groups run by a Polish NGO "Społeczna Inicjatywa Narkopolityki" (The Civil Society Drug Policy Initiative"). The NGO conducts educational campaigns and provides assistance to people addicted to drugs. Without any warning and explanation, it was accused of violating community standards in an automated decision. The case is pending.

Also, in the judgment of 25.03.2021 (I SA/Ke 31/21) the Provincial Administrative Court in Kielce dismissed a complaint against a decision to retain a driving license and to disclose information about it in a central information system (with referral to Articles 15-16 and 18 GDPR).

5.1.2. Question 1b: the intersections of freedom of expression and privacy in domestic case law

Question 1b - How does domestic case law approach the intersection of freedom of expression (freedom of speech) and privacy? How is this balance affected by the Charter and most particularly by Article 47, read together with Articles 7, 8, 11?

The question of the balance between the freedom of expression and information and other fundamental rights such as the fundamental right to private life, the right to protection of personal data and the right to an affective remedy and to a fair trial has already been approached by national courts.

The Netherlands

In the case C/13/579966, issued on 24 December 2015, the District Court of Amsterdam decided on the request of an appellant, a Dutch journalist, to remove the URL leading to a press article on the termination of the collaboration between them and the newspaper because of plagiarism from Google[11]. The Dutch court referred to *Google Spain* and acknowledged that an individual has a right to request a removal of their personal data from a search engine. Subsequently, the court balanced between the rights enshrined in Article 7 and Article 11 CFREU. As it determined, there was an overriding public interest in this case: the journalist should bear responsibility for plagiarism and acted in a professional role, which remains relevant to his current working life[12].

In the case C/15/03380, issued on 24 February 2017, the Dutch Supreme Court decided on the concept of an overriding public interest with regard to relation between protection of personal data and the right to information.[13] The case concerned a convicted assassin who requested Google to remove the URL showing information on a book about a crime he committed. The court addressed *Google Spain* and relying on CJEU's findings decided that the claimant had a right to be forgotten. According to the court's reasoning, if the information is no longer made available to the public, rights enshrined in Articles 7 and 8 CFREU take precedence over the economic interests of the data processor and the interests of the internet users[14]. The court stressed the importance of a proportionality test and a proper assessment whether the public interest indeed overrides the rights of an individual.

In the case C/13/615516, issued on 15 February 2018, the Court of Amsterdam once again approached the question of balance between freedom of expression and information and protection of personal data[15]. The case concerned a person who demanded Google to remove a result leading to a press article about his falsified CV. The claimant argued that this constituted processing of criminal data which was

[11] Netherlands, District Court of Amsterdam, 24 December 2015 C/13/579966. https://www.fricore.eu/db/cases/netherlands-district-court-amsterdam-24-december-2015-c13579966
[12] *Ibid.*
[13] Netherlands, Dutch Supreme Court, 24 February 2017 15/03380, https://www.fricore.eu/db/cases/netherlands-dutch-supreme-court-24-february-2017-1503380
[14] *Ibid.*
[15] Netherlands, Court of Amsterdam, 15 February 2018 C/13/615516, https://www.fricore.eu/db/cases/netherlands-court-amsterdam-15-february-2018-c13615516

prohibited by the Dutch data protection law. The court referred to *Google Spain* and considered several factors while assessing the case: the sensitive character of criminal data, inaccuracies in the published article and the 10-years period between the request and the publication of the article. As a result, it concluded that there was no overriding public interest.

France

***Cour de cassation*, 12 May 2016, No. 15-17729 – Data protection and freedom of the press**

The case was brought before the French courts by data subjects requesting that their names be deleted from the list of results displayed by a search engine operated by a newspaper, in order to provide access to its articles. Although the claimant could have relied on the right to be de-listed, as created by the CJEU in *Google Spain* (see Chapter 6), the claim was based on a different lawful basis: the "*droit d'opposition*" limb of the law governing the press. Consequently, the French Courts did not rule on the claim by reference to *Google Spain*.

The French *Cour de cassation* dismissed the claim, on the ground that ordering a press institution either to erase information contained in one of their articles from the website storing its articles — where such erasure would deprive the article of its interest -- or to limit its availability to the public by modifying the functioning of the search engine, exceeds the restrictions that may be placed on the freedom of the press. Given the tradition of the French *Cour de cassation* of giving limited reasons for its decisions, it is not possible to verify whether the Court endorses a balance of interests in light of the principle of proportionality.

Belgium

***Cour de cassation*, 29 April 2016, No. C-150052F**

In a situation similar to the French one above, the Belgian *Cour de cassation* reached a radically different conclusion. The claimant had based its claim on *Google Spain* and the right to be de-listed (see Chapter 6). The Belgian court recognized the influence of *Google Spain* on national case law, carried out a balance of interests, and concluded that by refusing to delete the name of the claimant from the article, the press institution had infringed the right to be forgotten.

Italy[16]

The influence of the *Google Spain* decision on Italian case law in data protection matters has probably been most relevant and significant with regard to the criteria governing the balance of interests carried out by judges between the right to information and the rights conferred by Articles 7 and 8 of the CFREU (i.e., the rights to respect for private life and to protection of personal data). Before proceeding to analyse the criteria developed in the Italian case law after *Google Spain*, it must be emphasized how significant a role has been played by the "Guidelines on the implementation of the CJEU's Judgment on Google Spain" issued by the Article 29 Data Protection Working Party, particularly with regard to the assessment of the public interest served by information in terms of the role played by the data subject in public life.[17] Indeed, according to the guidelines, the CJEU decision set out the concept of

[16] Drafted by Gianmatteo Sabatino

[17] See Court of Cassation decision no. 13161/2016; Milan *Tribunale*, decision of 5 October 2016; Rome *Tribunale*, decision of 3 December 2015; Milan *Tribunale,* decision of 28 February 2017. On that issue, see also Rizzuti, *Il diritto e l'oblio,* in Corriere Giur., 2016, 8-9, 1072.

"role in public life" as a ground to justify the refusal to de-list the name of a data subject from the results displayed on a search engine page. Though, in principle, the role in public life must be assessed on a case-to-case basis, the guidelines state that, "politicians, senior public officials, business-people and members of the (regulated) professions can usually be considered to fulfil a role in public life. There is an argument in favour of the public being able to search for information relevant to their public roles and activities".[18] On the basis of such grounds, intended as a further development of the balance of interests already upheld by the CJEU, Italian courts have viewed as "roles in public life" those played by officers and employers of a municipality-owned company,[19] by a lawyer,[20] and by a member of a National Authority.[21]

The passing of time, therefore, becomes only one of the several criteria[22] to be considered when carrying out the balance of interests, even if, probably owing to the relevance of decision no. 5525/2012 of the Court of Cassation, courts still appear, in some cases, to afford that criterion much more consideration than the others.[23] When, by contrast, personal data displayed, for instance, on a public register, concern an economic activity carried out by the subject in the form of a business enterprise — especially companies that do not have complete autonomy over their assets — even if the data is retained for a long period of time, the public interest in having knowledge of such data is still considered to prevail over the right to protection of personal data.[24] In other cases, the circumstance that the data subject held high-profile institutional office was enough to justify the indexing, by a search engine provider, of information related to a judicial proceeding, though it had occurred many years before.[25]

The proportionality in the reporting of the information and whether the information adheres to the truth are also criteria the courts take into account, though some further remarks should be made: in first place,

---

[18] The same concept is reassessed by Resolution 1165 (1998) of the Parliamentary Assembly of the Council of Europe on the right to privacy, which provides a possible definition of "public figures". It states that, "Public figures are persons holding public office and/or using public resources and, more broadly speaking, all those who play a role in public life, whether in politics, the economy, the arts, the social sphere, sport or in any other domain."

[19] See Milan *Tribunale*, decision of 28 February 2017.

[20] See Rome *Tribunale*, decision of 3 December 2015.

[21] See Milan *Tribunale*, decision of 5 October 2016. It is worth mentioning that in this case, though the public role was in principle recognized, the Court eventually upheld the data subject's claim on account of the circumstance that the information indexed by the search engine provider was incomplete and not up-to-date, thus not relevant for the public.

[22] See Milan *Tribunale*, decision no. 12623 of 4 January 2017. The decision considered several criteria to weigh in the balance of interests, including the passing of time, and upheld the prevalence of the individual's right to privacy over the public interest showed by the evidence, which was not specific enough, as the facts in the news referred to in the erased URLs did not lead to any criminal conviction. In particular, the decision stated that even cache copies of personal data have to be erased at the request of the data subject when there is no relevant public interest involved.

[23] See Court of Cassation, decision no. 13161/2016; Mantova *Tribunale*, decision of 28 October 2016.

[24] See Court of Cassation, decision no. 19761/2017.

[25] See NPDA decision no. 277 of 15 June 2017. It is worth mentioning that this same decision took two different stances in relation to several links to articles containing information on a judicial proceeding involving the data subject: in particular, the articles that only discussed the case generally were considered to contravene the data protection legislation, also taking into account the fact that the data subject's conviction in that proceeding had been spent. On the other hand, the articles containing such information and, in addition, other information regarding the professional activity of the data subject, were considered to fulfil a public interest prevailing over the right of protection to personal data.

it must be pointed out that such criteria cannot be invoked, on a general basis, when filing a complaint against an ISP but only when asking for the publisher of the information to be ordered to erase it.[26] Second, both proportionality and adherence to the truth are criteria that courts, even before *Google Spain*, have used in order to assess the legitimacy of the exercise of the right to information when dealing with claims not only of infringement of privacy but also damage to reputation.[27] Notwithstanding, even if the courts use criteria already adopted before the CJEU decision, it is important to highlight how such criteria, when applied to cases concerning the displaying of information on the internet, have been interpreted according to what the CJEU stated in the *Google Spain* decision about the relevance of the internet in terms of the danger it poses for data protection. In other words, Courts recognise how information published online is able to reach an otherwise unreachable number of people.[28] Judges cannot ignore this circumstance and, as a consequence, have to adjust the criteria used to carry out the balance of interests in order to ensure a high level of protection for data subjects.

More recently, in its decision n. 19681 of 22 July 2019, the Court of Cassation addressed the question of the relationship between the right to private life and the right to be forgotten on the one hand, and the right to the historical evocation of facts and events concerning past events, which form part of the freedom of the press and information (Article 21 of the Italian Constitution). The Court, relying on *Google Spain* (C-131/12), stated that the judge must assess in each case the existence of a concrete and actual public interest, which justifies the mention, by journalists, of information that allows identifying persons who were protagonists of those past facts and events. This mention must be considered lawful only in the hypothesis in which it refers to people who are of interest for the community, both for reasons of fame and for the public role played. Otherwise, according to the Court of Cassation, data subject's right to private life prevails.

5.1.3. Question 2: The role of public interest in revealing information vis-à-vis data and privacy protection

What is the role of public-purpose reveal of data (especially by journalists) on the general standard of privacy protection? To what extent does Article 47 influence the scope and enforcement of this standard?

Relevant CJEU cases

Within the following cluster of cases, the main case that is to be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

➢ Judgment of the Court (Second Chamber) of 14 February 2019, proceedings brought by *Sergejs Buivids*, Case C–345/17 (***Buivids***)

Cluster of cases

[26] See Court of Cassation, decision no. 13151/2017; NPDA decision no. 618 of 18 December 2014.

[27] See Cassino *Tribunale*, decision of 25 March 2014.

[28] See Court of Cassation, decision no. 13161/2016; Court of Cassation, decision no. 13151/2017.

➢ Judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C73/07, EU:C:2008:727

➢ Judgment of the Court (Second Chamber) of 14 February 2019, proceedings brought by *Sergejs Buivids*, Case C–345/17 (***Buivids***)[29]

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *GC, AF, BH, ED v. Commission nationale de l'informatique et des libertés (CNIL)*, C-136/17 (***GC and others***)

Relevant legal sources

EU law

Directive 95/46 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 (no longer in force)

Recital 2; Recital 14; Recital 15; Recital 17; Recital 27; Recital 37; Article 7; Article 9

Domestic law

Fizisko personu datu aizsardzības likums (Personal Data Protection Law) of 23 March 2000 (Latvijas Vēstnesis, 2000, No 123/124; 'the Personal Data Protection Law')

Article 5; Article 8(1)

The case:

The preliminary question has been referred to the CJEU by a Latvian court in the case concerning a penalty imposed on Mr Sergejs Buivids by the Latvian National Data Protection Agency. Mr Buivids was sanctioned for recording a video at a police station while he was making a statement in the course of criminal proceedings carried out against him — and for subsequent publication of this video on the Youtube.com platform. The Latvian data protection authority found this conduct to violate the domestic data protection rules (which implemented the 95/46 Directive), since Mr Buivids did not properly inform police officers that the video is going to published online. On these grounds, Mr Buivids was ordered to remove the video from the Youtube.com platform, as well as from all the other websites where it was proliferated.

Mr Buivids's appeal from this decision was dismissed by both the administrative courts of first and the second instance. As was concluded, the video depicts the police facilities, as well as features voices of police officers, Mr Buivids and the persons accompanying him. Moreover, it was found that Mr Buivids did not indicate precisely for what purpose he made and proliferated the video. At the same time, the video did not depict current events of social relevance, nor any dishonest conduct of the police officers. This led to the conclusion that the video in question did not involve journalistic purposes in the sense established by data protection rules. Mr Buivids brought the case to the Supreme Court of Latvia (*Augstākā tiesa*), which referred preliminary questions to CJEU.

Preliminary questions referred to the Court:

The Latvian Supreme Court referred to CJEU two preliminary questions:

[29] The same issue was also addressed in the *SY v. Associated Newspapers Ltd.* (C-687/18). On 29 October 2019 the referring court withdrew the preliminary question.

(1) Do activities such as those at issue in the present case, that is to say, the recording, in a police station, of police officers carrying out procedural measures and publication of the video on the internet site www.youtube.com, fall within the scope of Directive 95/46?

(2) Must Directive 95/46 be interpreted as meaning that those activities may be regarded as the processing of personal data for journalistic purposes, within the meaning of Article 9 of Directive [95/46]?'

The further analysis will focus on the second question, which is directly relevant for interconnection between data and privacy protection in extrapolation with freedom of speech (freedom of expression).

Reasoning of the Court:

In resolving the preliminary question, the Court departed from the general observation that every rule on the free flow of personal data should respect, in light of Article 1 of the 95/46 Directive, protection of fundamental rights and individual freedoms (including the privacy). At the same time, however, "those fundamental rights must, to some degree, be reconciled with the fundamental right to freedom of expression". As the Court pointed out, this obligation to reconcile stems from recital 37 of the 95/46 Directive, read together with Article 9 of this act. The Court also drew the attention to interconnections between the case in question and the human rights concerns, along with the case law of the ECHR case law.

By referring to its previous standpoint (judgment of 16 December 2008, *Satakunnan Markkinapörssi and Satamedia*, C73/07, EU:C:2008:727, p. 56–61) the Court also established that the concepts related to freedom of expression, such as the concept of journalism, should be framed in broad terms. This includes, *inter alia*, understanding journalism to include every act of the journalist activity (*i.e.,* disclosing information, opinions and ideas, in every possible medium), also beyond the scope of media activity. Such qualification is not excluded also with regard to uploading video on the Youtube.com platform — and hence, it cannot be denied from the outset that such activity may constitute processing personal data "solely for journalistic purposes" (*i.e.,* in line with the exception in Article 9 of the 95/46 directive). At the same time, however, not every proliferation of data through Internet websites constitutes journalism in that meaning. For these reasons, the qualification in question should be carried out separately for each case and hence, it rests primarily with a domestic court.

The Court also observed that against the case's factual background it cannot be discounted from the outset that recording and publication of a video, without informing a person featured at the recording about the recording as such and about a purpose of making it, violate the fundamental rights to privacy. The domestic court should, hence, establish whether such violation could fall within the ambit of the exception in Article 9 of the 95/46 Directive.

Conclusion of the Court:

In conclusions the Court found that video recording of police officers in a police station, while a statement is being made, and the publication of such a video on Internet website (in a type of Youtube.com) may constitute a processing of personal data solely for journalistic purposes, within the meaning of Article 9 of the 95/46 Directive. Such conclusion can be made only as long it is apparent that the video in question was made and published solely in order to disclose information, opinions or ideas to the public.

Elements of judicial dialogue

GC and Others (C-136/17) is a case of particular interest. In this dispute, Google was requested by four different entities to de-reference various links leading to web pages containing special categories of data

published by third parties (in the case of the first person — data on sex life, the second — religious beliefs, the third and fourth — judicial proceeding and data revealed alongside). The referring court asked for clarification of the scope of obligations of the operator of the search engine once the request for removal of specific categories of data (either sensitive or regarding judicial proceeding) has been lodged.

The Court firstly ascertained that, according to the Article 12(b) and Article 14(a) of Directive 95/46 (and currently according to the Article 17 of Regulation 2016/679), as a rule, the operator of a search engine must answer to requests for de-referencing in relation to links to web pages containing personal data falling within the special categories referred to by those provisions. Notwithstanding, the operator may refuse to accede to a request for de-referencing if he establishes that the processing of sensitive data on the website to which the link leads is covered by exceptions provided for by EU law.

According to the Court, it should be verified whether the data subject's right, not only overrides the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. Now, Article 17(3)(a) of Regulation 2016/679 expressly states that the data subject's right to erasure is excluded where the processing is necessary for the exercise of the right of information. Furthermore, the circumstances (Article 8(2)(e) of Directive 95/46 and Article 9(2)(e) of Regulation 2016/679) that the data in question are manifestly made public by the data subject applies to the operator of the search engine and to the publisher of the web page should be concerned. Even then, however, the data subject may require delisting due his or her particular situation.

Therefore, in case of every de-listing request, the operator of the search engine must ascertain, whether the display of the link once the data subject's name was searched is necessary for exercising the right of freedom of information of internet users, which is a right protected by Article 11 of the Charter (see the provisions Article 8(4) of Directive 95/46 or Article 9(2)(g) of Regulation 2016/679). When deciding on the balance of the rights, the operator of a search engine must consider particularities of the case at hand and take into account the seriousness of the interference with the data subject's fundamental rights to privacy and protection of personal data as well as the reasons of substantial public interest referred to in Article 8(4) of Directive 95/46 or Article 9(2)(g) of Regulation 2016/679/. In other words, the operator of the search engine must ascertain whether the display of this link is strictly necessary for protecting the freedom of information of internet users.

5.2. Guidelines emerging from the analysis

Enforcement of data protection law against a host provider

Domestic courts are entitled to remove or block access to information (content) that is either identical or closely similar (equivalent) to the content that has been previously declared unlawful. The injunction in question may oblige a host provider to monitor the content only for information that remains essentially unchanged compared with the content that was declared illegal. There is no need for the injunction to put an obligation of permanent content monitoring, if the new information differs from the older one (already declared to be unfair) merely in terms of wording.

In this way the domestic courts may impose injunctions that apply not merely to the particular state, but also that have a global effect. In this way — as the *Glawischnig-Piesczek* decision clearly sets forth — courts should revoke the relevant provisions of international law and act within their scope.

Establishing the 'journalist content' exception

Publication of the content that infringes one's privacy may be legitimate as long as the content has been published for journalist purposes. Even if such information has been published in an open-access repository (such as Youtube.com) there is no ground for its removal if it satisfies the definition of journalistic content in the sense of Article 9 of the 95/46 Directive.

It should be possible to clearly establish — given the circumstances of the particular case — that the information has been published solely in order to disclose information, opinions and ideas to the public. This task rests with a domestic court that should evaluate not only the content of the information, but also the context in which it was published and the potential array of its addressees. In this way the domestic judge should, hence, delve into the possible way of understanding the content by the average members of the society — and make sure whether this content may not harm the individual's privacy in disproportionate way. The latter would be the case when the content does not simply convey information, ideas and opinions for socially useful purposes.

6. Effective Data protection between administrative and judicial enforcement

6.1. Introduction

To ensure an effective protection of personal data, the EU relies mainly on national supervisory authorities as mentioned in Chapter VI and VII of the GDPR. The role of judicial enforcement should not, however, be underestimated.

Indeed, at the **national level**, data protection is enforced through both administrative and judicial enforcement mechanisms.

With regard to the first one, Article 58 of the GDPR confers to national supervisory authorities a broad catalogue of corrective, investigative, authorisation and advisory powers. All of the EU supervisory authorities have, amongst others, a competence to impose fines, issue a warning or reprimand to the data processor/controller, order the suspension of the processing of personal data, block and erasure of specific data, or order the controller or the processor to comply with the data subject's requests.

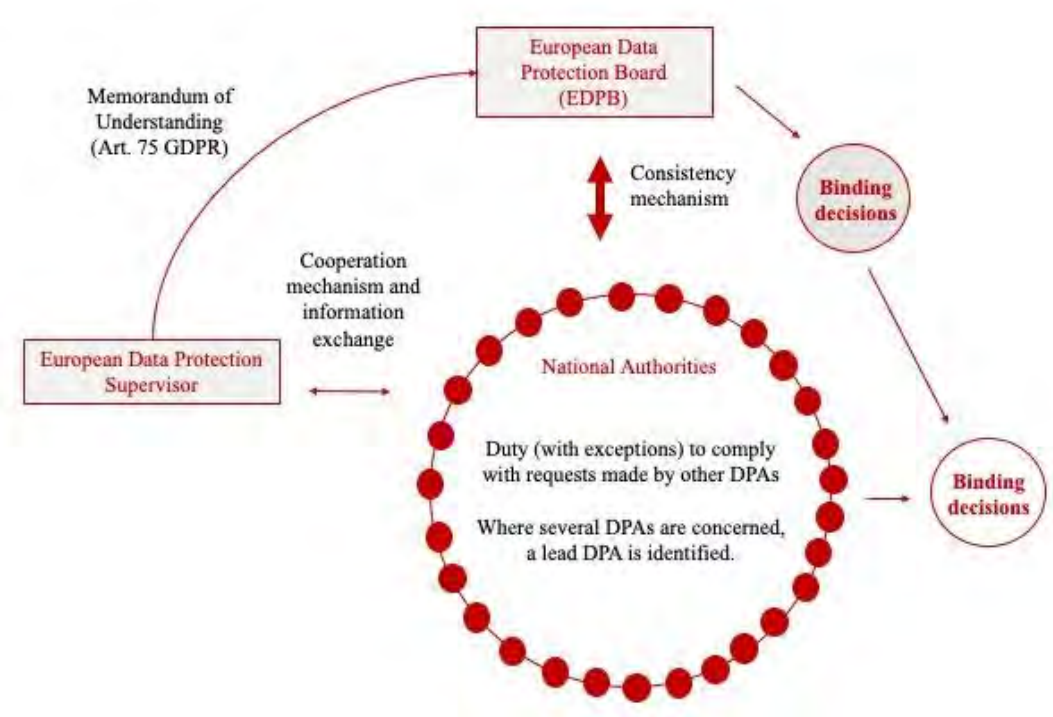
The power to apply financial charges belongs to the supervisory authorities, with the exception of those systems that do not recognise administrative fines (Denmark, Estonia). In the latter case, pursuant to Article 83 (9) of the GDPR, the fine is initiated by the competent supervisory authority and imposed by competent national courts. Recital 151 further specifies that in Denmark the fine is imposed by the national court as a criminal penalty and in Estonia by the supervisory authority in the framework of a misdemeanour procedure. In each case, the competent national courts shall recognise the recommendation of the DPA. A result should be equivalent to the administrative fines issued in other Member States.

At the **European level**, the action of the European Data Protection Supervisor (EDPS) and of the European Data Protection Board (EDPB) are of particular interest. The **European Data Protection Supervisor (EDPS)** is responsible for ensuring the protection of the fundamental rights and freedoms of natural persons and the right to data protection in relation to the processing of personal data by EU institutions and bodies (Article 52, EU Regulation 2018/1725). The tasks of the EDPS mainly relate to the application of EU Regulation 2018/1725 governing the processing of data by EU bodies and organs: this authority deals with complaints, conducts appropriate investigations, provides consultation to EU institutions on the processing of personal data, participates in the European Data Protection Board.

The **European Data Protection Board** (Article 68 GDPR) since 25 May 2018, replaced the Article 29 Working Party (Article 29 Directive 1995/46/EC), and endorsed certain WP29 documents of the Article 29 Working Group with the Endorsement 1/2018, dated May 25, 2018. The Board performs the function of ensuring the consistent application of EU Regulation 2016/679 and has the tasks of monitoring, advising the Commission, publishing guidelines, recommendations and best practices, and issuing opinions on codes of conduct drawn up at the European level (70 EU Regulation 2016/679). Under Article 65, GDPR, in order to ensure the correct and consistent application of the GDPR in individual cases, the Board shall adopt a binding decision where a supervisory authority concerned has raised a relevant and reasoned objection to a draft decision of the lead authority or the lead authority has rejected such an objection as being not relevant or reasoned. With respect to the activity of the EDPB, although the GDPR does not refer to the principle of good administration, the reference to Article 41 CFREU appears in the Rules of Procedure of the European Data Protection Board, as last modified in October 2020. Article 11 of that rules states:

"The Board shall respect the right to good administration as set out by Article 41 of the Charter. Before taking decisions, the Board shall make sure that all persons that might be adversely affected have been heard".

The complexity of the administrative enforcement required the creation of a system of **coordination between administrative authorities**, which is summarised in the following table:



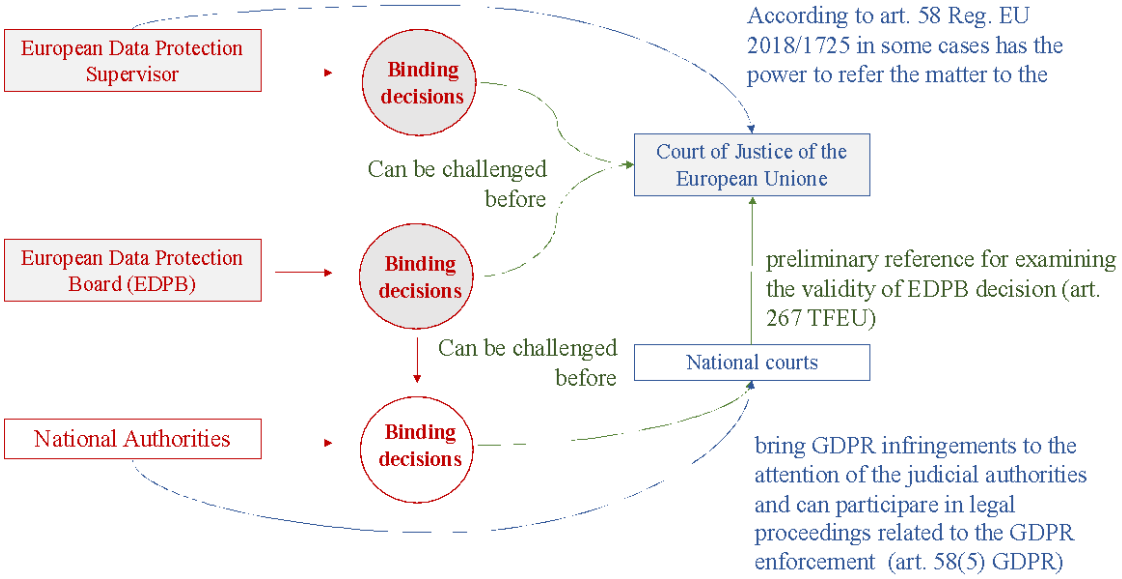
The GDPR provides a "diffuse" mechanism of cooperation between the various authorities and a "centralised" one.

With regard to the former, there is provision for the exchange of information between national supervisory authorities, mutual assistance, within a framework of cooperation. The distribution of competence among national authorities is established on the basis of various criteria, including the establishment of the controller and the existence of a complaint, in order to define both the "concerned" authorities and, in the case of several authorities involved, a lead authority. The coordination and cooperation between the lead authority and the other authorities concerned are regulated in Article 60 of EU Regulation 2016/679, according to which they must work to reach consensus. Within this framework, the supervisory authorities are obliged to comply with requests from other authorities, except for some limited cases. It also provides for the possibility of joint operations.

The 'centralised' cooperation mechanism mainly concerns the relationships between national DPAs and the EDPB, the contribution of national authorities to the activities of the EDPB and a consistency mechanism aimed at ensuring the cooperation of authorities and the uniform application of EU law.

Moreover, with regard to the relationships between the EDPB and the EDPS, Article 69 EU Regulation 2016/679 guarantees its independence in the exercise of the tasks referred to in Article 70 EU Regulation 2016/679, also with respect to the European Supervisor. Furthermore, the relationship between the EDPS and the EDPB is governed, according to Article 75 GDPR, by a memorandum of understanding, adopted on 25 May 2018 by the two Authorities. This document affirms the principles of independence and impartiality of the two authorities, those of good administration, integrity and the principle of cooperation, with a commitment to use the consensus method. In addition, without prejudice to professional secrecy, the two authorities exchange information on a regular basis for the purpose of the effectiveness of the arrangement.

Furthermore, **the relationships between administrative authorities and Courts are of particular interest,** and they are summarised in the following table:



With regard to the dialogue between the supervisory authorities and courts, judicial review is possible at national level against the decisions of the supervisory authority, and in some cases administrative authorities, as well as, at the conditions established by Article 80 GDPR, collective entities, may seek actions before courts.

As to the judicial review of administrative decisions, Article 78 gives an individual the right to an effective judicial remedy against a supervisory authority, and according to Article 58(4) of the GDPR the exercise by the supervisory authority of its powers shall be subject to appropriate procedural safeguards in accordance with Union, Member State law and the Charter, including effective judicial remedy and due process. The GDPR, however, does not clearly identify the extent of the judicial review by courts, i.e., whether it should be limited to the formal correctness of the decision of the supervisory authority (quashing the decision if appropriate, or requiring a new proceeding before the supervisory authority) or whether it may review the form and content of the decision (revising the content of the decision, and the remedies provided by the supervisory authority). Recital 143 explains only that the court "should exercise full jurisdiction, which should include jurisdiction to examine all questions of fact and law relevant to the dispute". No decision of the CJEU has addressed this issue in the area of data protection, although in other areas the effectiveness of judicial review has been addressed by the CJEU. For instance, in the *East Sussex Council* case (C-71/14) the CJEU affirmed that, where the European legislation does not detail the scope of judicial review, it is for the legal systems of the Member State to determine that scope, subject to the principles of equivalence and effectiveness[30]. Following the reasoning of the Court in *Puškár*, it seems that the Member States dispose of procedural autonomy as long as it is effective and not disproportionate.

[30] See paragraph 53.
See also the *Berlioz* case in the tax law area, paragraph 89 : "Those provisions of Directive 2011/16 and Article 47 of the Charter must be interpreted as meaning that, in the context of an action brought by a relevant person against a penalty imposed on that person by the requested authority for non-compliance with an information order issued by that authority in response to a request for information sent by the requesting authority pursuant to Directive 2011/16, the national court not only has jurisdiction to vary the penalty imposed but also has jurisdiction to review the legality of that information order. As regards the condition of legality of that information order, which relates to the foreseeable relevance of the requested information, the courts' review is limited to verification that the requested information manifestly has no such relevance."

With respect to the coordination mechanisms between the EDPB and courts, the dialogue can take place at two levels. As far as the European level is concerned, the EDPB's decisions can be challenged before the CJEU by any physical or legal person or by the supervisory authorities (Article 263 TFEU). Moreover, if a decision of the supervisory authority implementing a EDPB decision is challenged before a national court and the validity of the EDPB's decision is in question, that national court has no power to invalidate the EDPB decision, but if it considers the decision invalid must refer the question of validity to the CJEU (Article 267 TFEU as interpreted by the Court of Justice; recital 143 Regulation UE 2016/679).

Main questions addressed:

1. (a) In data protection cases, what is the role of the right to an effective judicial remedy (Article 47 CFREU), in defining the relationship between administrative and judicial enforcement?

(b) How does the right to effective judicial remedy affect coordination of administrative and judicial enforcement?

2. Is there a different institutional design between the administrative and judicial enforcement proposed by the ECtHR jurisprudence and that of the CJEU? When a mandatory preliminary administrative procedure is required before going to court, is it subject to different conditions under CJEU and the ECtHR standards in order to guarantee compliance with the principles of access to justice and the right to a fair trial?

3. a) Does Article 47 CFREU impact coordination between EU institutions and national authorities?

b) Is the supervisory authority of a Member State able to examine the claim of a person regarding the processing of personal data relating to him, and involving the transfer of personal data from a Member State to a third country, where the Commission has previously found that this third country ensures an adequate level of protection?

c) Does Article 47 CFREU impact coordination between national authorities?

4. Is the supervisory authority of a Member State able to examine the claim of a person concerning the validity of an act of the EU?

Cluster of relevant CJEU cases

➢ Judgment of the Court (Grand Chamber) of 16 July 2020, Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems, Case C-311/18 **("Facebook Ireland and Schrems/Schrems II")**

➢ Judgment of the Court (Grand Chamber), 15 June 2021, Case C-645/19, *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA, v Gegevensbeschermingsautoriteit,* **("Facebook Ireland and Others")**

➢ Judgment of the Court (Second Chamber) of 29 July 2019, Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, Case C-40/17 **("Fashion ID")**

➢ Judgment of the Court (Second Chamber) of 27 September 2017, Puškár v Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy, Case C-73/16, ("**Puškár**")

➢ Judgment of the Court (Second Chamber), 4 May 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v. Rīgas pašvaldības SIA 'Rīgas satiksme', Case C-13/16 ("**Rīgas satiksme"**)

➢ Judgment of the Court (Grand Chamber) of 6 October 2015, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, ("**Schrems**")

➢ Judgment of the Court (Grand Chamber) of 6 October 2020. *État luxembourgeois v B and Others*, Case C-245/19 and C-246/19

➢ Request for a preliminary ruling from the Fővárosi Törvényszék (Hungary) lodged on 3 March 2021 — *BE v Nemzeti Adatvédelmi és Információszabadság Hatóság*, Case C-132/21 (**BE v Nemzeti**)

➢ Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) lodged on 14 December 2021 — *TR v Land Hessen* (Case C-768/21)

➢ Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) lodged on 2 February 2022 — *AB v Land Hesse* (Case C-64/22)

➢ Request for a preliminary ruling from the Verwaltungsgericht Wiesbaden (Germany) lodged on 11 January 2022 — UF v Land Hesse (Case C-26/22)

Within this cluster, the aforementioned cases shall be presented as reference points for judicial dialogue within the CJEU and between EU and national courts on the question of the coordination between enforcement systems and the cooperation between national courts and national supervisory authorities.

6.1.1. Question 1: The right to effective judicial remedy and the coordination of administrative and judicial enforcement

(a) In data protection cases, what is the role of the right to an effective judicial remedy (Article 47 CFREU), in defining the relationship between administrative and judicial enforcement? (b) How does the right to effective judicial remedy affect coordination of administrative and judicial enforcement?

The possible relationships between administrative and judicial enforcement are the following:

a) *Alternative:* National legislation indicates that the national supervisory authority and the courts are alternative means of enforcement with respect to a violation of data protection legislation. The claimant can bring the claim either before an administrative authority or before a court.

b) *Complementary:* National legislation indicates that the national supervisory authority and courts are complementary with respect to a violation of data protection legislation. It defines the relationship between the two bodies. The claimant can bring the same claim before both, and the legislation can impose a sequence, *e.g.,* first the administrative authority and then the court.

a. simultaneous

b. sequential

c) *Independent:* National legislation does not say anything about the relationship between the national supervisory authority and the courts.

Relevant legal sources

EU Level

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Article 22
See, for comparison, Articles77-79, 83(7-8), GDPR
National Level
Slovak Constitution
Article 46

Code of Civil Procedure (Slovak): *Article 20, Paragraph 250v(1) and (3)*

The case(s):

Mr P, a Slovak citizen, presented before the Supreme Court of the Slovak Republic a claim to order the Finance Directorate, all tax offices under its control and the Financial Administration Criminal Office to remove his name from a list of people in directorship positions within companies, previously drawn up by the Finance Directorate. Although the list could only circulate among administrative offices, Mr. P. maintained that such a list, containing the Identity Number and Tax Identification Number of each mentioned individual, constituted a violation of his rights. He asked for the removal of his name and of any reference to him from the list and from other similar lists, as well as from the finance authority's IT system. Mr. P. never claimed nor proved that he had obtained the list with the consent (as was legally required) of the Finance Directorate or the Financial Administration Criminal Office. The Supreme Court dismissed the claim since Mr. P. (as well as the other two applicants) had not exhausted the remedies before the national administrative authorities. Mr. P. then lodged an appeal with the Constitutional Court of the Slovak Republic.

The Slovak Constitutional Court focused mainly on the jurisprudence of Article 6(1) ECHR in connection with Article 46 of the Slovak Constitution. In particular, the Constitutional Court addressed the obligation of the courts to justify their decision taking all the relevant facts and legal elements into account. This obligation was deemed as a prerequisite for the parties to exercise their right to an effective remedy. In this way, the Constitutional Court interprets Article 46 (1) of the Slovak Constitution in accordance with **Article 6 (1) ECHR** and on the basis of the ECtHR jurisprudence (in particular, *Garcia Ruiz v. Spain*; *Van de Hurk v. the Netherlands*; *Ruiz Torija v. Spain*; *Georgiadis v. Greece*; *Suominen v. Finland*; *Vetrenko v. Moldova*; *Wagner and J.M.W.L. v. Luxembourg*; *Pronina v. Ukraine*; *Krasulya v. Russia*; *Hiro Balani v. Spain*).

The Constitutional Court affirmed that in order to comply with the requirements of Article 46 of the Constitution (and Article 6 ECHR) the analysis of the Supreme Court should have taken into account all circumstances of the case in terms of the level of protection of personal data guaranteed by the Constitution and the level of protection of privacy guaranteed by the ECHR. Thus, the Constitutional Court concluded, after having analysed and compared the national and ECtHR jurisprudence, that the Supreme Court had failed to take into account the factual and legal arguments of the case and, most importantly, to provide a decision on the conditions that should have been met for the protection of personal data in the case of data processing by tax authorities.

Thus, the decision of the Constitutional Court completely disregarded the sequence proposed by the Supreme Court ruling between the preliminary administrative proceedings and the judicial proceedings, requiring the court to provide a detailed analysis of the claim and a decision on whether the processing of data by the tax authorities was lawful.

The Constitutional Court then affirmed that the Supreme Court had infringed the applicant's fundamental rights, namely the right to an effective remedy and a fair trial, the right to privacy and the right to protection of personal data. Thus, the Constitutional Court referred the case back to the Supreme Court. At this point, the Supreme Court, believing that the Constitutional Court had not taken into account the case-law of the EU Court of Justice, decided to refer to that court for a preliminary ruling.

Preliminary questions referred to the Court:

The Slovak Supreme Court presented four questions; for the purpose of this analysis, only the first question will be addressed in detail in this section.

The first question sought to verify if the mandatory preliminary administrative procedure adopted by the Slovak legislature in the case at issue is compliant with EU law and in particular with Article 47 CFREU.

"1. Does Article 47(1) of the Charter, under which every person whose rights — including the right to privacy with respect to the processing of personal data in Article 1(1) et seq. of Directive 95/46 — are violated has the right to an effective remedy before a court in compliance with the conditions in Article 47 of the Charter, against a provision of national law which makes the exercise of an effective remedy before a court, meaning an administrative court, conditional on the fact that the claimant, to protect his rights and freedoms, must have previously exhausted the procedures available under *lex specialis* — law on a specific subject — such as the Slovak Law on administrative complaints?"

Reasoning of the Court:

After stating that personal data collected for tax purposes fall within the scope of Directive no. 95/46, since they are dealt with by Article 13 (1) of that Directive, the Court proceeds to consider each of the preliminary questions.

Where the first one is concerned, the Court points out that the obligation to exhaust additional administrative remedies, while not excluded by Directive no. 95/46, must be scrutinised in light of Article 47 CFREU, Article 4 (3) of the TEU (principle of sincere cooperation) and Article 19 (1) of the TEU (effective judicial protection in the fields covered by EU law). Since such an obligation to exhaust additional administrative remedies constitutes a limitation of the right to an effective judicial remedy, it may be justified according to the criteria set in accordance to Article 52 (1) CFREU, namely only when:

i) provided by law;
ii) respectful of the essence of the right;
iii) subject to the principle of proportionality;
iv) compliant with objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others.

The Court focused in particular on the last two criteria.

With regard to the existence of objectives of general interest, the Court acknowledged that the obligation to lodge an administrative complaint before bringing a legal action has two main positive effects: first, it may relieve the courts of disputes that can be decided in a shorter time by the administrative authority concerned; and second, it may increase the efficiency of judicial proceedings in disputes in which a legal action is brought despite the fact that a complaint has already been lodged. Thus, the general obligation pursued objectives of general interest.

Regarding the test of proportionality, the Court relied on the AG opinion and on the decisions in *Alassini* and *Menini*. In particular, it explicitly referred to the criteria identified in the *Alassini* decision (paragraph 67), which should guide the proportionality test *vis-à-vis* the additional steps imposed in the national procedure, namely:

1. The procedures do not result in a decision which is binding on the parties;
2. The procedures do not cause a substantial delay for the purposes of bringing legal proceedings;
3. The procedures suspend the period for the time-barring of claim;
4. The procedures do not give rise to costs — or give rise to very low costs — for the parties;
5. The procedure must not be accessible exclusively by electronic means, nor be the only means by

which the settlement procedure may be accessed; and,

6. The procedures allow for interim measures in exceptional cases where the urgency of the situation so requires.

On the basis of these criteria, the Court affirmed that the obligation to exhaust the available administrative remedies appears appropriate for achieving the aforementioned objectives of general interest, and no less onerous and efficient method is available and capable of achieving those objectives.

Conclusion of the Court:

The Court declared that the Slovak legal provisions do not as such infringe EU law, and referred to the national court the assessment of the proportionality of the obligation to exhaust administrative remedies, also with regard to the additional costs of the proceedings imposed on the parties.

Elements of judicial dialogue:

The CJEU decision in *Puškár* arises from a preliminary reference under Article 267 TFEU. The Slovak Supreme Court resorted to a preliminary reference owing to a conflict of interpretation with the Slovak Constitutional Court. The CJEU acknowledges that the contrast between the national courts may affect the results of the decision in a specific case; thus, it addresses in detail the problem of coordination between administrative and judicial enforcement systems.

It is important to note that the conclusion of the CJEU is based on the jurisprudence of the same court in other areas of law, namely public procurement (e.g., *SC Star Storage*), migration and asylum law (e.g., decisions in *Tall* and *Sacko*), and in particular electronic communication (e.g., *Alassini*) and consumer protection (e.g. *Menini*).

From a different standpoint, the judicial dialogue between European and national courts at the same time addresses the horizontal aspect, with the decision of the CJEU able to provide a uniform interpretative perspective so to avoid further conflicts.

In Rīgas satiksme a question concerning the relationship between administrative and judicial enforcement has been raised and concerned the disclosure of personal data of a person responsible for a road accident to a third party in order to exercise a legal claim. However, the CJEU in this case did not address the manner in which the two enforcement mechanisms interact. It rather focused on the balance of interests between the protection of personal data and the possibility to bring an action for damages before a civil court for harm caused by the person concerned by the protection of that data (see more in Chapter 3, question 2).

In *Fashion ID* the Court, while not referring directly to the problem of coordination between administrative and judicial enforcement systems, evokes *Puškár* in the interpretation of Article 22 of the Directive. The Court followed the reasoning of *Puškár* where it confirmed that although Article 22 requires Member States to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law, it does not contain any provisions specifically governing the conditions under which that remedy may be exercised.

In the pending case *BE v Nemzeti* (C-132/21) the referring Court asked to the CJEU the following questions concerning the relationship between administrative and judicial enforcement:

"In the event that the data subject (…) simultaneously exercises his right to lodge a complaint under Article 77(1) [GDPR] and his right to bring a legal action under Article 79(1) [GDPR], may an interpretation in accordance with Article 47 of the Charter of Fundamental Rights be regarded as meaning:

(a) that the supervisory authority and the court have an obligation to examine the existence of an infringement independently and may therefore even arrive at different outcomes; or

(b) that the supervisory authority's decision takes priority when it comes to the assessment as to whether an infringement has been committed, regard being had to the powers provided for in Article 51(1) of Regulation 2016/679 and those conferred by Article 58(2)(b) and (d) of that regulation?

3. Must the independence of the supervisory authority, ensured by Articles 51(1) and 52(1) of Regulation 2016/679, be interpreted as meaning that that authority, when conducting and adjudicating upon complaint proceedings under Article 77, is independent of whatever ruling may be given by final judgment by the court having jurisdiction under Article 79, with the result that it may even adopt a different decision in respect of the same alleged infringement?"

Lastly, in the pending case *AB v Land Hesse* (Case C-64/22), the referring court asked to the CJEU whether according to Article 77(1) GDPR, read in conjunction with Article 78(1) thereof, the outcome that the supervisory authority reaches and notifies to the data subject

(a) has the character of a decision on a petition. The national judge specify that this would mean that judicial review of a decision on a complaint taken by a supervisory authority in accordance with Article 78(1) GDPR is, in principle, limited to the question of whether the authority has handled the complaint, investigated the subject matter of the complaint to the extent appropriate and informed the complainant of the outcome of the investigation, or

(b) is to be understood as a decision on the merits taken by a public authority. The national judge specify that this would mean that a decision on a complaint taken by a supervisory authority would be subject to a full substantive review by the court in accordance with Article 78(1) of the GDPR, whereby, in individual cases — for example where discretion is reduced to zero — the supervisory authority may also be obliged by the court to take a specific measure within the meaning of Article 58 of the GDPR.

In the pending case *UF v Land Hesse* (Case C-26/22) the national judge raised similar questions.

Impact on national case law in Member States other than the state of the court referring the preliminary question to the CJEU:

ITALY

Although not directly applying the decision taken in *Puškár*, before the entry into force of the GDPR the Italian Supreme Court addressed the compatibility with Article 24 of the Italian Constitution of the alternative enforcement proceedings before the supervisory authority and before the judicial courts (excluding in the case of a claim before the civil courts the possibility for a data subject to present the same claim before the supervisory authority, and vice versa).[31] In decision no. 6775/2016, 7 April 2016, the Supreme Court (Labour law section) concluded that Article 145 of the Italian Data Protection Code (now repealed) providing for the two alternative enforcement mechanisms is compatible with Article 24 of the Constitution (and therefore compatible with the right of the data subject to a defence) in cases where the claim addresses the "same object". In this sense, the alternative proceedings follow the general procedural rules of *lis pendens*. Whereas, when the claim before the judicial authority addresses the compliance of the data processor with a decision of the supervisory authority and/or the action for pecuniary or moral damages, the choice between the two alternative enforcements cannot apply (similarly, also, in Supreme Court no. 19534/2014, 17 September 2014).

[31] Note that Article 24 of the Italian Constitution provides that:
"Anyone may bring cases before a court of law in order to protect their rights under civil and administrative law. Defence is an inviolable right at every stage and instance of legal proceedings.
The poor are entitled by law to proper means for action or defence in all courts.
The law shall define the conditions and forms of reparation in case of judicial errors." (official translation)

AUSTRIA

The question of whether a citizen may file a complaint not only before the supervisory authority but also before the national court appeared in the Maximillian Schrems lawsuit against Facebook Ireland Ltd, filed before the Austrian court in 2014. During the proceedings, Facebook argued that only the Irish DPA should be responsible for the case. The Vienna Regional Court found itself twice not competent to consider the lawsuit — the second time in December 2018, after the Court's decision in case C-498/16 (*Schrems II*).

In the decision 11 R 24/19h, 25 March 2019, the Higher Regional Court of Vienna ("Oberlandesgericht Wien") admitted the right to submit the civil lawsuit before the national court on the grounds of Article 79 of the GDPR. The Court derived from this provision that Article 17 (1a) of the GDPR and §45 (2) of the Austrian Data Protection Act (DSG) asserted the right to erasure also in the judicial proceedings. According to the Court, §29 (1) DSG that standardises the jurisdiction for claims for damages does not stand in the way because it is only *lex specialis* to the GDPR.

POLAND

In Poland, there has not been any case directly approaching the issue discussed in *Puškár* so far. However, the question of coordination between judicial and administrative enforcement may appear in the recently opened case before the District Court in Warsaw.

Wojciech Klicki, a lawyer and privacy activist, sued the Polish Post for violating the GDPR by processing data of Polish citizens without a clear legal basis. The case concerns preparations for presidential elections which due to the COVID-19 pandemic were supposed to take place via mail on the 10 of May 2020 (eventually they were postponed). However, the law introducing the new form of elections came into effect on the 9 of May 2020. Nevertheless, the Polish Post had demanded from municipalities access to electoral register already on 16 of April 2020. After their refusal, it turned out that the Post had already had access to the social security number register from the Ministry of Digitalisation They argued that the decision of the Prime Minister was a legitimate basis for the processing.

The Polish data protection authority agreed with that interpretation and claimed that there had been no violation of the GDPR. The DPA did not initiate any proceedings but issued a statement where he argued that the PM's decision constituted a legitimate basis for the processing. Hence, the lawyer decided to pursue a judicial recourse instead of an administrative one.

According to Polish law, the court has to inform the DPA about the proceeding. The court should also suspend the process if the DPA initiated its own examination. So far the authority refused to take any action, arguing that the processing is legal. However, it may join the judicial proceedings before the District Court. While assessing compensation for the damage caused by infringement of data protection laws, the court is bound by the DPA's decision assessing the scope of those infringements.

6.1.2. Question 2: Interaction between the CJEU and the ECtHR

Is there a different institutional design between the administrative and judicial enforcement proposed by the ECtHR jurisprudence and that of the CJEU? When a mandatory preliminary administrative procedure is required before going to court, is it subject to different conditions under CJEU and the ECtHR standards in order to guarantee compliance with the principles of access to justice and the right to a fair trial?

Relevant legal sources:

ECHR Level

Article 6(1) ECHR

"In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interest of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice."

The analysis:

The issue of the distinction between the approaches of ECtHR and CJEU jurisprudence was mentioned in the *Puškár* case described above. In particular, the Slovak Supreme Court presented a fourth question seeking to resolve the conflict of jurisprudence between the CJEU and the ECtHR emerging from the interpretation by the Constitutional Court of the interconnection between the right to an effective legal remedy and the right to data protection. However, the Slovak Supreme Court in its preliminary reference did not clarify which were the specific decisions leading to the alleged conflict. This affected the ability of the CJEU to reply.

Although the CJEU did not provide a response regarding the potential "conflict" between its case-law and that of the ECHR, since this was raised in too general terms, for the purpose of the present analysis, it is useful to examine whether the European courts adopt different approaches with regard to the exercise of the right to an effective legal remedy in case of mandatory administrative proceedings in order to comply with Articles 47 CFREU and 6 ECHR, respectively.

The relevant ECtHR jurisprudence on the right to a fair trial includes cases addressing the following issues:

a. the inclusion of preliminary administrative procedure, and
b. the reasonable length of the proceedings.

Under a., the ECtHR acknowledged that the right of access to the courts is not absolute. In this sense, the prior intervention of administrative and professional bodies can be justified by the demands of flexibility and efficiency (see ECtHR decision in *Le Compte, Van Leuven and De Meyere v. Belgium*, § 51). In particular, the Strasbourg court found no violation if judicial bodies do not in themselves satisfy the requirements of Article 6 ECHR, insofar as the proceedings before those bodies are "*subject to subsequent control by a judicial body that has full jurisdiction*" and does provide the Article 6 guarantees (see ECtHR decision in *Zumtobel v. Austria*; *Bryan v. the United Kingdom*).[29]

Under b., the ECtHR has developed a broad jurisprudence addressing the importance of administering justice without delays that might jeopardise its effectiveness and credibility. Thus, a positive obligation is imposed on the Member States: to organise their judicial systems in such a way that courts are able to guarantee everyone's right to a final decision on disputes concerning civil rights and obligations within a reasonable time (*Comingersoll S.A. v. Portugal*; *Lupeni Greek Catholic Parish and Others v. Romania*). In order to evaluate the reasonable time in practice, all of the proceedings should be taken into account (*König v. Germany*).

In this sense, it is important to note that the application of Article 6(1) ECHR also takes into account proceedings which, although not wholly judicial in nature, are nonetheless subject to close supervision by a judicial body (see ECtHR decision in *Siegel v. France*). Thus, in order to define the duration of the whole procedure, the non-judicial proceedings are to be taken into account in calculating the reasonable time. Similarly, this happens when an application to an administrative authority is a prerequisite for bringing court proceedings (see ECtHR decisions in *König v. Germany*; *X v. France*; *Kress v. France*). The jurisprudence of the ECtHR does not indicate a precise timeframe for complex procedure, however, it

has affirmed that delays caused by the conduct of non-judicial authorities are deemed as violations of Article 6 (see ECtHR decision in *Schouten and Meldrum v. Netherlands*; *Kritt v. France*; *Clinique Mozart SARL v. France*).
From the analysis above, it emerges that the ECtHR does not differ from the position of the CJEU in regard to the compatibility of a preliminary administrative procedure with the right to a fair trial, insofar as it provides for a subsequent judicial review by a court with full jurisdiction. However, the ECHR has not addressed the case where this procedure is mandatory, whereas the CJEU, as early as the *Alassini* decision, provided a clear set of guidelines to evaluate whether the additional step in the procedure can be deemed compatible with the right to an effective remedy.
With regard to the reasonable length of the proceedings, the ECtHR provides a standard that takes into account whether the inclusion of administrative and non-judicial proceedings may affect the duration of the overall procedure. In this sense, the ECtHR standard is more detailed than the CJEU standard defined in the *Alassini* and *Puškár* decisions and may complement the latter.

6.2. Administrative authorities and effective protection of data subjects

DPA may not refer questions to the CJEU and Article 47 does not directly apply to those. However, the CJEU has had the chance to decide over questions concerning the role of DPAs in ensuring effective protection of data subjects, either as single authorities (question 3) or by means of cooperation among several DPAs (question 4)

6.2.1. Question 3: Coordination between EU institutions and national authorities

a) Does Article 47 CFREU impact coordination between EU institutions and national authorities? b) Is the supervisory authority of a Member State able to examine the claim of a person regarding the processing of personal data relating to them, and involving the transfer of personal data from a Member State to a third country, where the Commission has previously found that this third country ensures an adequate level of protection?

The main case that is to be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

➢ Judgment of the Court, (Grand Chamber), 6 October 2015, *Schrems* v. *Data Protection Commissioner*, C-362/14 (***Schrems I***)

Relevant legal sources:

Directive 95/46 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
Article 25 (6); Article 28 (3)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
Article 46 (2); Article 46 (3) (4); Article 52 (2); Article 52 (4)

The case(s) and preliminary questions referred to the Court:

As presented above in Chapter 1 on territorial scope, *Schrems* (C-362/14) concerned a transfer of the personal data of EU residents to servers belonging to the US, where they were processed.
The High Court of Ireland, hearing the appeal against the decision of the Irish Data Protection Commissioner, decided to present a preliminary reference asking:

"Whether and to what extent Article 25(6) of Directive 95/46, read in the light of Articles 7, 8 and 47 of the Charter, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Decision 2000/520, by which the Commission finds that a third country ensures an adequate level of protection, prevents a supervisory authority of a Member State, within the meaning of Article 28 of that directive, from being able to examine the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection?"

Reasoning of the Court

Focusing on the interplay between national supervisory bodies, national and European courts regarding the competence to verify the level of protection offered by third countries, the Court distinguishes two scenarios:

1. In the first scenario, pursuant to Article 25(1), the Member State should assess the adequacy of the level of the level of protection of personal data. In this case, on the basis of Article 8 CFREU and Article 28 of Directive 95/46, the Court attributes the responsibility for monitoring compliance with EU rules to the national supervisory authorities.
2. In the second scenario, by contrast, the Member State, the national supervisory authorities (and the courts) are bound by the decision of the Commission affirming that there is compliance with the level of protection. In this case, neither the Member State nor the national supervisory authorities may evaluate or even contest the Commission's evaluation, by adopting decisions or accepting behaviours contrary to the decision.

However, the Court acknowledges that it would be contrary to the system provided by Directive 95/46, and implicitly contrary to the right to an effective remedy, if a national supervisory authority could not examine a claim concerning the protection of a person's rights and freedoms in regard to the processing of his personal data which has been or could be transferred from a Member State to the third country covered by that decision.

Elements of judicial dialogue

After *Schrems* (C-362/14) it was revealed that Facebook had never relied on the Safe Harbour in transatlantic data transfer but used standard contractual clauses instead. Maximillian Schrems filed a complaint before the Irish Data Protection Commissioner, demanding the DPC to prohibit or suspend the transfer of his personal data to Facebook. The DPC argued that the case concerns the validity of the Decision 2010/87 on standard contractual clauses and initiated a proceeding against Schrems and Facebook.
Then, in the follow up case ***Facebook Ireland and Schrems* (C-311/18),** which concerns a data transfer to the US on the grounds of standard contractual clauses, the High Court of Ireland referred to the Court, amongst others, a following preliminary question:

"If a third country data importer is subject to surveillance laws that in the view of a [supervisory authority] conflict with [the standard contractual clauses] or Article 25 and 26 of Directive [95/46] and/or the Charter, is a data protection authority required to use its enforcement powers under Article 28(3) of the Directive to suspend data flows or is the exercise of those powers limited to exceptional cases only, in light of recital 11 of [Decision 2010/87 on standard contractual clauses], or can a [supervisory authority] use its discretion not to suspend data flows?"

The CJEU in its decision applied the GDPR instead of Directive 95/46 because of the entry into force of the former and the lack, in the present case, of a decision taken relying on the Directive.
The CJEU considered that the powers of the competent supervisory authority are subject to full compliance with the decision in which the Commission finds, where relevant, under the first sentence of Article 45(1) of the GDPR, that a particular third country ensures an adequate level of protection. In that case, the Court stated that it is clear from the second sentence of Article 45(1) of that regulation, read in conjunction with recital 103 thereof, that transfers of personal data to the third country in question may take place without requiring any specific authorisation.
Furthermore, the CJEU, relying on *Schrems* (C-362/14) affirmed that under Article 288(4) TFEU a Commission adequacy decision is, in its entirety, binding to all the Member States to which it is addressed and is therefore binding to all their organs in so far as it finds that the third country in question ensures an adequate level of protection and has the effect of authorising such transfers of personal data. Accordingly, the Court considered that, until such time as a Commission adequacy decision is declared invalid by the Court, the Member States and their organs, which include their independent supervisory authorities, cannot adopt measures contrary to that decision, such as acts intended to determine with binding effect that the third country covered by it does not ensure an adequate level of protection and, as a result, to suspend or prohibit transfers of personal data to that third country.
Nevertheless, the Court stated that:

- a Commission adequacy decision adopted pursuant to Article 45(3) of the GDPR cannot prevent persons whose personal data has been or could be transferred to a third country from lodging a complaint, within the meaning of Article 77(1) of the GDPR, with the competent national supervisory authority concerning the protection of their rights and freedoms in regard to the processing of that data.
- a decision of that nature cannot eliminate or reduce the powers expressly accorded to the national supervisory authorities by Article 8(3) CFREU and Article 51(1) and Article 57(1)(a) of the GDPR. Accordingly, the CJEU stated that, even if the Commission has adopted a Commission adequacy decision, the competent national supervisory authority, when a complaint is lodged by a person concerning the protection of their rights and freedoms in regard to the processing of personal data relating to them, must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the GDPR and, where relevant, to bring an action before the national courts in order for them, if they share the doubts of that supervisory authority as to the validity of the Commission adequacy decision, to make a reference for a preliminary ruling for the purpose of examining its validity.

-

6.2.2. Question 3c: The cooperation between national authorities and the right to seek action of national not-leading DPA

Does Article 47 CFREU impact coordination between national authorities?

The main case that is to be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

➢ Judgment of the Court (Grand Chamber), 15 June 2021, Case C-645/19, *Facebook Ireland Ltd, Facebook Inc., Facebook Belgium BVBA, v Gegevensbeschermingsautoriteit,* **("Facebook Ireland and Others")**

Relevant legal sources:

EU law

Regulation 2016/679

Recitals 1, 4, 10, 11, 13, 22, 123, 141 and 145; Article 3 concerning the territorial scope; Article 4 in relation to the definitions of "main establishment", "cross-border processing"; Article 51 headed 'Supervisory authority'; Article 55 headed 'Competence'; Article 56 headed 'Competence of the lead supervisory authority; Article 57(1) headed 'Tasks"; Article 58(1), (4) and (5) headed 'Powers'; Article 60, headed 'Cooperation between the lead supervisory authority and the other supervisory authorities concerned'; Article 61(1) headed 'Mutual assistance'; Article 62 headed 'Joint operations of supervisory authorities'; Article 63, headed 'Consistency mechanism'; Article 64 (4), headed Opinion of the Board; Article 65(1) headed 'Dispute resolution by the Board'; Article 66(1) and (2) headed 'Urgency procedure'; Article 77 headed 'Right to lodge a complaint with a supervisory authority'; Article 78 headed 'Right to an effective judicial remedy against a supervisory authority'; Article 79 headed 'Right to an effective judicial remedy against a controller or processor',

The case

On 11 September 2015, the President of the Privacy Commission brought legal proceedings seeking an injunction against Facebook Ireland, Facebook Inc., and Facebook Belgium before the Dutch-language Court of First Instance, Brussels, Belgium. The object of those injunction proceedings was to bring to an end what the Privacy Commission describes, *inter alia*, as a 'serious and large-scale infringement, by Facebook, of the legislation relating to the protection of privacy' consisting in the collection by that online social network of information on the internet browsing behaviour both of Facebook account holders and of non-users of Facebook services using various technologies. Those features permit Facebook to obtain certain data of an internet user who visits a website page containing features, such as the address of that page, the 'IP address of the visitor to that page, and the date and time of the visit in question. By judgment of 16 February 2018, the Dutch-language Court of First Instance of Brussels held that it had jurisdiction to give a ruling on those injunction proceedings, in so far as the action concerned Facebook Ireland, Facebook Inc., and Facebook Belgium. On the substance, that court held an injunction against Facebook Ireland, Facebook Inc., and Facebook Belgium. On 2 March 2018 Facebook Ireland, Facebook Inc., and Facebook Belgium brought an appeal against that judgment before the Brussels Court of Appeal. Before that court, the DPA acts as the legal successor both of the President of the Privacy Commission, who had brought the injunction proceedings, and of the Privacy Commission itself. The referring court held that it has jurisdiction solely to give a ruling on the appeal brought in so far as that appeal concerns Facebook Belgium. Conversely, the referring court held that it lacked jurisdiction to hear that appeal in relation to Facebook Ireland and Facebook Inc. Before giving a ruling on the substance of the main proceedings, a question raised by the referring court is whether the DPA had the required standing and interest to bring proceedings. With regard to the facts subsequent to 25 May 2018, Facebook Belgium claims that the DPA has no competence and has no right to bring such an action given the existence of the 'one-stop shop' mechanism now provided for under the provisions of Regulation 2016/679. On the basis of those provisions, it is claimed that only the Data Protection Commissioner (Ireland) is competent to bring injunction proceedings against Facebook Ireland, the latter being the sole controller of the personal data of the users of the social network concerned within the EU.

Preliminary question referred to the Court:

In the view of the referring court, the question that arises is whether, with respect to the facts subsequent to 25 May 2018, the DPA may bring an action against Facebook Belgium, since Facebook Ireland has been identified as the controller of the data concerned. Since that date and by virtue of the 'one-stop shop' rule, it appears that, in accordance with Article 56 of Regulation 2016/679, only the Data Protection Commissioner (Ireland) is competent, subject to review only by the Irish courts. Therefore, the national court referred several questions to the CJEU. The following question focuses on the impact of Article 47 CFR:

'Should Article 55(1), Articles 56 to 58 and Articles 60 to 66 of [Regulation 2016/679], read together with Articles 7, 8 and 47 of the [Charter], be interpreted as meaning that a supervisory authority which, pursuant to national law adopted in implementation of Article 58(5) of that regulation, has the competence to initiate or engage in legal proceedings before a court in its Member State against infringements of that regulation cannot exercise that competence in connection with cross-border data processing if it is not the lead supervisory authority for that cross-border data processing?'

Reasoning of the Court:

Firstly, the Court considered that the exercise of the power of a Member State's supervisory authority to bring actions before the courts of that State cannot be ruled out where, after the mutual assistance of the lead supervisory authority has been sought, under Article 61 of Regulation 2016/679, the latter does not provide the former with the requested information. The CJEU held that in that situation the supervisory authority concerned may adopt a provisional measure in the territory of its own Member State (Article 61(8) GDPR) and, if it considers that there is an urgent need for the adoption of final measures, that authority may request an urgent opinion or an urgent binding decision from the European Data Protection Board (Article 66(2) GDPR). Further, the Court, relying on Article 64(2) GDPR, affirmed that a supervisory authority may request that any matter that is of general application or that produces effects in more than one Member State be examined by the European Data Protection Board with a view to obtaining an opinion, in particular where a competent supervisory authority does not comply with the obligations for mutual assistance imposed on it by Article 61 GDPR. Moreover, the Court recalled that, following the adoption of such an opinion or such a decision, and provided that the EDPB approves, after taking account of all the relevant circumstances, the supervisory authority concerned must be able to take the necessary measures to ensure compliance with the rules on the protection of the rights of natural persons as regarding the processing of personal data contained in Regulation 2016/679 and, for that purpose, exercise the power conferred on it by Article 58(5) of that regulation.

As to the compatibility of these rules with Article 47 of the Charter, the Court stated that the manner in which the possibility that a supervisory authority other than the lead supervisory authority may exercise the power laid down in Article 58(5) of Regulation 2016/679, with respect to an instance of cross-border processing of personal data, is circumscribed takes nothing away from the right of every data subject, laid down in Article 78(1) and (2) of that regulation, to an effective legal remedy, in particular, against a legally binding decision of a supervisory authority concerning them, or against a failure by the supervisory authority which has the competence to adopt decisions under Articles 55 and 56 of that regulation, read together with Article 60 thereof, to handle a complaint that that data subject has lodged.

Furthermore, the Court stated that it is clear, in particular, from Article 51(1) of Regulation 2016/679 that the supervisory authorities are responsible for monitoring the application of that regulation, for the purpose, *inter alia*, of protecting the fundamental rights of natural persons regarding the processing of their personal data. Accordingly, the Court stated that the rules on the allocation of competences to adopt decisions between the lead supervisory authority and the other supervisory authorities, as laid down by that regulation, take nothing away from the responsibility incumbent on each of those authorities to

contribute to a high level of protection of those rights, with due regard to those rules and to the requirements of cooperation and mutual assistance. In the same vein, the CJEU considered that the use of the 'one-stop shop' mechanism cannot under any circumstances have the consequence that a national supervisory authority, in particular the lead supervisory authority, does not assume the responsibility incumbent on it under Regulation 2016/679 to contribute to providing effective protection of natural persons from infringements of their fundamental rights as recalled in the preceding paragraph of the present judgment, as otherwise that consequence might encourage the practice of forum shopping, particularly by data controllers, designed to circumvent those fundamental rights and the practical application of the provisions of that regulation that give effect to those rights.

Conclusion of the Court:

The Court concluded that Article 55(1), Articles 56 to 58 and Articles 60 to 66 of Regulation (EU) 2016/679 (GDPR), read together with Articles 7, 8 and 47 CFREU must be interpreted as meaning that a supervisory authority of a Member State which, under the national legislation adopted in order to transpose Article 58(5) of that regulation, has the power to bring any alleged infringement of that regulation to the attention of a court of that Member State and, where necessary, to initiate or engage in legal proceedings, may exercise that power in relation to an instance of cross-border data processing even though it is not the 'lead supervisory authority', within the meaning of Article 56(1) of that regulation, with respect to that data processing, provided that that power is exercised in one of the situations where Regulation 2016/679 confers on that supervisory authority a competence to adopt a decision finding that such processing is in breach of the rules contained in that regulation and that the cooperation and consistency procedures laid down by that regulation are respected.

Elements of judicial dialogue

The CJEU assessed the competences of DPAs under the directive 95/46 in Holstein (C-210/16), and the differences between the rules provided for by the directive and the system introduced with the GDPR seems evident comparing Facebook Ireland and Others (C-645/19) with Holstein (C-210/16). As to the latter, the CJEU affirmed that Articles 4 and 28 of Directive 95/46 must be interpreted as meaning that, where an undertaking established outside the EU has several establishments in different Member States, the supervisory authority of a Member State was entitled to exercise the powers conferred on it by Article 28(3) of that directive with respect to an establishment of that undertaking situated in the territory of that Member State even if, as a result of the division of tasks within the group, first, that establishment is responsible solely for the sale of advertising space and other marketing activities in the territory of that Member State and, second, exclusive responsibility for collecting and processing personal data belongs, for the entire territory of the EU, to an establishment situated in another Member State. Furthermore, the CJEU in Holstein (C-210/16) stated that according to Directive 95/46 where the supervisory authority of a Member State intends to exercise its powers of intervention (Article 28 (3) with respect to an entity established in the territory of that Member State, on the ground of infringements of the rules on the protection of personal data committed by a third party responsible for the processing of that data whose seat is in another Member State, that supervisory authority is competent to assess, independent of the supervisory authority of the other Member State, the lawfulness of such data processing and may exercise its powers of intervention with respect to the entity established in its territory without first calling on the supervisory authority of the other Member State to intervene.

Lastly, in the pending case TR v Land Hessen (Case C-768/21) the referring court asked as to whether, according to Article 57(1)(a) and (f), Article 58(2)(a) to (j) GDPR, read in combination with Article 77(1) thereof, where the supervisory authority finds that data processing has infringed the data subject's rights, the supervisory authority must always take action in accordance with Article 58(2) of that regulation.

6.2.3. Question 4: Duty of cooperation of national authorities regarding the possible invalidity of an EU act

Is the supervisory authority of a Member State able to examine the claim of a person concerning the validity of an act of the EU?

The main case that is to be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

➢ Judgment of the Court, (Grand Chamber), 6 October 2015, *Schrems* v. *Data Protection Commissioner*, C-362/14 (***Schrems I***)

Relevant legal sources:

EU Level

Article 28(3) Directive 95/46
Article 58 GDPR

The case and preliminary question referred to the Court:

The problem of the role of the supervisory authority *vis-à-vis* the role of the courts was not addressed directly in the preliminary questions referred in the *Schrems* case (C-362/14) (see description of the case in Chapter 1 on territorial scope). However, in order to identify which authority is responsible for ruling on the validity of a European act, the CJEU addressed, in detail, the duty of cooperation between a supervisory authority and a court.
In a follow-up case *Facebook Ireland and Schrems* which concerns a data transfer to the US on the grounds of standard contractual clauses, the High Court of Ireland referred to the Court, amongst others, a preliminary question whether a data protection authority is required to suspend data flows if a third country data importer is subject to surveillance laws and hence does not comply with the GDPR and the Charter. In the ruling the Court approached the duty to cooperate between national authorities and the courts, as well as general obligation to consider with all due diligence a complaint lodged by an individual on the grounds of Article 77 of the GDPR.

Reasoning of the Court:

In the implementation of an act of the EU, several actors, including national supervisory authorities and courts, may find a lack of compatibility of such act with the fundamental rights and freedoms. However, neither the supervisory authorities nor the courts have the power to declare an EU act invalid. The exclusive jurisdiction to rule on the validity or invalidity of an EU act lies with the CJEU. This is based on legal certainty and the uniform application of EU law.
Additionally, given the specific features of supervisory authorities, the latter do not fall within the definition of "tribunal" in Article 267 TFEU, thus they do not have the possibility of referring questions for preliminary rulings to the CJEU. As a matter of fact, though, the supervisory authorities constitute the first step in the evaluation of the validity of EU acts, and there must be cooperation between the supervisory authorities and the national courts in order to access the CJEU.
Therefore, the different actors may play different roles in the following scenarios:

1) an individual may present a claim before the national supervisory authority, claiming the incompatibility of an EU act with fundamental rights and freedoms. The national supervisory authority concludes that the claim is unfounded. Then, the claimant should, pursuant to Article 28(3) of Directive

95/46[32] read in light of Article 47 CFREU, have access to judicial remedies enabling him to challenge such a decision before the national courts. In this case, if the national courts do not share the evaluation of the supervisory authority and still have doubts regarding the compatibility of the EU act with fundamental right and freedoms, they must present a preliminary question to the CJEU.

2) An individual may present a claim before the national supervisory authority, claiming the incompatibility of an EU act with fundamental rights and freedoms. The national supervisory authority concludes that the claim is founded. Then the supervisory authority, pursuant to Article 28(3) of Directive 95/46[33] must, particularly, in light of Article 8(3) CFREU, be able to institute legal proceedings. In this case, the supervisory authority may put forward its doubts regarding the validity of the EU act, and if the national courts share them they will submit a reference for a preliminary ruling for the purpose of examining the decision's validity.

In *Facebook Ireland and Schrems* (C-311/2018) the Court confirmed that the formula introduced in *Schrems* (C-362/14) may be applied in the environment of the GDPR as well. In the ruling the Court shared the opinion of the Advocate General that the findings in *Schrems* regarding the duty to cooperate between national authorities and the courts may be applied by analogy to EU acts other than an adequacy decision, such as Decision 2010/87 on standard contractual clauses. The supervisory authorities are obliged to consider with all due diligence a complaint lodged by an individual on the grounds of Article 77 (1) of the GDPR.

According to the Court, if a supervisory authority takes the view, following an investigation, that a data subject whose personal data have been transferred to a third country is not afforded an adequate level of protection in that country, it is required to take appropriate action in order to remedy any findings of inadequacy, irrespective of the reason for, or nature of, that inadequacy. Furthermore, the Court confirmed the DPA's obligation to suspend or prohibit a transfer of personal data to a third country if, in its view, the standard data protection clauses cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer. In order to avoid possible divergences among the DPAs, the Court reminded that a supervisory authority may refer the matter to the European Data Protection Board which may adopt a binding decision.

In the case where the Commission has issued and adequacy decision, the Court confirmed that the DPAs cannot individually suspend or prohibit data flows to the third country in question until invalidation of the decision in question. However, the Court stressed that existence of an adequacy decision does not prevent individuals from lodging a complaint before the competent national supervisory authority under Article 77(1) of the GDPR. The DPA is then obliged to consider the complaint and exercise its powers with complete independence.

Subsequently, the Court followed reasoning of *Schrems* and opinion of the AG, confirming that in cases where there may appear doubts around the validity of an EU act, the DPA shall act under requirements of Article 58(5) of the GDPR and Article 8(3) of the Charter and initiate legal proceedings before national courts which further submit a reference for a preliminary ruling. This will concern Commission's adequacy decisions pursuant to Article 45 (3 and 5), decisions on the code of conduct (Article 40 (9) and.

Moreover, the question of a possible invalidity of the act of EU body may appear as well in the context of consistency procedures before the EDPB. Amongst others, the binding decisions issued by the Board

[32] In particular, Article 28(3) (in fine) provides that "Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts."

[33] In particular, Article 28(3) (last indent) provides that each authority shall be endowed with "the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities."

as a result of a dispute resolution may also be a subject of claims. Recital 143 to the GDPR explains that, following Article 263 TFEU, any natural or legal person has the right to bring an action for annulment of decisions of the Board before the Court. The right to challenge them makes the DPAs the sole addressees, and a controller, processor or complainant where the EDPB's decisions concern them directly.

Recital 143 further explains that the national court has no power to declare the Board's decision invalid and must refer the question of validity to the Court in accordance with Article 267 TFEU. A national court may not refer a question on the validity of the decision of the Board at the request of a natural or legal person which had the opportunity to bring an action for annulment of that decision, in particular if it was directly and individually concerned by that decision, but had not done so within the period laid down in Article 263 TFEU (see also the Introduction of this chapter).

7. Effective, proportionate and dissuasive sanctions and remedies

7.1. Introduction. Remedies and sanctions within the GDPR

What is the relationship between sanctions and remedies? Which authority can apply sanctions and which one can administer remedies? What are the procedural instruments of coordination when the administrative authority administers sanctions and the judicial body remedies?

The effective protection of natural persons concerning the processing of personal data calls for effective, proportionate and dissuasive sanctions and remedies against infringers of the data subjects' rights. In most Member States, the major focus has been on administrative sanctions, implemented by national supervisory authorities. However, the relevance of civil remedies should not be underestimated. The role of collective redress is also essential, even if not fully developed at the European level (see the box at the end of Chapter 8 and for a comparison of collective redress in consumer and data protection at the EU level, see Chapter 9). Within the GDPR the system of remedies and sanctions is highly articulated; the principle of effectiveness, proportionality, and dissuasiveness are of particular importance in its interpretation, as several provisions of the GDPR demonstrate.

With regard to **remedies,** the data subjects' rights are significant, considering that they shape an important set of remedies for granting the data subject the means for reacting against unlawful processing and exercising control over data concerning her. The **data subjects' rights** are the following: the right of access (Article 15 GDPR), the right to rectification (Article 16 GDPR), the right to erasure (Article 17 GDPR), the right to restriction of processing (Article 18 GDPR), the right to data portability (Article 20 GDPR), the right to object (Article 21 GDPR), and the right to not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, except for the exception provided for by Article 22 (2) GDPR.

Furthermore, Article 82 regulates the right to **compensation** of persons who suffered material or non-material damage as a result of an infringement of the GDPR. Such compensation, as expressly stated by Article 82 should be **effective** (see also recital 146, according to which compensation should be **full and effective**).

Furthermore, according to Article 58 GDPR, **Data Protection Authorities** have **investigative powers** (*e.g.*, to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or a Member State procedural law), **corrective ones** (*e.g.*, to impose a temporary or definitive limitation including a ban on processing; to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 GDPR; corrective powers include the power to impose an administrative fine) and **authorisation and advisory powers** (*e.g.*, to issue, on its own initiative or on request, opinions to the national parliament, the Member State's government). According to recital 129 of the GDPR those powers should be **effective**.

Moreover, the GDPR expressly states that **sanctions** must be **effective, proportionate, and dissuasive** (see Article 83, Article 84, recitals 151-152 GDPR). Article 83 GDPR identifies some criteria to be considered in determining the amount of administrative fines, such as the nature, gravity, and duration of the infringement taking into account the nature, scope, or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.

The GDPR partially regulates the **coordination between DPAs' corrective powers and the imposition of fines**. In particular, Article 83 GDPR provides that, depending on the circumstances of each individual case, administrative fines may be imposed in addition to, or instead of, the following corrective measures, provided for by Article 58 GDPR: i) issuing warnings to a controller or processor

that intended processing operations are likely to infringe provisions of this Regulation; ii) withdrawing a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met; iii) ordering the suspension of data flows to a recipient in a third country or an international organization. Furthermore, according to Article 83 GDPR a criterion for determining the amount of administrative fines is the existence of corrective measures referred to in Article 58(2) against the controller or processor concerned with regard to the same subject-matter and the compliance with those measures. This means that effectiveness, proportionality and dissuasiveness should be assessed taking into account the possible combination between fines and other corrective measures.
For sake of clarity in this Casebook we will use the term 'corrective measures' for measures different from fines, whereas the latter will be referred to as fine, sanctions or penalties.
As to the **role of judicial authorities,** in addition to what has already been said with respect to the powers of the administrative authorities pursuant to Article 58 GDPR, the data subject has the right to lodge a complaint with a supervisory authority (Article 77), and the right to an **effective judicial remedy** where they consider that his or her rights under the GDPR have been infringed as a result of the processing of their personal data in non-compliance with the GDPR (Article 79, recital 139 GDPR). Furthermore, according to Article 80 GDPR, collective redress should be available with an opt-in formula for the exercise of the data subjects' rights before DPAs and Courts. Moreover, Member States may choose to establish an opt-out class action for the exercise of data subject rights and an opt-in class action for exercising the right to compensation provided for by Article 82 (On collective redress see also the box at the end of Chapter 8 and paragraph XX of chapter 9).

Moreover, according to Article 83 GDPR, DPAs should have the competence of establishing administrative fines (in this respect, see also the introduction of chapter 6). Nevertheless, according to that provision, if the Member States' legal system does not provide for administrative fines, the fine may be initiated by the competent DPA and imposed by competent national courts, while ensuring that those legal remedies are **effective** and have an **equivalent effect** to the administrative fines imposed by DPAs. Considering the complexity of the system of remedies and sanctions drawn by EU data protection legislation, and that their application may have a significant impact on fundamental rights, the following question arises as a general question including more specific sub-questions along the chapter.

What is or should be the impact of Article 47 CFR, Article 19 TEU and of the principles of effectiveness, proportionality and/or dissuasiveness on the definition and the implementation of sanctions and remedies for violations of data protection carried out by administrative authorities and Courts? Does the application of the principles of effectiveness, proportionality and dissuasiveness differ when they are applied to sanctions or remedies?

Main questions addressed

1. What is the relationship between sanctions and remedies? Which authority can apply sanctions and which one can administer remedies? What are the procedural instruments of coordination when the administrative authority administers sanctions and the judicial body remedies?

What is or should be the impact of Article 47 CFR, Article 19 TEU and of the principles of effectiveness, proportionality and/or dissuasiveness on the definition and/or implementation of sanctions and remedies for violations of data protection carried out by administrative authorities and Courts? Does the application of the principles of effectiveness, proportionality and dissuasiveness differ when they are applied in interpreting sanctions or remedies?

2. In order to ensure an effective remedy, should data subjects be entitled to obtain the removal from the list of results displayed by a search engine of a particular operator, and from links to web pages published by third parties?
3. In order to ensure the effective protection of personal data within the EU and full compensation of victims, should courts award compensation for material and non-material damages for any infringement of EU data protection law regardless of whether specific harm is found to have been caused by the infringement?

4. How do the principle of effectiveness and Article 47 CFREU influence the array of full compensation in the case of unlawful collection and processing of data?

5. Which is the role of the principle of proportionality in the application of sanctions?

6. Which is the role of the principle of proportionality in applying the right to be de-listed, which stems from the right to erasure provided for by Article 17 GDPR?

7. What is the relationship between data protection/privacy and information to be provided to the data subject, considered the importance of the latter for the exercise of data subjects' rights? Do Article 47 CFREU and the principles of effectiveness and proportionality play a role in this regard?

Furthermore, the issues related to balancing multiple individuals' rights and Article 47 CFREU are addressed in a box at the end of the chapter.

Relevant legal sources:

EU Level
Charter of Fundamental Rights of the EU
Article 47 - Right to an effective remedy and to a fair trial

Directive 95/46 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 *(Act no longer in force, date of end of validity: 24/05/2018, repealed by Regulation (EU) 2016/679)*
Chapter II. General rules on the lawfulness of the processing of personal data; Article 12 - Right of access; Article 14 - The data subject's right to object; Article 22 - Remedies; Article 23 - Liability; Article 24 - Sanctions

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 (General Data Protection Regulation)
(In force since: 25/05/2018)

Article 13 - Information to be provided where personal data are collected from the data subject; Article 14 - Information to be provided where personal data have not been obtained from the data subject; Article 15 - Right of access by the data subject; Section III. Rectification and erasure; Article 16 - Right to rectification; Article 17 - Right to erasure ('right to be forgotten'); Article 18 - Right to restriction of processing; Article 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing

CHAPTER VIII. Remedies, liability and penalties
Article 77 - Right to lodge a complaint with a supervisory authority; Article 78 - Right to an effective judicial remedy against a supervisory authority; Article 79 - Right to an effective judicial remedy against a controller or processor; Article

80 - Representation of data subjects; Article 81 - Suspension of proceedings; Article 82 - Right to compensation and liability.

7.2. The impact of the principle of effectiveness on the system of sanctions and remedies drawn by the GDP

7.2.1. Question 1: The impact of the principle of effectiveness on remedies: the example of the right to "de-listing"

In order to ensure an effective remedy, should data subjects be entitled to obtain the removal from the list of results displayed by a particular operator search engine and, links to web pages published by third parties?

Within the following cluster of cases, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *G.C., A.F., B.H., E.D.* v *Commission nationale de l'informatique et des libertés* (CNIL), Case C-136/17 (***GC and Others)***

Cluster of relevant CJEU cases

➢ 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***)

➢ Judgment of the Court (Second Chamber), 26 July 2019, *Fashion ID Gmbh & Co.KG* v. *Verbraucherzentrale NRW EV*, Case C-40/17 (***Fashion ID***)

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *G.C., A.F., B.H., E.D.* v *Commission nationale de l'informatique et des libertés* (CNIL), Case C-136/17 (***GC and Others)***

➢ Judgement of the Court (Grand Chamber), 24 September 2019, *Google LLC v. Commission nationale de l'informatique et des libertés* (CNIL), C-507/17 (***Google v. CNIL***)

➢ Judgment of the Court (Third Chamber) of 3 October 2019, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, C-18/18

➢ Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 24 September 2020 — *TU, RE v Google LLC*, Case C-460/20 (**TU, RE v Google LLC**) [pending]; AG Opinion, 7 April 2022

➢ Request for a preliminary ruling from the Hof van beroep te Brussel (Belgium) lodged on 2 March 2021 — *Proximus NV v Gegevensbeschermingsautoriteit*, Case C-129/21, (**Proximus**) [pending]

Relevant legal sources

EU Charter of Fundamental Rights

Article 8 Right to data protection; Article 7 right to a private life; Article 11; Freedom of expression; Article 52 Scope of guaranteed rights

EU Regulation (EU) 2016/679 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)

Article 17 Right to erasure ('right to be forgotten')

The case and relevant legal sources:

GC, AF, BH and ED requested Google to de-reference in the list of results displayed by the search engine operated by Google in response to searches against their names various links leading to web pages published by third parties.

Google refused to comply with the users' request. Then, the data subjects brought complaints before the CNIL, seeking for Google to be ordered to de-reference the links in question. By letters dated 24 April 2015, 28 August 2015, 21 March 2016 and 9 May 2016 respectively, the president of the CNIL informed them that the procedures on their complaints had been closed. The applicants sought an action before the French Council of State against those refusals of the CNIL to serve formal notice on Google to carry out the de-referencing requested.

Preliminary question(s) referred to the Court:

Several questions were referred by the CJEU.

In its first question, the referring court essentially asks whether the prohibition or restrictions relating to the processing of sensitive data apply also, subject to the exceptions provided for by the directive, to the operator of a search engine in the context of his responsibilities, powers and capabilities as the controller of the processing carried out for the needs of the functioning of the search engine.

The other questions concerned the scope of the obligations of the search engine, in relation to the type of data (sensitive and judicial data), and the purposes of the processing.

Reasoning of the Court:

The CJEU, relied on its previous case law and specifically on *Google Spain* (C-131/12), a leading case with regard to the "de-listing" and the role of the principle of effectiveness in shaping remedies. In the present case, the Court stated that in so far as the activity of a search engine is liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as a controller (*i.e.*, the person determining the purposes and means of processing) must ensure that the processing meets the requirements of data protection laws in order that the guarantees laid down by that legislation may have full effect and that "**effective and complete protection of data subjects**, in particular of their right to privacy, may actually be achieved".

Then, the CJEU, relying on its previous case law affirmed that, in order to respect data subjects' rights the operator of a search engine is obliged to remove from the list of results appearing as a result of a search carried out on the basis of a person's name, links to web pages, published by third parties and containing information relating to that person, even where that name or that information is not previously or simultaneously deleted from the web pages in question, and that may be the case even where their publication on those web pages is in itself lawful.

Furthermore, the Court affirmed, in light of her fundamental rights under Articles 7 and 8 CFR, that when the data subject, request that personal data concerning her no longer be made available to the general public on account of its inclusion in such a list of results, the right to the protection of personal data and the right to a private life override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. Nevertheless, the CJEU stated that that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his or her fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.

The Court expressly referred to Article 17 GDPR concerning the right to erasure and the right to be forgotten, interpreting it in light of fundamental rights and the principle of proportionality (see, in this chapter, Question 7), and specifically the right to information (see also in this respect, Chapter 5).

Conclusion of the Court:

The CJEU stated that the prohibition or restrictions relating to the processing of special categories of personal data, apply also, subject to the exceptions provided for by data protection laws, 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**, on the occasion of a verification performed by that operator, under the supervision of the competent national authorities, following a request by the data subject.

Furthermore, according to the CJEU, the operator of a search engine is in principle required to answer to requests for de-referencing in relation to links to web pages containing sensitive data. Nevertheless, the refusal to answer to the request for de-listing of the search engine could be justified by the fact that the processing is lawful, considering the exceptions to the prohibition of processing provided for by EU law, and interpreting these exceptions in light of fundamental rights (with regard to the role of freedom of expression and the balance of that freedom with the right to data protection and to a private life see Chapter 5, §XX).

Impact on the follow-up case:

Council of State, 6 December 2019, No. 401258.

Regarding the "right to de-referencing" of personal data relating to criminal proceedings, the Council of State stated that the provisions of Article 46 of the Law No. 78-17 of 6 January 1978 ensure the implementation in national law of those of Article 10 of the GDPR, which repealed and replaced those of Article 8(5) of Directive 95/46/EC of 24 October 1995. Expressly relying on *GC and Others* (C-136/17), the Council of State affirmed that the two links still in dispute led to web pages containing the words spoken by the applicant in an interview he gave to a magazine with a large circulation about her conviction. Then, the French judge considered that these pages therefore contain information which constitutes personal data relating to the criminal proceedings and that **the interference with the fundamental rights to privacy and protection of personal data of the data subject is likely to be particularly serious because of the sensitivity of such data.** Accordingly, the Council of State affirmed that that it is in principle the responsibility of the CNIL, upon receiving a request for it to give formal notice to the operator of a search engine to de-list links to web pages published by third parties and containing such data, to comply with this request. For an analysis of the impact of the principle of proportionality within the interpretation of criteria to be adopted, according to the Council of State, for balancing fundamental rights at stake, see Question 7 in this chapter.

Elements of judicial dialogue:

GC and Others (C-136/17) followed a leading case on the right to be de-listed: *Google Spain* (C-131/12; for an explanation of the judgement see the Guidelines on the implementation of the CJEU judgment in *Google Spain*" adopted by Article 29 Data Protection Working Party (WP29) in 2014: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf; see also the RE-JUS data protection Casebook, Chapter 6, Question 1 available at: https://www.rejus.eu/sites/default/files/content/materials/rejus_casebook_effective_justice_in_data_protection_.pdf).

In this judgement, the CJEU stated the that the operator of a search engine is a controller within the meaning of EU legislation. Accordingly, the data subject may exercise her rights against that operator, and in certain circumstances, and particularly following a balance of interests, the data subject has a right to be de-listed from the list of results displayed by a search engine. According to the CJEU, such a right can notably also be asserted against the operator of the search engine in a case where the name or

information is not erased beforehand or simultaneously from the web pages to which the list is linked, and even when the publication on those pages was lawful. The data subject may ask to be de-listed on the grounds that the information relating to him should, given the time elapsed since the publication, no longer be linked to his name, unless it should appear that, given the role played by the data subject in public life, such interference with their fundamental rights is justified by the preponderant interest of the general public in having access to the information in question. The Court thus concludes that supervisory or judicial authorities may order the operator of the search engine to remove links to web pages published by third parties containing information relating to a person from the list of results displayed following a search made on the basis of that person's name, without an order to that effect presupposing the previous or simultaneous removal of that name and information — of the publisher's own accord or following an order of one of those authorities — from the web page on which they were published. For the Court, such right to be de-listed is driven by ***the principle of effectiveness***, since, given

"the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, **effective and complete protection of data users** could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites".

With regard to the extension of the controllers' obligations, according to *Google v. CNIL* (C-507/17), the fact that the search engine is operated by an undertaking with seat in a third State does not exempt the controller form the obligations and guarantees laid down by Directive 95/46 and Regulation 2016/679 when processing of personal data for the purposes of that search engine's operation is carried out in the context of the advertising and commercial activity of an establishment of the controller in the territory of a Member State (see, in this respect, Question 1a of Chapter 1).

Furthermore, in relation to the pending case *TU, RE v Google LLC* (C-460/20) the AG in its opinion affirmed that according to Article 17(3) GDPR:

- within the context of the weighing-up of conflicting fundamental rights arising from Articles 7, 8, 11 and 16 CFREU, which is to be undertaken within the scope of the examination of a request for de-referencing made to the operator of a search engine on the basis of the alleged false nature of the information which appears in the referenced content, it is not possible to concentrate conclusively on the issue of whether the data subject could reasonably seek legal protection against the content provider, for instance by means of interim relief. In the context of such a request, it is incumbent on the data subject to *prima facie* provide evidence of the false nature of the content the de-referencing of which is sought, where that is not manifestly impossible or excessively difficult, in particular with regard to the nature of the information concerned. It is for the operator of the search engine to carry out the checks which fall within its specific capacities, contacting the publisher of the referenced web page, where possible. Where the circumstances of the case so indicate in order to avoid irreparable harm to the data subject, the operator of the search engine will be temporarily able to suspend referencing, or in search results to indicate that the truth of some of the information in the content to which the link in question relates is contested,.
- within the context of the weighing-up of conflicting rights and interests arising from Articles 7, 8, 11 and 16 CFR, in connection with a request for de-referencing made to the operator of a search engine seeking to obtain the removal, from the results of an image search carried out on the basis of a natural person's name, of photographs displayed in the form of thumbnails depicting that person, account should not be taken of the context of the publication on the internet in which those thumbnails originally appear.

Moreover, the judgement *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (C-18/18) is of particular interest. In that case, the CJEU addressed the question if the extension of the duties of host providers to remove unlawful information, under Article 15 of Directive 2000/31. In that regard, the CJEU stated that that provision does not preclude a court of a Member State from:
i) ordering 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;
ii) ordering a host provider to remove information which it stores, the content of which is 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 by 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, and
iii) ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.
In that case, the Court stated that in order for an injunction which is intended to bring an end to an illegal act and to prevent it being repeated, in addition to any further impairment of the interests involved, to be capable of achieving those objectives **effectively**, that injunction must be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal. The Court affirmed that otherwise, the effects of such an injunction could easily be circumvented by the storing of messages which are scarcely different from those which were previously declared to be illegal, which could result in the person concerned having to initiate multiple proceedings in order to bring an end to the conduct of which he is a victim.
Lastly, in the pending case *Proximus* (C-129/21) the referring Court asked to the CJEU whether Article 17[(2)] GDPR must be interpreted as precluding a national supervisory authority from ordering a provider of public directories and directory enquiry services which has been requested to cease disclosing data relating to an individual to take reasonable steps to inform search engines of that request for erasure. In this respect, the data subject's right to an effective remedy in relation to the right to erasure could play a role in the future CJEU's reasoning, jointly with the principle of proportionality (see Section XX of this Chapter).

Impact on national case law in Member States different from the state of the court referring the preliminary question to the CJEU:

France[34]
The French case-law before *Google Spain* recognised that the *Google Suggest* service can constitute an offence under press law, when it offers suggestions about a person or a company that can cause prejudice to them[35]. There, judges ruled that the *Google Suggest* algorithm is not automatic, owing to the possibility for Google to ban certain terms or content from its product. Yet, the interpretation of the

[34] Drafted by the students of Master PIDAN (UVSQ)

[35] *TGI* Paris, 15 February 2012, *Kriss Laure/Larry P, Google Inc*

Cour de cassation goes against the decision of the courts of first instance[36], which considered that this service is automated, and thus that *Google* cannot be liable for unlawful content put forward via *Google Suggest*.

After Google Spain, French case law tends to verify the **proportionality** of the rights in issue. There, judges examine the balance between the legitimate interest of the public to know the information published and referenced, and the right of data subjects to data protection.

For this purpose, tribunals and courts examine the veracity, the date of publication, the intimacy and the prejudicial aspect of personal data disclosed[37]. For instance, when an issue concerns the functioning of public institutions, the de-listing would be an infringement of freedom of expression.[38]

For example, a judgment of the *Tribunal de Grande Instance de Paris* refused to order Google to de-list URLs leading to publications concerning the conviction of a doctor, sentenced on 23 December 2015. There, those Internet links allowed the public to be informed about a criminal case that resulted in a significant conviction. Otherwise, the referencing concerned accurate information on a recent event. The processing could not have become inadequate or irrelevant. A balance of interest was preserved between the rights of the person concerned and the legitimate interest of Internet users in expression and information.[39]

The Tribunal uses the same reasoning as the CJEU in the *Google Spain* case but adds that requests to be de-listed are only possible if the search engine has previously been approached and has unlawfully refused.

Judicial tribunals and courts directly refer to the *Google Spain* decision to examine whether the operator of a search engine must be ordered to de-list URLs. The judges specify that Articles 38 (right of opposition for legitimate reasons concerning the processing of personal data) and 40 (rectification or erasure of personal data that is inaccurate, equivocal or outdated) of the Law of 6 January 1978[40] must be interpreted accord to the case law of the CJEU.[41]

One decision by the *Cour de cassation*[42] examined a decision of a court of appeal that considered that a newspaper publisher cannot be forced to delete the reference to a publication on its website, or to make it unaccessible. Thus, the *Cour de cassation* admitted that imposing a modification of the normal reference of a newspaper publisher goes beyond limitations on the freedom of the press. Thus, it seems clear that the right provided under the *Google Spain* case can only be claimed against a search engine provider, and not a newspaper publisher.

---

[36] *C. cass. civ. 1ère*, 19 June 2013, no 12-17.591

[37] See for example, TGI Paris, ord. réf., 24 November 2014; TGI Toulouse, ord. réf. 21 January 2015, Franck J. c.. SARL Google France et Google Inc., légipresse 2015, no 324, p. 107; TGI Paris, ord. réf. 24 November 2014, David T.SA Google Inc., légipresse 2015, no 326-15, p. 209; TGI Paris, ord. réf. 13 May 2016, M. x c. Google France et Google Inc.; TGI Paris, ord. réf. 12 May 2017, Mme. X c. Google France et Google Inc., RLDI, no 138, 1 June 2017. On this issue, see also Anne DEBET, « Mise en oeuvre de Google Spain par les tribunaux français », in Comm. com. électr., no 9, September 2016, comm. 75

[38] In this connection see, *Cour d'appel de Paris*, 28 May 2014, where a judge condemned for corruption asked for the de-listing of a press article on the website of the press editor

[39] *TGI* Paris, 10 February 2017, *M. X c/ Google France, Google Inc.*

[40] *L. n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*

[41] See for example, *TGI* Paris, 10 February 2017, *M. X c/ Google France et Google Inc.*; CA Lyon, 8th chamber, 28 February 2017, RG no 15/05788.

[42] *C. cass., ch. civ. 1ère*, 12 May 2016, no 15-17.729

It can be considered that the decision of the *Cour de Cassation* demonstrates that de-referencing can only be imposed on a search engine, and cannot be applicable to the people generating the information. This is based on the principle that the modification of a normal reference in a press organ (website archives) goes against the freedom of the press, even though an infringement could undermine the rights of a person who would be justified in asking for the de-listing of the press article highlighted by a search engine.

Judges also use the same construction as in the *Google Spain* case. They consider that a search engine provider cannot be liable for defamatory statements contained in links it has referenced.

The French decisions have also ruled that Google France, the French establishment of Google Inc., is to be held responsible for the data processed by Google Inc., after an economic analysis of the activities of the French establishment.[43]

French administrative courts also hear cases concerning the de-listing of personal information. In this regard, the assembly of the *Conseil d'État* directly refers to the Google Spain case.[44] Judges were required to examine the refusal of Google Inc. and the French administrative authority to de-list several links redirecting to websites concerning personal data of data subjects. The *Conseil d'État* first recalls that the right to be de-listed is recognized by the *Google Spain* case, as the right to seek the removal by a search engine provider of information that could infringe privacy, reputation and personal data protection. Here, the courts emphasise that this right is not absolute and can be balanced by the right to information.

Confronted with several issues of interpretation, the *Conseil d'État* asked for a preliminary ruling by the European Court of Justice, seeking clarification of the obligations of search engine providers to de-list, notably concerning sensitive data, which were not covered by the *Google Spain* judgment. It did not discuss whether there should be an automatic de-listing of sensitive data.

In the same way, the *Conseil d'État* also submitted several questions for preliminary ruling to the CJEU, before deciding whether Google must 'de-list' information on all extensions of its search engine, or in some countries only.[45] In this case, the French data protection authority ordered Google to apply the removal to the list of results obtained from a search, and also to all extensions of Google's domain name.

Yet French judges have allowed some exceptions. The *Conseil d'État* (*Conseil d'État, sous- sections 2 et 7, 15 février 2016, n°389140*) considered that a decree establishing a procedure to block access by Internet users to websites with child pornography or which encourage terrorism, is justified by legitimate interests. There, the decree allows an administrative authority to ask the publisher or website host to de-list the unlawful content.

Still, even if courts allow injunctions against a publisher of content or against a website host, the de-listing only applies to illegal content, not content referring to personal information, such as in the *Google Spain* case.

<u>On other types of remedies:</u> *Cour de cassation*, commercial chamber 25 June 2013, no 12-17037:

Even if the law does not expressly so state, the sale of a file including personal data that has been unlawfully collected and processed (no declaration to the French data protection authorities) is void since the object of the sale -- the undeclared processing of data -- is unlawful and thus cannot be seen as being available for trade.

---

[43] *TGI* Paris, 16 September 2014, *M. et Mme. X et M. Y c/ Google France*

[44] See, for instance, *Conseil d'État*, plenary session, 24 February 2017, *Mme. Chupin et autres*, no 391000; *Conseil d'État,* 19 July 2017, *Google Inc.*, no 399922

[45] *Conseil d'État*, 19 July 2017, *Google Inc.*, no 399922

This decision implicitly relies on the principles of effectiveness and dissuasiveness since it deprives a file including unlawfully processed personal data of any commercial interest. From the perspective of the principle of effectiveness, a parallel issue arises as to whether invalidity of a contract represents an adequate remedy as an *ex post* measure where it might not prevent the material transfer of data, albeit subject to subsequent "restitution". Indeed, data protection is a field in which the civil remedies normally applied to market transactions may fail to effectively protect the personal interests at stake.

Italy[46]

The Italian case law before *Google Spain* appeared to be fairly strict in assessing the obligations owed by search engine providers. Such providers were indeed regarded as mere "intermediaries", which could not be held responsible for the processing and publishing of personal data by the "source websites". Thus, the obligation to ensure that the data processing was in accordance with the relevant legal provisions rested only on the shoulders of the publishers of the data (i.e., the source websites).[47]

By contrast, Italian case law after *Google Spain* unanimously embraces the view, upheld by the CJEU, that search engine providers must be regarded as data controllers. Moreover, when the provider has its own subsidiary set up in a Member State, which only engages in marketing activities and thus not the finding, indexing and storing of information on the internet — which are instead carried out by the parent company situated outside the EU – such provider can nevertheless be regarded as subject to EU law[48] according to Article 4 of Directive 95/46. It is worth mentioning, nonetheless, that the Italian decisions based their reasoning also on the circumstance that the NDPA decision of 10 July 2014, referring to an official 2010 determination by Google Inc., ruled that Google Italy S.r.l., should be considered as the Italian representative of Google Inc., for the purposes of the legislation concerning data protection (i.e., Legislative Decree no 196/2003).

The Italian case law also contains an interesting development with regard to the obligations owed by an internet service provider (ISP) such as the manager of a social network service (i.e., Facebook) employed by third parties to process and publish personal data (the so-called "hosting providers"). A decision from an Italian court[49] ruled that, whereas Directive 2000/31 on electronic commerce — to which ISP are subject — explicitly excludes the liability of the provider engaging in activities of *mere conduit*, caching and hosting, the provider must instead be regarded as liable when, after being informed of the publishing, on its own hosting platform, of information not compliant with the data protection provisions, it does not ensure, even without a specific order from the authorities, that such information is removed. In other words, while there is no *ex ante* obligation on the ISP to control the content of the information published, a proper balancing between the right to information and the right to data protection, as laid out by the CJEU in *Google Spain*, can only occur when the provider plays an active role, thus intervening, *ex post*, in order to remove information not compliant with the data protection legislation and contested by the data subjects. As a consequence, it should be pointed out that the Italian

---

46 Drafted by Gianmatteo Sabatino and by C. Angiolini

47 See Court of Cassation, decision no 5525/2012

48 See, in particular, Milan *Tribunale*, decision of 5 October 2016 and decision no 618 of 2014 of the Italian National Data Protection Authority. Both decisions upheld that Google Italy S.r.l. could indeed be considered as representative of Google Inc. in Italy. On the issue, see also RICCIO, *Il difficile equilibrio tra diritto all'oblio e diritto di cronaca*, in *Nuova Giur. Civ.*, 2017, 4, 549.

49 North Naples Tribunal, decision of 3 November 2016.

courts have devised a "double level of protection"[50] for subjects whose data is published on the internet and indexed by search engines: on the one hand these subjects can directly ask the Internet Service Provider (such as a search engine provider) to prevent personal data from being too easily accessible to the public and, as already pointed out, this request will be fulfilled by removing the websites containing contested information from the results displayed by inserting the data subject's name in the search engine research bar[51]; on the other hand, any complaint regarding the erasure, removal or adjustment of information must be addressed to the publisher of such information,[52] since that is the party solely responsible for the content of the information displayed.

Moreover, the Court of Cassation in its decision n. 19681/2019, expressly mentioning *Google Spain* (C-131/2012) affirmed that with regard to the relationship between the right to be forgotten and the right to the historical evocation of facts and events concerning past events (as part of the freedom of expression), the mention of personal data concerning persons who were protagonists of those facts and events is lawful only in the hypothesis in which that information refers to people whose activities in the present moment is in the interest of the community, both for reasons of fame and for the public role covered. Otherwise, the right of the interested parties to confidentiality with respect to past events that may hurt them in dignity and honour and of which the collective memory is now extinguished would prevail.

The Court of Cassation, in its decision n. 9147/2020, relying on *Google Spain* (C-131/12) and on *GC and Others* (C-136/17), stated that the right to be forgotten consists in not being exposed without time limits to a representation of one's person that is no longer current, with prejudice to reputation and confidentiality, due to the republication, after an important time interval, of a piece of news relating to past events. The Court pointed out that the protection of the mentioned right has to be balanced with the public interest to the knowledge of the fact (freedom of expression), also considering the need of preservation of the news for historical-social and documentary purposes. Furthermore, the Court stated the result of the above mentioned balance may the de-listing of the article from a search engine, without the erasure from the newspaper webpage. In this respect, in its decision no. 15160 of 31 My 2021, the Court of Cassation, relying on European case law, stated that the right to be forgotten must be considered in strict connection with the rights to privacy and personal identity and that in balancing the public interest in information and personality rights, the former becomes recessive when the information is illicit, false, or unsuitable to provoke or feed a debate on events of public interest, for historical, scientific, health or national security reasons (this last requirement requires the quality of public character of the subject to whom the events in question refer. In the absence of at least one of these requirements, the conservation of the information in the database is unlawful, and the data subject may request for the erasure of the data, to which the service provider is obliged to give effect. Furthermore, the Court stated that where there is a public interest in the news, the data subject, whose data are not indispensable for the purposes of the accessibility of the news on the database, can request

---

[50] See RUSSO, *Diritto all'oblio e motori di ricerca: la prima pronuncia dei tribunali italiani dopo il caso Google Spain – Il commento, in Danno e Resp.*, 2016, 3, 299.

[51] The connection between the results displayed and the name inserted in the search bar must be interpreted broadly: for instance, when a web page containing contested information is displayed as a result of inserting in the search bar the name of the data subject plus some additional related terms, the request for the removal of such results is still admissible and can be scrutinised and upheld by the NDPA or a Court when the ISP does not comply. On this issue, see Italian NPDA decision no 277 of 15 June 2017.

[52] See Rome *Tribunale*, decision of 3 December 2015.

and obtain the "de-indexing", thus balancing freedom of expression with personality rights (On balancing fundamental rights at stake see also: Cass., No. 7559/2020; Cass. No. 19 May 2020 no. 9147). Moreover, regarding the data subject's request, in its decision no 20861, 21 July 2021, the Court of Cassation stated that the request for de-indexing requires the precise identification of the search results that the plaintiff intends to remove, and therefore, normally, the indication of the URL, of the contents relevant for this purpose, even if it is not excluded that a precise representation of the single information that is associated to the keywords may prove, according to the circumstances, suitable to give precise knowledge of the thing that is the object of the request, so as to allow the defendant to provide adequate and precise defences on the point.

Furthermore, on the basis of what the CJEU established in *Manni* (decision of 9 March 2017, C-398/15), the Court of Cassation, in its decision no 19761/2017, considered that with the establishment of the business register and the exclusion of a rule of exception, as required by the CJEU, the Italian legislature had achieved a correct balance between individual and collective needs. Therefore, the Court upheld the legitimacy of registering and retaining in the register information relating to the role of administrator and liquidator performed by a person in a company, even if the company went bankrupt and was struck from the register, as the requirements of business registration must prevail over the private interest in preventing its functioning, and also to satisfy the need for certainty in commercial relations addressed by the setting up of the business registry. The decision expressly refers to the *Google Spain* judgment and to the provisions of the ECHR.

With regard to *Eva Glawischnig-Piesczek* (C-18/18) the decision of the Tribunal of Milan with regard to the appeal against the order no. 15584 issued on 10.5.2019 by the Italian DPA is of particular interest. In that case, the Tribunal, relied on the CJEU case C-18/18. The Italian court, with reference to the identification of the person required to delete the data, considered that Facebook Ireland provides hosting services in accordance with Article 14 of Directive 2000/31, and that the purpose of Article 14(1) of the directive is to exempt the hosting service provider from liability if it meets one of the two conditions listed in that provision, namely a) not being aware of the unlawful activity or information, or b) acting immediately to remove such information or to disable access to it as soon as it becomes aware of it. The Court stated than that according to Article 14(3) of Directive 2000/31, read in light of recital 45 thereof, this exemption is without prejudice to the possibility for national courts or administrative authorities to require the hosting service provider concerned to bring an infringement to an end or to prevent it, including by removing or disabling access to the unlawful information. Therefore, the Court, relying on *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, (C-18/18) ordered Facebook Ireland Ltd to remove and block all unlawful Facebook posts containing personal data relating to children.

POLAND

Typically, claims for content removal arising from the online publication of personal information are based not on the data protection law, but rules on infringement of personality rights (Article 23 and 24 of Polish Civil Code). Under these provisions the person can request removal (or de-listing) of the content (also personal data) from e.g., a given online platform.

However, there are numerous issues — both related to the procedural technicalities and the court's approach — that undermine the effectiveness of such a claim in practice.

The optimal starting point for the analysis of Polish case law related to the right to be forgotten is the case of Tadeusz Węgrzynowski and Szymon Smolczewski ended by judgment of the ECtHR of 16.7.2013 (Action no. 33846).[53] The dispute started with a publication of article which caused damage to the

[53] In the case the judicial dialogue between Polish national courts and European courts (namely: European Court of Human

reputation of the applicants. After winning a case against the journalists who wrote the text Mr Węgrzynowski and Smolczewski found that it was still accessible on journal's website and requested its removal. Polish courts dismissed the claim due to the *res indicata* principle. However, it was underlined that removal of the article would amount to censorship and to rewriting history and was not justified anyway — in such a case it would be appropriate to supplement the text with a link to the information on the first judgement. This manner of balancing between the rights guaranteed under Article 10 (freedom of expression) and under Article 8 (right to respect for private life) of the Convention was approved by the ECHR.

A similar approach was adopted in the Judgement of Court of Appeal in Warsaw, I ACa 74/14, issued shortly after CJEU's award in *Google Spain*.[54] The court ascertained that the publisher of the website does not have to remove from it the archival publication containing outdated and unflattering information about the person who requests it. Accepting such a way would in fact be an unlawful form of censorship and interference with the autonomy of the press, expressed in the possibility of collecting and archiving journalistic materials.

The next judgement of the right to be forgotten in the online environment illustrates how problematic its realisation might be.[55] In this case the applicant requested the defendant to "take steps to remove a telephone recording from web portals, including in particular requesting the owners or administrators of portals for this purpose". His request, however was not granted due to the fact that its imprecision rendered its execution impossible.

The analysis of the judgement allows to identify what are the main **practical obstacles of the application of the right to be forgotten** in case of online materials according to the Polish judiciary.[56] The first difficulty lies in the accuracy of the claim request as well as the precision[57] and independence of the decision on that request, the second — editing the operative part of the judgment in a way that enables its concretisation by either party; deciding when the behaviour of third parties, not controlled by the defendant, can be seen as a result of the violation of the good by the latter (e.g., sharing content by others); determining the activities that the plaintiff may require under Article 24 of the Civil Code (what can be classified as a measure to remedy the effects of the infringement). Yet another issue is the liability limitation of the entities intermediating in sharing content provided by the rules on online service providers.

A change in the manner of approaching claims related to the right to be forgotten is to be observed in the judgement of Supreme Administrative Court, I OSK 2926/13, 9 April 2015,[58] which — in contrast to the previous judgements — explicitly refers to the ***Google Spain*** case. The claim was lodged against an operator of an internet browser, which allows to access entry to an online encyclopaedia on the

---

Rights can be observed. https://trybunal.gov.pl/uploads/media/Sprawa_Wegrzynowski_i_Smolczewski_przeciwko_Polsce__skarga_nr_33846_07___wyrok_z_dnia_16_lipca_2013_r..pdf

[54] 17 June 2014. http://orzeczenia.waw.sa.gov.pl/content/$N/154500000000503_I_ACa_000074_2014_Uz_2014-06-17_001.

[55] Judgement of Supreme Court, II CSK 747/13, 14 January 2015.

[56] See : B. Baran, K. Południak-Gierz, Perspektywa regulacji prawa do bycia „zapomnianym" w Internecie. Zarys problematyki, Zeszyty Naukowe Towarzystwa Doktorantów UJ Nauki Społeczne, No 17 (2/2017), p. 139-159. https://depot.ceon.pl/bitstream/handle/123456789/13711/Baran,%20Po%20udniak-Gierz%20Perspektywa%20regulacji%20prawa%20do%20bycia%20zapomnianym.pdf?sequence=1

[57] This issue appeared also in the Judgement of Court of Appeal in Warsaw, 15 February 2017, VI ACa 1935/16. In the opinion of the regional court, the request to remove the articles from the defendant's website was unfounded, since the entire publication could not be considered as prejudicial to the plaintiff's personal rights — the plaintiff should have indicated relevant fragments of the article in his request.

[58] https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/i-osk-2926-13-wyrok-naczelnego-sadu-administracyjnego-522555584.

claimant (the latter has not been generated by the browser operator). The court addressed the issue of the territorial scope of the right to be de-listed. It ascertained that — under the Google Spain doctrine — the geographic "location" of data or its processing cannot affect the possibility to claim that this data is removed from the search results. Thus, storing data on a server located abroad neither excludes Polish jurisdiction nor influences the applicability of the right to be forgotten. The Court underlined that it should be verified whether the processing of data cannot be understood as "creation of such technical premises, that make it *de facto* possible to get access to personal data without their physical retention." By this the Court reinforced the view that trans-border data processing can take a form of analysis and display of data — it is not necessary to determine the physical (geographic) location of the data storage. This line of reasoning was followed in the subsequent judgement (Judgement of Court of Appeal in Warsaw, 27 August 2015, II SA/Wa 900/15), in which the case was re-examined. The fact that the data processed are not stored by the processing entity does not in itself exclude the possibility of recognising this entity as their administrator as it would allow to easily circumvent data protection law.

Another issue is that **the removal claims are in Poland mostly based on the rules on personality rights which are not appropriate to guarantee personal data protection**. Here, the key judgement was issued by the common court (see: Judgement of District Court in Warsaw, 12 October 2015, I C 1164/13). Here the claimant requested obliging the defendant to remove the consequences of the violation of the plaintiff's personal rights by ceasing to display in the search engine — after entering the name, surname and place of residence of the plaintiff — a link to a particular website and a fragment of press material appearing at the indicated reference. The way of display of data suggested that claimant is a gangster whereas he participated in crushing a criminal group, which was obvious from the text to which the link lead. Though the claim was based on the personality rights protection regulation (Article 23 and 24 of Polish Civil Code), the court underlined that the functioning of a search engine operator is based on personal data processing and, thus, the operator can be considered to be the data controller within the meaning of the Article 2 letter d of the directive 95/46. The premises of claims related to the infringement of personality rights are as follows: either the infringement of personality rights or their endangerment, and illegality (understood as being contrary to the legal order or principles of social coexistence) of the infringer's actions. In the case at hand defendant's actions could not have been considered illegal. When the user enters the search into the search engine window, the search engine identifies and displays search results at specific positions according to its own algorithms that have been developed to identify relevant and useful search results. Shaping the content of links and descriptions (snippets) from search results lies primarily with entities administering websites displayed on search results lists. The search results and snippets therefore do not contain any statements from the search engine operator. Thus, the defendant cannot be held responsible for thereof. Secondly, the infringement of personality right of the claimant was not significant and temporary. In light of the above, the claim was dismissed by the court of the first instance.

The court of appeal, basing on the ***Google Spain*** judgement, challenged this way of reasoning,[59] underlining that the fact that the search results create a negative picture of the person, while the article towards which the link leads does not, is sufficient to conclude that the search results infringe claimant's personality rights (reputation). Though the display for search results for a phrase containing the name, surname and place of residence of the plaintiff was lawful, and the publication of the article itself did not infringe the plaintiff's personal rights, it was still justified to request removal of a particular link from the displayed list of search results, especially that the search results infringed his reputation. Secondly, the search engine operator, by setting the mechanisms of search results display, can be held liable for thereof (as the personal data controller) and is obliged to remove a link in question if processing of personal data is contrary to the data protection regulation. Not fulfilling this request rendered his behaviour illicit in

[59] Judgement of Court of Appeal in Warsaw, I ACa 2462/15,3 April 2017.

light of the Article 23 of Polish Civil Code. Finally, the removal of links should not be seen as a censorship, but as a proportionate remedy for personal rights infringement.

The dispute reached the third instance and was sent by the Supreme Court for re-examination after GDPR came into force.[60] The focal point of the justification of the award is **the interplay between the personality rights and personal data protection regimes**. The personal data are not personality rights, though can be seen as elements of the identity and privacy. Due to the relationship between personal data and some personality rights, the application of the provisions on the protection of personality rights may, in certain situations, ensure protection of personal data, and *vice versa*. However, this does not change the fact that the person seeking protection under Articles 23 and 24 (and 448 in case of compensation) of Polish Civil Code must prove that its requirements are met. The fact that, when the redress is sought within personal data protection regime — in light of the *Google Spain* judgement "the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful" does not mean that the same scope of protection can be obtained by a person who asserts claims against the internet search engine operator in the regime of personality rights protection identifying the infringed right as the reputation, not privacy. The Court did not observe infringement of the former, as it ascertained that the content displayed as a search result, though suggesting that the claimant was a gangster did not have a negative impact on his good name and reputation, as the Internet users are aware of the automatic way of functioning of the browser and does not attribute value to the snippets but verify the information on the page to which the link leads. Thus, the judgement of the Court of Appeal was set aside and the case was submitted for re-examination.

The interplay between the data protection rules and protection of personality rights regulation was also addressed in the judgement of Court of Appeal in Warsaw, I ACa 1565/15, issued on 25 November 2016.[61] Firstly, the court underlined that these protective regimes are independent from each other. In order to verify whether the publication of personal data constitutes an infringement of personality rights (in this case: reputation) and therefore justifies removal or compensation claim, it is crucial to prove that the information is false or outdated. In contrast, this might not be necessary when the person bases their claim on the data protection rules. Also, the fact that personal data is processed without the consent of the person concerned does not in itself constitute the infringement of personal rights and protection under Article 23 and 24 of Polish Civil Code. Finally, in light of the provisions on the liability of provider of electronic services, the Internet operator's liability for processing or storing unlawful personal data is excluded unless he knew that the data processing was illegal.

Another matter which caused difficulties to the Polish courts **was establishing the person against which the delisting claim should be directed** (see: Judgement of District Administrative Court in Warsaw, 20 March 2018, II SA/Wa 1035/17). In the case at hand the decision of the data protection authority (Generalny Inspektor Ochrony Danych Osobowych) obliging limited liability company based in W. remove personal data of M. K. from search engine results was challenged based on the argument that this entity does not process nor is involved in processing of personal data by the search engine. The data protection authority claimed that the company should be considered an entity established by the search engine operator. In cases concerning complaints of natural persons residing in Poland about the refusal to delete their personal data disclosed in search results in the internet search engine, the decisions

---

[60] Judgement of Supreme Court, I CSK 690/17, 13 December 2018, http://www.sn.pl/sites/orzecznictwo/Orzeczenia3/I%20CSK%20690-17-1.pdf

[61] https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/i-aca-1565-15-wyrok-sadu-apelacyjnego-w-krakowie-522099694

can be directed to this Polish based company as the entity established by the search engine operator, not the search engine operator established abroad. The court ascertained that the decision should be addressed to the personal data controller, as only he can be requested for de-listing of certain content and this entity was not established in the proceeding. The processing of personal data takes place as part of the activities carried out by the data controller responsible for this processing in the territory of a given Member State, if the operator of an internet search engine establishes a branch or a subsidiary in a given Member State, whose purpose is to promote and sell advertising space offered for through this search engine, and the activities of this branch or subsidiary are targeted at people residing in that country. In this case, the data protection authorities are entitled to issue a decision against the search engine operator as the data processing in takes place in that member state. It does not however, mean, that the decision of this authority can be directed to the branch or subsidiary of the search engine operator in that Member State.[62]

After GDPR came into force, another issue emerged that is: **in case of the claim of personal data removal based on the data protection rules, which courts should have material jurisdiction**? This question was addressed by the District Court in Łódź in the judgement issued on 25 July 2019, III Ca 396/19. Firstly the court observed that, though on certain occasions personal data processing might lead to the infringement of personality rights, in situations in which data processing (even unlawful) does not infringe personality rights, the data subject should request their removal from the database in an administrative proceeding. Thus, in such cases the administrative courts have jurisdiction, not the common courts. This conclusion, though accurate at the time of lodging the claim, became inaccurate with the GDPR's entry into force on 25 of May 2018, as the Court found. Article17 clause 1 point d of GDPR provides that the data subject has the right to request the administrator to immediately delete personal data concerning him, and the administrator is obliged to delete the data without undue delay if they were processed unlawfully. At the same time Article 79 paragraph 1 of GDPR grants such a person — without prejudice to available administrative or extrajudicial remedies (including the right to lodge a complaint with a supervisory authority) — the right to an effective remedy before a court. Therefore, the judicial protection provided for in the latter provision also applies to the exercise of the right of the person to whom the personal data pertains to demand of data removal. There is no doubt that such a request was made by the plaintiff in this case. The Polish provisions implementing the GDPR provide that to the extent not covered by Regulation 2016/679, to claims for violation of the provisions on the protection of personal data, the provisions of the Polish Civil Code shall apply. Thus, Article 79 of GDPR provides for a new civil law claim, independent for the protection of personality rights. This claim can take different forms, including the one specified in the Article 17 of GDPR. Also, in case of proceedings initiated by lodging such a claim, the provisions of the Polish Code of Civil Procedure shall apply. Therefore, from 25 May 2018 this case has become a civil law case within the meaning of Article 1 of the Code of Civil Procedure and the common courts have jurisdiction in this regard.

[62] Same reasoning in: Judgement of District Administrative Court in Warsaw, 24 July 2018, II SA/Wa 1332/17.

7.2.2. Question 2: Effective remedies and the principle of full compensation

In order to ensure the effective protection of personal data within the EU and full compensation of victims, should courts award compensation for material and non-material damages for any infringement of EU data protection law regardless of whether specific harm is found to have been caused by the infringement?

A focus on compensation under the GDPR:

Article 82 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 damage suffered. More precise provisions follow, distinguishing between the controller's and processor's liability. The burden of proving the absence of liability is placed on the controller/processor, similarly to what was provided in the 95/46/EC Directive.
Unlike other pieces of EU legislation (compare, e.g., the Antitrust Damages Directive) there is no provision for the principle of full compensation. By contrast, compensation for non-material damages is specifically provided for.
How to deal with non-material losses is a matter on which national legislation is applicable, possibly leading to different outcomes depending on legal traditions and rules, including those dealing with punitive damages and any sanction-like function of damages. Together with national specificities, the principles of effectiveness, proportionality and dissuasiveness may play a major role in this respect. On the one hand, overcompensation may be banned under the principle of proportionality (see, again, for comparison, article 3, Antitrust Damages Directive); on the other hand, punitive damages may be used within certain limits to increase deterrence and, to some extent, effectiveness.

Within the following clusters of cases, the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

Italian Court of Cassation (*Corte di cassazione*), Third Civil Chamber, 15 July 2014, n. 16133 (University of "Rome Three" v. Pieraccini et al.)

Relevant EU case law

➢ Judgment of the EU Civil Service Tribunal (First Chamber), 5 July 2011, Case F 46/09, *V. and EDPS v European Parliament*

➢ Judgment of the General Court (Sixth Chamber), 3 December 2015, Case T 343/13, *CN and EDPS v European Parliament*

➢ Request for a preliminary ruling from the Varhoven administrativen sad (Bulgaria) lodged on 2 June 2021 — *VB v Natsionalna agentsia za prihodite*, Case C-340/21, (**VB**) [pending]

➢ Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 12 May 2021 — UI v Österreichische Post AG, Case C-300/21 (**UI**) [pending]

➢ Request for a preliminary ruling from the Landgericht Saarbrücken (Germany) lodged on 1 December 2021 — GP v juris GmbH (Case C-741/21), (**GP**) [pending]

Relevant national case law

➢ Judgement of the Italian Court of Cassation (Corte di cassazione), Third Civil Chamber, 15 July 2014, n. 16133 (University of "Rome Three" v. Pieraccini et al.)

➢ Judgement of the Italian Court of Cassation (Corte di cassazione), First Civil Chamber, 8 February 2017, n. 3311 (S.G. v. Società italiana degli avvocati amministrativisti)

➢ Judgement of the Italian Court of Cassation, 20 August 2020, n. 17383

Relevant legal sources:

EU Level

Directive 95/46 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 cited above

See, for comparison, article 82, GDPR

National Level

Legislative Decree n. 196/2003, Italian Data Protection Code, implementing article 95/46/EC Directive

Article 15

This provision admits a claim for damages for economic and non-economic loss by referring to Civil Code article 2050 on liability for dangerous activities. That article makes those who carry on dangerous activities liable for damages caused unless they prove they adopted all necessary measures to avoid the occurrence of those damages.

The case(s):

Three university students filed a complaint with the Tribunal of Rome since their names were included in an Excel file listing 3724 students enrolled at the University, showing their personal data, including tax codes, University student status, employment positions and wage status. The file could be accessed via Internet by a Google search based on the students' names. The Tribunal found there was an infringement of the Italian Privacy Code (the data processing being disproportionate in respect of the aim pursued), ordered the personal data to be taken down from the web and awarded €3,000 in damages for non-economic loss to each plaintiff.

The case was brought before the Court of Cassation by the University of Rome, which challenged the decisions by lower courts especially in regard to the award of damages for non-economic loss, as its seriousness or gravity were not ascertained.

Reasoning of the Court:

Relying on its previous case law (see partial decision no 26972/2008 by Joint Chambers), the Court stated that non-economic losses may be recovered only if: i) fundamental rights are violated or the law expressly allows for recovery of non-economic losses, ii) the infringement is serious and iii) the damages are not trivial (*"futili"*). Damages have to be proved and may not be ascertained *ex se* (automatically). The criteria of seriousness of infringement and gravity of consequences are based on a balance between the principle of solidarity towards the victim and the principle of tolerance imposed within human society. Reference is made to Article 2 of the Constitution, on the protection of fundamental rights and the principle of solidarity, as well as to the case law of the ECtHR (decision no 77/07, 7 January 2014) with regard to the principle of "*de minimis non curat praetor*" (the judge does pay attention to trivial matters), intended as a "European rule of tort law".

Moreover, the Court establishes a link between the principles of solidarity and of effectiveness (of fundamental rights). Indeed, the effective protection of these rights through compensation becomes sustainable within society only if the infringement is serious and the consequences are not trivial.

The Court also highlights the distinct role of injunctions and damages, and the possibility of a modular enforcement in which the remedial response is adjusted against the material needs of protection of the victim. Whereas injunctions mainly have a preventive function, damages will be used only if prejudice is concrete, effective and substantial.

Conclusion of the Court:

The Court concludes that in data protection cases, non-economic losses may be recovered if the infringement is serious and the consequences are substantial and concrete.

Elements of judicial dialogue:

- *Horizontal dialogue (national level)*

The decision follows the position taken by the Italian Court of Cassation in the last 10-15 years on compensation for non-economic damages (see partial decision no 26972/2008 by Joint Chambers). It is confirmed by recent judgements. For example, in the decision no. 3311/2017, upholding a decision dismissing a data subject's claim for damages suffered by having received ten unsolicited email messages in three years. In that case the Court additionally condemns the claimant for abuse of the process of the court under article 96 of the Italian civil procedure code. More recently, in its decision of 20 August 2020, n. 17383 the Court of Cassation reiterated that, with regard to non-economic damages, the violation of the fundamental right to the protection of personal data is subject to compensation only if the breach is serious and the consequences of that breach (the damage) are of significative gravity (see also: Cass. 27301 of 7 October 2021; Cass. No. 16402, 26 February 2021).

As to other countries, as the following decisions are of particular interests:

Germany:

- judgement of Amtsgericht Diez, 07-11-2018, 8 C 130/18 (claimant received spam email and asked for compensation of 500 EUR, and the court held that the infringement of GDPR without damages as a consequence thereof does not give rise to a claim for damages and that "minimal damages" do not give raise to damages under Article 82 GDPR);
- judgement of Amtsgericht Bochum, 11-03-2019, 65 C 485/18 (A misdirected email does not constitute a damage for the purposes of Article 82 GDPR.);
- judgement of Oberlandesgericht Dresden, 4. Zivilsenat, Beschluss vom 11-06-2019, Az.: 4 U 760/19 (a minor loss does not give rise to claims for non-material damages under 82 GDPR);
- Landgericht Karlsruhe; 02-08-2019; 8 O 26/19 (a mere infringement of GDPR provisions does not give rise to the claims under Article 82 of GDPR); - judgement of Landsgericht Munich, 07.11.2019, 34 O 13123/19 (damage claim cannot be justified only by the fact that personal data processing was contrary to data protection provisions).

Austria:

- judgement of Oberlandesgericht Innsbruck; 13-02-2020 ("A data protection violation must in any case intervene in the emotional sphere of the victim, … a minimum level of personal impairment will have to be required for the existence of non-material damage")

Netherlands:

- judgement of Rechtbank Overijssel; 28-05-2019; AK_18_2047 (500 EUR of damages awarded for sharing a document without required anonymization — pursuant to article 82 of GDPR and national provisions of Civil Code);
- judgement of Rechtbank Amsterdam; 02-09-2019; 7560515 CV EXPL 19-4611 (damages of 250 EUR awarded — pursuant to article 82 of GDPR and national provisions of Civil Code);
- judgement of Rechtbank Noord-Nederland; 15-01-2020; C / 18 / 189406 / HA ZA 19-6 (All damage should be compensated and the concept of damage should be interpreted broadly — rejection of claim should not be based on the fact that the damage cannot be precisely specified or is relatively small.);

United Kingdom:

- the decision of the Court of Appeal in Lloyd v Google LLC [2019] EWCA Civ 1599 (02 October 2019) (damages can be claimed also when there was no pecuniary loss or distress (under the provisions implementing directive 95/46).

Poland:
On the one hand, compensation claims based solely on the infringement of data protection rules have not been found. There are no judgements where the claim would be based on Article 82 of GDPR. However, there is a substantial amount of cases in which the publication of content (e.g., personal data) constituted an infringement of personal rights[63]. In these instances the court focused on the protection of personal rights and compensation for harm caused by it, not compensation for infringement of data protection rules. The issues concerning the non-material character of damage and the doubt as to what may constitute the harm in a particular situation are discussed by the judiciary.

As a rule, the courts did not take into consideration the possibility of awarding compensation for non-material damages for any infringement of EU data protection law regardless of whether specific harm is found to have been caused by the infringement.

- *Vertical dialogue (between EU and national courts) and horizontal among foreign national courts*

The judgment examined here also refers to the case law of the ECtHR (decision no 77/07, 7 January 2014) with regard to the principle of "de minimis non curat praetor" (the judge does pay attention to trivial matters), intended as a "European rule of tort law" followed in other EU jurisdictions either in legislation or case law.
Moreover, though not referred in the judgment examined; other decisions of EU courts are worth mentioning in the field of compensation of data subjects for non-material damages. In particular, in Case F 46/09 (*V. and EDPS v European Parliament*), the EU Civil Service Tribunal addressed the issue of whether the annulment of an act of the Parliament (namely, a decision refusing an offer of employment based on the unlawful processing of medical data of the candidate) may in itself constitute appropriate and, in principle, sufficient reparation for non-material damage and, if not, how non-material damage should be assessed. Based on long standing EU case law, the Tribunal concludes that the annulment of the administration's unlawful act cannot constitute full reparation for the non-material damage: (*i*) if that act contains an assessment of the abilities and conduct of the person concerned which is capable of offending them (see judgment of 7 February 1990 in Case C 343/87 *Culin v Commission*, paragraphs 25 to 29, and in *Pierrat v Cour de Justice*, paragraph 62); (*ii*) where the illegality committed is particularly serious (judgments of 30 September 2004 in Case T 16/03 *Ferrer de Moncada v Commission*, paragraph 68, and of 7 July 2009 in Joined Cases F 99/07 and F 45/08 *Bernard v Europol*, paragraph 106); (*iii*) where the annulment of an act has no practical effect. Since the non-material damage to the applicant is not entirely compensated for by the annulment of the decision at issue, the Tribunal engages in an assessment of the fair amount of compensation the Parliament must pay to the applicant for that damage, in the light, in particular, of the *illegalities* established and of their *consequences*. These two elements resemble the assessment criteria used in the Italian decision examined above.

[63] Judgement of the Court of Appeal in Warsaw, 25-11-2016, I ACa 1565/15, judgement of the Supreme Court, 13-12-2018, I CSK 690/17, judgement of the Supreme Court, 28-09-2011, I CSK 743/10, judgement of the Court of Appeal in Cracow, 22-12-2016, I ACa 1080/16, judgement of the Court of Appeal in Bialystok, 30-09-2015, I ACa 403/15, judgement of Court of Appeal in Warsaw, 3 April 2017, I ACa 2462/15, judgment of the Polish Supreme Court, 15 May 2019, II CSK 158/18.

Moreover, the pending case *VB* (C-340/21) concerning the interpretation of Article 80 GDPR is of particular interest with regard to non-material damages. In such a case, the referring court asked to the CJEU whether, according to Article 82(1) and (2) GDP, read in conjunction with recitals 85 and 146 thereof, in a case involving a personal data breach consisting in unauthorised access to, and dissemination of, personal data by means of a 'hacking attack', the worries, fears and anxieties suffered by the data subject with regard to possible misuse of personal data in the future fall *per se* within the concept of non-material damage, which is to be interpreted broadly, and entitle them to compensation for damage where such misuse has not been established and/or the data subject has not suffered any further harm.
Furthermore, in the pending case *UI* (C-300/21) the national Court asked to the CJEU the following questions:
"1. Does the award of compensation under Article 82 of Regulation (EU) 2016/679 (1) (the GDPR) also require, in addition to infringement of provisions of the GDPR, that an applicant must have suffered harm, or is the infringement of provisions of the GDPR in itself sufficient for the award of compensation?
2. Does the assessment of the compensation depend on further EU-law requirements in addition to the principles of effectiveness and equivalence?
3. Is it compatible with EU law to take the view that the award of compensation for non-material damage presupposes the existence of a consequence of the infringement of at least some weight that goes beyond the upset caused by that infringement?"

Lastly, in the pending case GP (C-741/21) the referring court asked to the CJEU whether
i) In light of recital 85 and the third sentence of recital 146 GDPR, the concept of 'non-material damage' in Article 82(1) of the GDPR covers any impairment of the protected legal position, irrespective of the other effects and materiality of that impairment?
iii) it is permissible or necessary to base the assessment of compensation for non-material damage on the criteria for determining fines set out in Article 83 of the GDPR, in particular in Article 83(2) and 83(5) of the GDPR?
iv) the compensation must be determined for each individual infringement, or are several infringements — or at least several infringements of the same nature — penalised by means of an overall amount of compensation, which is not determined by adding up individual amounts but is based on an evaluative overall assessment

7.2.3. Question 3: Impact of the principle of effectiveness on the array of full compensation

How do the principle of effectiveness and Article 47 CFREU influence the array of full compensation in the case of unlawful collection and processing of data?

Within the following clusters of cases, the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

➢ Judgment of the EU Civil Service Tribunal (First Chamber), 5 July 2011, *V. and European Data Protection Supervisor (EDPS)*, F 46/09

Relevant CJEU case law

➢ Judgment of the EU Civil Service Tribunal (First Chamber), 5 July 2011, *V. and European Data Protection Supervisor (EDPS)*, F 46/09

➢ Judgment of the General Court (Sixth Chamber), 3 December 2015, *CN and European Data*

Protection Supervisor (EDPS), T 343/13

Relevant legal sources:

EU Level

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
(Act no longer in force, date of end of validity: 10/12/2018, repealed by Regulation (EU) 2018/1725)

Article 2 Definitions; Article 4.1.; Article 5 Lawfulness of processing; Article 6 ; Article 7.1.; Article 10. 1.; Article 18 The data subject's right to object

The case:

V, after passing the contract agent selection tests for the 25 Member States in the secretarial field, underwent pre-recruitment medical examination in June 2006, after which she lodged a complaint on the examiner — dr K. Subsequently, she was declared physically unfit for the position she applied — firstly by dr K, and then by the medical committee. As a result, she was not employed. She brought an action *inter alia* against this decision of Commission (Case F-33/08), which was dismissed.
On 9 December 2008 the European Parliament made the applicant an offer of employment as a member of the contract staff, which was accepted by her on the following day. The offer was made subject to compliance with the conditions of engagement laid down in Article 82 of the CEOS and to the positive outcome of the pre-recruitment medical examination (appointment set on the 7 January 2009). On 12 December 2008, the Parliament's medical service received a copy of the applicant's pre-recruitment medical file from the previous proceeding. Based on the medical examination from June 2006, the Parliament's medical officer declared the applicant physically unfit to perform 'any duties in any European [i]nstitutions' and the Parliament withdrew the offer of employment of 10 December 2008.
V brought the action against the European Parliament seeking annulment of the decision by which the Director for Administrative Management of Personnel of the European Parliament withdrew, on the ground of unfitness for recruitment, the offer of employment which had been made to her on 10 December 2008 and of the opinion of the Parliament's medical officer of 18 December 2008, as well as compensation for the damage suffered.

Reasoning of the Court:
The Court observed that the medical officer's opinion was issued with disregard to the applicant's right to respect for private life and that the decision at issue is, accordingly, also unlawful for that reason (127 - infringement of the right to respect for privacy). By asking the Commission for the transfer of those medical data, the Parliament's medical officer infringed Articles 6 and 7 of Regulation 45/2001 (143).
The administration can be held liable for damages because the allegedly wrongful act committed by the institutions was illegal, the applicant suffered actual harm, and there was a causal link between the act and the damage.
The Court found that the required causal link is attained if the unlawful act committed has deprived a person of a chance of being recruited, resulting in material damage for the person concerned in the form of loss of income. In the case at hand, the recruitment decision was already made — the applicant's engagement depended solely on establishing her physical fitness. It was not proved that, provided that the medical examination for recruitment had been conducted in a regular manner, the applicant would

not have been recruited due to the information collected by the Parliament's medical service on the applicant's state of health in January 2009. The Court underlined also that a candidate for recruitment cannot be required to disclose all his medical history to his future employer. In addition, the knowledge of disorders other than physiological disorders does not automatically justify a refusal of recruitment.
As to the non-material damage, though the annulment of an act which has been challenged may in itself constitute appropriate and sufficient reparation for the damage, it should be assessed whether the act contained a possibly offensive assessment of the abilities and conduct of the person. Being that the case, the annulment of the administration's unlawful act cannot constitute full reparation.
Also, if the illegality of actions committed by the administration was particularly serious, it justifies the award of compensation for the non-material damage. In the case the infringement of the right to respect for private life and of Regulation 45/2001 were seen as particularly serious.
Finally, it was observed that in situations where the annulment of the act lacks practical effect, it cannot in itself constitute appropriate and sufficient reparation. The Court underlined the permanent effect which an unlawful processing of subject's data — namely bringing certain information relating to the applicant's health — might have. The information, once unlawfully provided, might have a continuous impact on the person to which it was revealed. Therefore, annulment of the act at issue might not effectively protect applicant rights, as it cannot erase the doubts as to the fitness of the applicant which have already emerged, hindering objective analysis of her health in the future.

Conclusion of the Court:
For these reasons, the Court ascertained that the applicant have the right to compensation for material damage caused by the above. In order to establish the height of compensation the Court assessed that the chances of being recruited were *ex aequo et bono* 50%, the remuneration for the period in question - EUR 15 600.60, the unemployment benefits the applicant received amounted to EUR 960 a month, and therefore ordered the defendant to pay the applicant the sum of EUR 5 000 for the material damage.
Furthermore, as the annulment of the act did not entirely compensated for the non-material damage (in particular the infringement of the right to respect for private life and of Regulation No 45/2001), the Court awarded the applicant with the compensation of EUR 20 000.

Elements of judicial dialogue:
- Horizontal (within CJEU)

➢ Judgment of the General Court (Sixth Chamber), 3 December 2015, *CN and European Data Protection Supervisor (EDPS)*, T 343/13.
V. and EDPS (F 46/09) was complemented by the decision of the Court in *CN and EDPS* (T 343/13). **In this judgement, the Court addressed the impact of the principle of effectiveness on establishing the entity legitimised to claim compensation for unlawful collection and processing of data as well as the scope of costs which can be considered damages caused by the unlawful act in question.**
CN, an official of the Council of the EU, submitted an online petition to the European Parliament, on the support granted to disabled family members of a European official and the difficulties encountered by European officials suffering health problems during their careers. The document which summarised the petition and Council's answer to it was published online. It included the name of the applicant as well as data on his serious illness and the disability of his son. CN requested removal of the notice in April 2012 and on 20 April 2012 the Parliament informed that the content was removed. Nevertheless, the notice remained accessible for some time. CN claimed that from the information he was given when consenting to processing of his data was not clear. For this reason, he lodged an application requesting

award of EUR 1000 of compensation for material damage and EUR 40 000 in compensation for non-material damage suffered.
The Union incurs the non-contractual liability under the second sentence of Article 340 TFEU for unlawful conduct of its institutions if the allegedly wrongful act committed by the institutions is illegal, the applicant suffers actual harm, and there us a causal link between the act and the damage. In order for the liability to arise, all the aforementioned premises must be fulfilled.
Firstly, the Court examined the unlawfulness of the institutions' conduct. Publication of the applicant's data on the website by the Parliament constituted processing of personal data within the meaning of Article 2(b) of Regulation 45/2001. As a rule, the processing of personal data revealing data concerning health is prohibited under Article 10(1) of Regulation 45/2001, unless the data subject has given his or her express consent (see: Article 10(2)(a)). This consent must be freely given specific and informed (Article 2(h) of Regulation 45/2001). Also, the scheme and the purpose of the right of petition to the Parliament should be taken into account — being the instrument of democratic participation it should be transparent so that it can trigger a public debate as to the issue at hand. The specific content of the petition was the key element that was aimed to be brought to public discussion by the applicant — and it was to be considered in public. In light of the above, the Court ascertained that the applicant had unambiguously provided a 'freely given specific and informed indication' of his wishes in relation to the processing of his personal data by the Parliament, including their disclosure in the context of the processing of a petition by the Parliament. Thus, the Parliament's actions cannot be deemed unlawful and the applicant cannot be awarded a compensation on this basis.
Accordingly, the Court ascertained that the fulfilment of premise of consent for data processing must be interpreted in light of the circumstances of the case. In order for the liability to arise, the breach of rule of law must be sufficiently serious. In this case, the Court — after examining the interests at hand as well as the circumstances and the function of the petition — holds that the Parliament did not commit a sufficiently serious breach of law by disseminating the personal data in question on the internet.
Another issue which was raised during the proceeding regards the entity entitled to claim damages — the applicant claimed that also his son's sensitive data had been processed unlawfully, for what the applicant demanded compensation. However, neither the applicant was a representative of his son in the proceeding nor was the son the party to the action. The Court ascertained that in order to ensure the effectiveness of the condition relating to the breach of legal provision conferring rights on individuals, the protection offered by the rule invoked must be effective *vis-à-vis* the person who invokes it, and that person must therefore be among those on whom the rule in question confers rights. A rule which does not protect the individual against the unlawfulness invoked by him, but protects another individual, cannot be accepted as a source of compensation. The applicant cannot, therefore, invoke unlawfulness resulting from the alleged breach of rights of a third party, namely his son. Thus, one cannot claim compensation for the damaged caused to another.

➢ Lastly, in the pending case GP (C-741/21) the referring court asked to the CJEU whether
i) In light of recital 85 and the third sentence of recital 146 GDPR, the concept of 'non-material damage' in Article 82(1) of the GDPR covers any impairment of the protected legal position, irrespective of the other effects and materiality of that impairment?
iii) it is permissible or necessary to base the assessment of compensation for non-material damage on the criteria for determining fines set out in Article 83 of the GDPR, in particular in Article 83(2) and 83(5) of the GDPR?
iv) the compensation must be determined for each individual infringement, or are several infringements — or at least several infringements of the same nature — penalised by means of an overall amount of compensation, which is not determined by adding up individual amounts but is based on an evaluative overall assessment.

7.3. The impact of the principle of proportionality on remedies and sanctions

7.3.1. Question 4: Sanctions and the principle of proportionality

Which is the role of the principle of proportionality in the application of sanctions?

A short view on the GDPR rules:

Compared with Directive 46/95, Regulation (EU) 2016/679 (GDPR), as shown in the introduction to this chapter, has paid much greater attention to the application of general principles (and specifically effectiveness, dissuasiveness and proportionality) to sanctions and other measures (for an overview, see the introduction of this chapter).

The legislator has acknowledged that the task of a supervisory authority is not an easy one and needs guidance. Such guidance, mainly provided through the lens of general principles (effectiveness, proportionality and dissuasiveness) should also steer enforcers when combining administrative fines with other measures (namely the so called "corrective" measures, see Article 58(2)), since administrative fines are conceived as alternative or complementary to these measures "depending on the circumstances of each individual case" (see Article 83(2)).

Similar guidance could apply to the other sanctions that, aside from these administrative fines, Member States may adopt under Article 84 in order to sanction infringements of this Regulation, having particular (but not exclusive) regard to those not addressed by administrative fines pursuant to Article 83. Those penalties should also be effective, proportionate and dissuasive. It seems plausible to state that, when applying these principles, the enforcer (administrative or judicial authority) should take into account whether or not other penalties or measures are available.

Within the cluster of cases, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

➢ Judgment of the Court, 6 November 2003, *Bodil Lindqvist*, Case C-101/01 (***Lindqvist***)

The case:

The facts of the case, as well as the relevant legal sources, have been described in Chapter 2, question 2. To sum up, Mrs. Lindqvist, who was a maintenance worker, had infringed Swedish law on data protection by setting up pages on the internet, after she had followed a data processing course. The internet pages, meant to allow parishioners preparing for their confirmation to obtain information they might need, displayed personal data on a number of people working with her on a voluntary basis in a parish of the Swedish Protestant Church. As soon as Mrs Lindqvist became aware that these pages were not appreciated by some of her colleagues, she removed them.

She was nevertheless prosecuted and charged with breach of the law. The amount of the fine was SEK 4,000, which was arrived at by multiplying the sum of SEK 100, representing Mrs Lindqvist's financial position, by a factor of 40, reflecting the severity of the offence. Mrs Lindqvist was also sentenced to pay SEK 300 to a Swedish fund to assist victims of crimes.

Preliminary question referred to the Court:

Several questions were referred to the Court, but none focusing on the issue of the proportionality of the sanction. However, the Court addressed that issue in its reasoning under question 6, by which the referring court asked whether the provisions of Directive 95/46 introduce a restriction that conflicts

with the general principles of freedom of expression or other freedoms and rights, which are applicable within the EU and are enshrined *inter alia* in article 10 of the ECHR.

Reasoning of the Court:

While the main part of the reasoning concerns the balance between the freedom of expression of the controller, and the right of the data subject to the protection of private life and personal data (on which see Chapter 3, question 2), the Court addresses the issue of the **proportionality** of the sanction in what seems to be an *obiter* statement. After recalling that Member States should, at the stage of the application at national level of the legislation implementing Directive 95/46 in individual cases, find a balance between the rights and interests involved, the Court also deals with the issue of the sanction by stating: "Whilst it is true that the protection of private life requires **the application of effective sanctions** against people processing personal data in ways inconsistent with Directive 95/46, **such sanctions must always respect the principle of proportionality.** That is so a fortiori since the scope of Directive 95/46 is very wide and the obligations of those who process personal data are many and significant (§88).

It is for the referring court to take account, in accordance with the principle of proportionality, of all the circumstances of the case before it, in particular the duration of the breach of the rules implementing Directive 95/46 and the importance, for the persons concerned, of the protection of the data disclosed" (§89)

The Court thus puts both *principles of effectiveness and proportionality* into perspective, and which should be considered together when imposing a sanction. Sanctions are to be effective, but they should not be disproportionate. And national courts or authorities should take into account all circumstances of the case in order to assess what should be the adequate sanction. Although the Court only refers to the duration of the breach and to the importance of the protection of the data disclosed, it seems that other circumstances could be considered, such as the awareness of the controller that he was infringing the law, the purpose he was pursuing, or his good faith.

Impact on national case law in Member States different from the state of the court referring the preliminary question to the CJEU:

France

French *Conseil d'Etat*, 28 September 2016, no 389448: the *Conseil d'Etat* observes that when the French supervisory authority imposes, in addition to the main sanction, a measure consisting of publicising the sanction imposed on the controller, such additional sanction is necessarily subject to the principle of proportionality, even if the law does not expressly so state. The legality of the sanction should be assessed, in particular, in light of the type of publishing medium, and of the time during which the publication is available to the public. In the case considered, the additional sanction (publicity of the main sanction) is, because of the seriousness of the infringement, justified in principle since it tends to reinforce the dissuasiveness of the main sanction. However, because it does not define the time period during which the publication will be online and available to the public, the sanction is excessive. It should be annulled, insofar as it does not define for how long the publication should stay online in a non-anonymous manner.

Cour de cassation, Commercial Chamber 25 June 2013, no 12-17037: Even if the law does not state expressly so, the sale of a file including personal data that has been unlawfully collected and processed (no declaration to the French data protection authorities) is void since the object of the sale — the undeclared processing of data — is unlawful and thus cannot be seen as being available for trade.

This decision implicitly relies on the principles of effectiveness and dissuasiveness since it deprives a file including unlawfully processed personal data of any commercial interest.

Belgium

Decision no. 2020/AR/1333 of 27 January 2021 decided by the Court of Appeal of Bruxelles is of particular interest. In that decision, the Court of Appeal assessed the proportionality of a sanction established by the DPA according to Article 83 GDPR. The Court stated that by immediately imposing an administrative fine - a very substantial one — on a private individual who sent e-mails mentioning the e-mail addresses of all the persons to whom the e-mail was addressed, the Authority disregarded the fundamental principles of the proportionality of the sanction. In its reasoning the Court considered that where the decision is to be adopted on a case-by-case basis, starting from the principle of good faith, in the absence of a prior warning and of any precedent, and where the infringer immediately apologise (the day after the applicant was informed of the problem of which he was unaware), the sanction of immediately imposing an administrative fine, in addition to the fact that it is set from the outset at a significant sum of 5,000 euros, is disproportionate. The Court criticised the fact that the Authority did not consider the possibilities of achieving the goal of the European legislation by another decision, considering that several elements that demonstrate that the infringer did not show any intention to disregard the principles of personal data protection, but rather that the violation he committed was the result of negligence or inadvertence and that he immediately rectified the situation and apologised. Accordingly, the Court affirmed that the imposition of fines from the first inadvertent infringement does not correspond to the principles governing the matter, taking into account that several kind of sanctions exists (from the warning to the financial sanction). Moreover, the Court considered that the Authority failed to take into account the presumption of good faith.

7.3.2. Question 5: the principle of proportionality and the right to be de-listed

Which is the role of the principle of proportionality in applying the right to be de-listed, which stems from the right to erasure provided for by Article 17 GDPR?

Within the cluster of cases, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts:

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *G.C., A.F., B.H., E.D.* v *Commission nationale de l'informatique et des libertés* (CNIL), Case C-136/17 (***GC and Others)***

Cluster of cases:

➢ 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***)

➢ Judgment of the Court (Second Chamber), 9 March 2017, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce* v *Manni*, Case C-398/15 (***Manni***)

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *G.C., A.F., B.H., E.D.* v *Commission nationale de l'informatique et des libertés* (CNIL), Case C-136/17 (***GC and Others)***

➢ Judgement of the Court (Grand Chamber), 24 September 2019, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), C-507/17 (***Google v. CNIL***)

➢ Judgment of the Court (Third Chamber) of 3 October 2019, *Eva Glawischnig-Piesczek v Facebook*

Ireland Limited, C-18/18

➢ Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 24 September 2020 — *TU, RE v Google LLC*, Case C-460/20 (**TU, RE v Google LLC**) [pending]

➢ Request for a preliminary ruling from the Hof van beroep te Brussel (Belgium) lodged on 2 March 2021 — *Proximus NV v Gegevensbeschermingsautoriteit*, Case C-129/21, (**Proximus**) [pending]

The case

The facts of the case are explained in the question 1 of this Chapter.

Preliminary questions referred to the Court

For our analysis the second question referred to the CJEU is of particular importance. In this question, the national court essentially asked whether:

i) the operator of a search engine is required to accede to requests for de-referencing in relation to links to web pages containing sensitive data;

ii) such an operator may refuse to accede to a request for de-referencing if he establishes that the links at issue lead to content comprising sensitive data but whose processing is covered by one of the exceptions to the prohibition of processing of such data;

iii) whether that the operator of a search engine may also refuse to accede to a request for de-referencing on the ground that the links whose de-referencing is requested lead to web pages on which sensitive data are published solely for journalistic purposes or those of artistic or literary expression and the publication is therefore covered by the related exception.

Reasoning of the Court

The Court observed that according to Article 17(3) of Regulation 2016/679 the right to erasure (being the right to be delisted a part of it) is not to apply to the extent that the processing is necessary on one of the grounds set out in Article 17(3), among which there is the exercise of the right of freedom of expression and information.

The Court, in deciding on the application of the right to be de-listed in case of processing of sensitive data, considered then that the explicit mention, in Article 17 GDPR, of freedom of expression, guaranteed by Article 11 CFR, demonstrates that "the right to protection of personal data is not an absolute right but (…) must be considered in relation to its function in society and be balanced against other fundamental rights, **in accordance with the principle of proportionality**". The CJEU referred to **Article 52(1) CFR,** according to which limitations to fundamental rights may be imposed as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, **subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others**. Then, the Court stated that Article 17(3)(a), expressly lays down the requirement to strike a balance between the fundamental rights to privacy and protection of personal data guaranteed by Articles 7 and 8 of the Charter, on the one hand, and the fundamental right of freedom of information guaranteed by Article 11 of the Charter, on the other hand.

Conclusion of the Court

The Court stated that the operator of a search engine is in principle required to answer to requests for de-referencing in relation to links to web pages containing personal data falling within the special categories referred to by those provisions. Nevertheless, where an exception to the prohibition of the

processing of this kind of data apply, such an operator may refuse to answer to a request for de-referencing, provided that the processing satisfies all the other conditions of lawfulness laid down by the directive, and unless the data subject has the right to object to that processing on compelling legitimate grounds relating to his particular situation.

Furthermore, where the operator of a search engine has received a request for de-referencing relating to a link to a web page on which sensitive data 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 CFR, ascertain, having regard to the reasons of substantial public interest and in compliance with the conditions laid down in EU data protection laws, 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 CFR.

Impact on the follow-up case

French Council of State, 6 December 2019, No. 401258.
In the paragraph concerning question 4 the decision of the Council of State has already been summarised. With regard to the specific question of the role of the proportionality principle, the Council of State affirmed that in order to assess whether the right to de-referencing can be legally defeated on the grounds that access to personal data relating to criminal proceedings on the basis of a search for the name of the person concerned is strictly necessary to inform the public, the CNIL must take into account, in particular, the nature of the data in question, their content, their more or less objective nature, their accuracy, their source, the conditions and date on which they are put online and the repercussions that their listing is likely to have for the person concerned and, on the other hand, the notoriety of that person, their role in public life and their function in society. Moreover, according to the Council of State, it must also take into account the possibility of accessing the same information from a search on keywords that do not mention the name of the data subject. In the particular case where the link leads to a web page which refers to a stage of a judicial procedure which no longer corresponds to the current judicial situation of the data subject but it appears, after the balance carried out under the conditions set out previously, that the maintenance of its referencing is strictly necessary to inform the public, the operator of a search engine is required, at the latest at the time of the request for de-referencing, to arrange the list of results in such a way that the disputed links are preceded on this list of results by at least one link leading to one or more web pages containing up-to-date information, so that the resulting image accurately reflects the current legal situation of the person concerned. Even though, under the Code of Criminal Procedure, access to data relating to a person's criminal convictions is in principle possible only under restrictive conditions and for limited categories of persons (relating to the lack of notoriety of the person concerned, the length of time the facts have been known, the criminal conviction and the repercussions on the applicant's rehabilitation), by finding that the applicant who alleges that he has lost two jobs as a result of the link in question, the CNIL could not legally consider that maintaining the links based on a search carried out on its name (given the nature and content of the disputed information, which gives the public direct and permanent access to the applicant's conviction, even if this information comes from press articles whose accuracy is not disputed) was strictly necessary to inform the public for the sole reason that the judicial columns allow the public to exercise a right of oversight over the functioning of criminal justice.

Elements of judicial dialogue

CG and Others (C-136/17) should be read in light of the CJEU case law, and in particular of *Google Spain* (C-131/12), *Google v. CNIL* (C-507/17), *Manni* (C-398/15) .
In *Google Spain* (C-131/12) Google referred to the **principle of proportionality**, arguing that, by virtue of that principle, any request seeking the removal of information must be addressed to the publisher of the website concerned because it is he who takes the responsibility for making the information public, who is in a position to appraise the lawfulness of that publication and who has available to him the most effective and least restrictive means of making the information inaccessible. **The Court rejected this argument.**
In *Google v. CNIL* (C-507/17) the Court, defining the territorial scope of the right to be de-listed, affirmed that the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of **proportionality** (on this judgement and the right to be de-listed see also Question 1a of Chapter 1).
GC and Others (C-136/17) is interestingly complemented also by the decision of the Court in ***Manni*** (C-398/15). Mr Manni requested that the personal data related to him be erased from the public companies register, after the elapse of a certain period of time. In these registers it was mentioned that he had been the director of a company which had been declared insolvent 15 years before. He claimed that that information caused him prejudice in the course of his current business. After recalling that the transcription of certain information into a public companies register, imposed by Directive 68/151, qualifies as "processing of personal data", the Court observed that such a processing, by the authority responsible for keeping the register, satisfies several grounds for legitimacy set out in Article 7 of Directive 95/46, namely: those set out in subparagraph (c) thereof, relating to compliance with a legal obligation; subparagraph (e), relating to the exercise of official authority or the performance of a task carried out in the public interest; and subparagraph (f) relating to the realisation of a legitimate interest pursued by the controller or by the third parties to whom the data are disclosed. However, the issue at stake was whether the authority responsible for keeping the register should, after a certain period had elapsed since a company ceased to trade, and on the request of the data subject, either erase or anonymise that personal data, or limit its disclosure.

In relation to this issue, the Court noted that according to EU data protection laws personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed; when the availability of data is no longer necessary, data subjects have a right to obtain from the controller the erasure or blocking of the data. Such right is to be considered in light of the purpose of the processing or, here, the registration.

The Court observed that the purpose of the disclosure provided for by Directive 68/151 is, in particular, to protect the interests of third parties in relation to joint stock companies and limited liability companies, since the only safeguards they offer to third parties are their assets, and to guarantee legal certainty in relation to dealings between companies and third parties in view of the intensification of trade between Member States following the creation of the internal market. The Court observed moreover that for several reasons, it is absolutely necessary to access data concerning a company, long after its dissolution. For the Court, given 'the considerable heterogeneity in the limitation periods provided for by the various national laws in the various areas of law, highlighted by the Commission, it seems impossible, at present, to identify a single time limit, as from the dissolution of a company, at the end of which the inclusion of such data in the register and their disclosure would no longer be necessary'.

For this reason, Member States cannot guarantee that the natural persons referred to in Directive 68/151 have the right to obtain, as a matter of principle, after a certain period of time from the dissolution of the company concerned, the erasure of personal data concerning them, which has been entered in the register pursuant to the latter provision, or the blocking of that data from the public. Such a situation does not result in disproportionate interference with the fundamental rights of the persons concerned, and particularly their right to respect for private life and their right to protection of personal data as guaranteed by Articles 7 and 8 of the Charter, because the disclosure concerns only a limited amount of data, because other legitimate interests are at stake, and because persons engaging in such activity are aware of these requirements. Finally, national courts are to engage in a case-by-case analysis to decide if, exceptionally, it is justified, on compelling legitimate grounds relating to their particular situation, to limit, on the expiry of a sufficiently long period after the dissolution of the company concerned, access to personal data relating to the natural person referred to in Directive 68/151, entered in that register, to third parties who can demonstrate a specific interest in consulting that data.
With regard to the balancing between fundamental rights and interests at stake, in the pending case *TU, RE v Google LLC* (C-460/20) the referring court asked the CJEU whether in the case of a request for de-referencing made against the data controller of an internet search engine, which in a name search searches for photos of natural persons which third parties have introduced into the internet in connection with the person's name, and which displays the photos which it has found in its search results as preview images, within the context of the weighing-up of the conflicting rights and interests arising from Articles 7, 8, 11 and 16 of the Charter pursuant to Article 17(3)(a) of the GDPR, the context of the original third-party publication should be conclusively taken into account, even if the third-party website is linked by the search engine when the preview image is displayed but is not specifically named, and the resulting context is not shown with it by the internet search engine.

Lastly, in the pending case *Proximus* (C-129/21) the referring Court asked to the CJEU whether Article 17[(2)] GDPR must be interpreted as precluding a national supervisory authority from ordering a provider of public directories and directory enquiry services which has been requested to cease disclosing data relating to an individual to take reasonable steps to inform search engines of that request for erasure. The principle of proportionality may play a significant role in interpreting Article 17(2) according to which, where the controller has made the personal data public and is obliged 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. In particular, the question arises as to whether the concept of "reasonable steps" could or should be interpreted in light of the principle of proportionality, and/o in light of the data subjects' right to an effective remedy (on the latter see Section XX in this chapter).

Impact on national case law in Member States other than the one of the court referring the preliminary question to the CJEU

See Question 1 of this Chapter.

7.3.3. Question 6: Proportionality, effectiveness, data/privacy protection and the information obligations

What is the relationship between data protection/privacy and information to be provided to the data subject, considered the importance of the latter for the exercise of data subjects' rights? Do Article 47 CFREU and the principles of effectiveness and proportionality play a role in this regard?

Within the following cluster of cases, the main case that is to be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts is:

➢ Judgment of the Court (Third Chamber), 7 May 2009, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, C-553/07 (***Rijkeboer***)

Relevant CJEU caselaw

➢ Judgment of the Court (Third Chamber), 7 May 2009, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, C-553/07 (***Rijkeboer***)

➢ Judgment of the Court (Third Chamber), 17 July 2014, *YS (C-141/12) v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel (C-372/12)*, Joined Cases C-141/12 and C-372/12 (***YS and Others***)

➢ Judgment of the Court (Third Chamber), of 1 October 2015, *Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others*, C-201/14 (***Bara and Others***)

➢ Judgment of the Court (Second Chamber), 26 July 2019, *Fashion ID Gmbh & Co.KG* v. *Verbraucherzentrale NRW EV*, Case C-40/17 (***Fashion ID***)

➢ Judgment of the General Court (Sixth Chamber), 3 December 2015, *CN and European Data Protection Supervisor (EDPS)*, T 343/13 (***CN v Parliament***)

➢ Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others v Premier ministre and Others*, Joint Cases C-511/18, C-512/18 and C-520/18 (***La Quadrature du Net***)

➢ Request for a preliminary ruling from the *Itä-Suomen hallinto-oikeus* (Finland) lodged on 22 September 2021 — J.M., Case C-579/21, (**Itä-Suomen**) [pending]

➢ Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 9 March 2021 — *RW v Österreichische Post AG*, Case C-154/21, (**RW**)

See also: WP 29 Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Relevant legal sources:

EU Level

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

Section I Principles relating to data quality (Article 6); Article 10 Information in cases of collection of data from the data subject; Article 11 Information where the data have not been obtained from the data subject

SECTION V - THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA Article 12 Right of access; Article 13 Exemptions and restrictions; Article 14 The data subject's right to object; Article 22 Remedies; Article 23 Liability

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

(In force since: 25/05/2018)

Section 2 Information and access to personal data; Article 13 Information to be provided where personal data are collected from the data subject; Article 14 Information to be provided where personal data have not been obtained from the data subject; Article 15 Right of access by the data subject; Article 78 Right to an effective judicial remedy against a supervisory authority; Article 79 Right to an effective judicial remedy against a controller or processor; Article 80 Representation of data subjects; Article 82 Right to compensation and liability

National Level
Article 110 of Wet gemeentelijke basisadministratie persoonsgegevens, Stb. 1994, No 494; 'the Wet GBA'

The case:
Mr Rijkeboer requested the College (municipal authority) to inform him of all instances in which his personal data from that local authority personal records had, in the two years preceding the request, been disclosed to third parties. He wanted to know the identity of these entities and the content of the disclosed data. The College complied partly with this request, providing him with the data relating to the period of one year preceding the request, as the previous information was automatically erased, in accordance with national provisions (Article 110 the Wet GBA). Mr Rijkeboer lodged a complaint with the College against the refusal and the national court (the Raad van State) referred the following question to the Court for a preliminary ruling.

Preliminary question referred to the Court:
Can, pursuant to the Directive and, in particular, to Article 12(a) thereof, an individual's right of access to information on the recipients or categories of recipient of personal data regarding them and on the content of the data communicated be limited to a period of one year preceding his request for access? (31)

Reasoning of the Court:
The CJEU considered that the case involved two categories of data, personal data kept by the local authority on a person, such as his name and address, which constitute, in the present case, the basic data, and information concerning recipients or categories of recipient to whom those basic data are disclosed and thus concerning the processing of the basic data.
In accordance with the national legislation at issue in the main proceedings, the latter information was stored for only one year. The time-limit on the right of access to information on the recipient or recipients of personal data and on the content of the data disclosed concerned that second category of data, in so far as those data were stored for only one year.
The CJEU, in order to determine whether or not Article 12(a) of the Directive authorised such a time-limit, interpreted that article having regard to its purposes of protecting the fundamental rights and freedoms of natural persons, and of permitting the free flow of personal data between Member States. The CJEU relied on its previous case law and pointed out the importance of protecting privacy with respect to the processing of personal data (*Österreichischer Rundfunk and Others*, Joined cases C-465/00, C-138/01 and C-139/01, §70; *Lindqvist*, C-101/01 paragraphs 97 and 99; *Promusicae*, C-275/06, §63; *Satamedia*, C-73/07, §52).
The CJEU stated that the data subject should be sure that his personal data are processed in a correct and lawful manner, that is to say, in particular, that the basic data regarding him are accurate and that they are disclosed to authorised recipients. **The CJEU highlighted that the right of access is necessary to enable the data subject to exercise its other rights** . The CJEU affirmed that the right to access to information on the recipients or categories of recipient of personal data and on the content of the data

disclosed may concern the past, in order to ensure that the data subject can **effectively exercise** her rights. With regard to the question of the scope of that right in the past, the CJEU stated that the setting of a time-limit with regard to the right to access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed must allow the data subject to exercise the different rights laid down in the Directive. In this respect, the CJEU affirmed that the length of time the basic data are to be stored may constitute a useful parameter without, however, being decisive.
The CJEU gave some elements for striking the balance between data subjects rights and the obligations of the controller. On the one hand the court considered that where the length of time for which basic data are to be stored is very long, the data subject's interest in exercising the rights to object and to other remedies may diminish in certain cases. On the other hand, the CJEU stated that if, for example, the relevant recipients are numerous or there is a high frequency of disclosure to a more restricted number of recipients, the obligation to keep the information on the recipients or categories of recipient of personal data and on the content of the data disclosed for such a long period could represent an excessive burden on the controller. In this respect, the CJEU recalled Article 12(c) of the Directive, which expressly provides for an exception to the obligation on the controller to notify third parties to whom the data have been disclosed of any correction, erasure or blocking, namely, where this proves impossible or involves a disproportionate effort. The CJEU stated that in accordance with other sections of the Directive, the **disproportionate** nature of other possible measures should be considered, taking into account the number of data subjects and the age of the data. Furthermore, in accordance with Article 17 of the Directive concerning security of processing, Member States are to provide that the controller must implement appropriate technical and organisational measures which, regarding the state of the art and the cost of their implementation, are to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Conclusion of the Court:

Article 12(a) of Directive 95/46/EC requires Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed in respect of the present and of the past. Therefore, Member States should determine a time-limit for storage of these information which would provide for a fair balance between the interest of the data subject in protecting his privacy and the burden which the obligation to store that information represents for the controller. The Court stated that:
"Rules limiting the storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed to a period of one year and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. It is, however, for national courts to make the determinations necessary."

Impact on the follow-up case

➢ ECLI:NL: RVS:2009: BK4335 – continuance of national proceedings after preliminary ruling in Rijkeboer.

The follow-up case to the Rijkeboer decision was heard by the Dutch Council of State. After citing an extract from Rijkeboer, the Council of State stated that in its appeal the College had not plausibly demonstrated that a retention period of longer than one year entails an excessive burden. The Council of state considered that the Rotterdam court (of first instance) had therefore correctly considered the limitation of the right to information on the provision of data in the year prior to the request, as provided for in Article 103 (1) of the Municipal Personal Records Database Act, to be contrary to Article 12 of the

directive. The appeal on that ground therefore failed. The Dutch judgment does not refer to Articles 7, 8 or 47, or the principles of effectiveness and proportionality.

Elements of judicial dialogue:

- Horizontal (within CJEU)

The right to access data is subject of analysis by the CJEU in *YS and Others* (joined cases C-141/12 and C-372/12, issued on 17 July 2014) and in *Smaranda* (C-201/14).

In *YS and Others* (C-141/12 and C-372/12) the dispute originated in the Netherlands and concerned denial of access to the draft decision ('the minute') issued by an officer of the Immigration and Naturalisation Service responsible for dealing with an application for a residence permit which included personal data of the applicant and an assessment of these information in light of the applicable legal provisions. The national courts referred the several questions to CJEU, between other as to the scope of the right to access to the processed data. With regard to the question whether the data subject was entitled to have access to the entire document, the Court, recalling that the right of access is provided for in Article 8(2) CDFUE, stated that the form in which the data are processed must enable the data subject to verify that they are accurate and processed in a manner consistent with the legislation in order to enable him to exercise his rights.

In *Smaranda* (C-201/14) there was a communication of data from one public administration to another, and the person concerned brought a claim before a court, questioning the lawfulness of that communication in several respects, including that the national legislation did not provide to the data subject the information on the communication of personal data. The national court asked whether national provisions may restrict information both on the communication of the data and on their subsequent processing. In answering that question, t**he CJEU stated that that information necessarily affects the exercise of the data subject's rights. Moreover, the Court notes that the principle of fair processing requires the data subject to be informed.**

In the cases considered in this section Articles 8, 47 and 52 of the CDFEU seems to be relevant. In particular, the right to an effective remedy (Article 47 CFR) comes into play with respect to the necessity of information to be provided to the data subject in order to allow her to exercise her rights. Moreover, the relevance of the principle of proportionality, recalled by the CJEE in *Rijkeboer* (C-553/07) is twofold: on the one hand, it is provided as a balancing criterion within the wording "**disproportionate effort"** of the data controller (now Article 14 GDPR), and, on the other hand, in relation to Article 52 CFR, which requires the application of that principle in limiting the exercise of the rights and freedoms provided for in the Charter, such as the data subject's right to access to personal data, set forth in Article 8(2) CFR.

The scope of the information which should be provided in order to ensure that the data subjects' rights is capable of exercising his rights was tackled in the case *Fashion ID* (C-40/17). The company "Fashion ID" embedded in its website a plugin from third party platform (Facebook). Once the Fashion ID website was accessed the user's website requested content from Facebook, transmitting at the same time data on the user. Nevertheless, the Fashion ID did not control the scope of transmitted data nor its further processing. However, the Court ascertained that the duty to inform under Article 10 of Directive 95/46 is incumbent also on the operator of the website in which a plugin from a third party platform is embedded, with regard to the processing operations where he is to be qualified as a controller (see Chapter 2). Thus, it could be argued that Fashion ID is obliged only to provide information the collection and transmission of personal data — the processing activities for which it is a (joint) controller. Those duties do not emerge in case of operations involving the processing of personal data at other — previous or subsequent — stages. (paras 100-101).

Furthermore, in *La Quadrature du Net* (C-511/18, C-512/18, C-520/18), the CJEU, in a case concerning the application of Directive 2002/58, stated that where exceptionally a national public authority collect in real time traffic and location data, that authority must notify the persons concerned, in accordance with the applicable national procedures, to the extent that and as soon as that notification is no longer liable to jeopardise the tasks for which those authorities are responsible. According to the CJEU, that notification is, indeed, necessary to enable the persons affected to exercise their rights under Articles 7 and 8 CFR, to request access to their personal data that has been processed, and where appropriate, to have the latter rectified or erased, as well as to exercise the right to an effective remedy, in accordance with Article 47 CFR, of an effective remedy before a tribunal.

Furthermore, in relation to data subject's information the right to access, provided for by Article 15 GDPR may play a role. In this respect, in *RW* (C-154/21), the referring court asked the CJEU as to whether Article 15(1)(c) GDPR is to be interpreted as meaning that the right of access is limited to information concerning categories of recipients where specific recipients have not yet been determined in the case of planned disclosures, but that right must necessarily also cover recipients of those disclosures in cases where data has already been disclosed. In answering this question, the CJEU might take into account, in light of the right to an effective remedy, that the information concerning the specific recipients may be necessary in order to allow the data subject to exercise her rights *vis-à-vis* the recipients of personal data concerning her.

Impact on national case law in Member States other than the one of the court referring the preliminary question to the CJEU

Italy
The Italian case law addressed the question of the relationship between information provided to the data subject and the effective possibility for the data subject to exercise her rights. For example, in a dispute concerning the violation of the data subject's right of access, the Court of Rome, in its judgment of 12 April 2012, stated that, "the omission or incompleteness of information [may] result in an obstacle to the exercise of the right against whom that right has been violated". The Court affirmed that a function of the right of access is to allow the data subject to exercise their claims in relation to unlawful data processing and to know, according to a principle of transparency, the manner in which the processing of personal data concerning them has taken place.
Furthermore, the Supreme Court of Cassation in the judgement of 16 April 2015, n. 7755, stated that Article 2, recognising fundamental rights and Article 24, providing the right to bring an action before the court of the Italian Constitution require that when personal data is processed unlawfully or incorrectly there should be the possibility of seeking for an injunction.

Spain
Spanish Courts considered the right to know at all times who is processing personal data and what use is being made of it as part of the fundamental right to data protection, as provided also by Article 18(4) of the Spanish Constitution (*Tribunal Constitutional,* n. 292, 30 novembre 2000).

Poland
Within the judgements on the provision of information about data processing, Polish court has explicitly referred to the interplay between data/privacy protection and information to be provided to the data subject considering the importance of the latter for the exercise of data subjects' rights (Judgement of the of District Administrative Court in Warsaw of 11 December 2019, case No. II SA/Wa 1030/19).

A company, whose main activity was provision of information services, ran a database with information of natural persons who were self-employed (either conduction economic activities in past or currently). The data processed in this system were obtained from publicly available sources, including public registers. Prior to the GDPR coming into force, the company informed data subjects about data processing using the e-mail addresses stored within the above system (682 439 persons out of 7 594 636) and published an information in this regard on its website. With respect to 181,142 people, the company only had mobile phone numbers, and with regard to 6,499,226 people — mailing addresses, of which 2,924,443 records related to inactive business activities. The company explained that the implementation of the information obligation in its basic form (i.e., individual contact with each data subject) would cause a "disproportionate effort" on the part of the company, as referred to in Article 14 paragraph 5.b of Regulation 2016/679. It would constitute an organisational burden which would critically disrupt the functioning of the company, and possibly even result in its closure. In light of the above, the company decided not to inform remaining data subjects individually.

Polish Data Protection Authority saw this decision as infringing the information obligations under Article 14 paragraph 1 and paragraph 2 of Regulation 2016/679. In this context, the court followed the view presented by the Data Protection Authority and stated that sending the information referred to in Article 14 Regulation (EU) 2016/679 by traditional mail, to the address of the self-employed person (regardless of whether this activity has been suspended) as well as contacting this person via telephone is neither impossible not requires a disproportionate effort in the case of the company processing the addresses and the telephone numbers of these data subjects. However, the sanction applied by the Data Protection Authority (fulfilment of the information obligation was supposed to be accompanied with payment of an administrative fine of 943.470,00 PLN) could not be considered proportionate. Not only the seriousness of the infringement at hand (namely, the persons who were individually informed could have been deprived of the possibility to exercise their rights under data protection law) should be taken into account when deciding on the administrative fine, but also the effectiveness, dissuasiveness and proportionality of the sanction must be granted. However, the sanction must correspond with the characteristics of the infringer so that it is effective, dissuasive and proportionate in this particular case. Thus, the sanction (especially the height of fine) cannot be determined so that it is dissuasive not only for the infringer but also for all the potential and future administrators.

The Netherlands

The decision issued by the Council of State, on 2 October 2019, 201802949/1/A3 is of particular interest. In this case, the appellant requested a copy of his personal data which had been processed by the Mayor and Municipal executive (College). The College had used his data to send three letters, and shared this information with the appellant as requested. The Association of Dutch Municipalities (VNG) posted a copy of the access request made by the appellant on their forum, as an example to show municipalities how to deal with such requests. This forum post was wrongly not anonymised. The appellant requested the College to provide a list of people who had received his information, which was denied. The College argued that it lacked the authority to share details of the people who had received the appellants information. Instead, the appellant should request VGN to provide this information. The Court of first instance ruled that the College could not be held responsible. The appellant appealed this decision, claiming that the College should be held to be responsible.
The Court is tasked with deciding whether the College, in their capacity as data controller, is responsible for the appellant's data becoming available on the VGN forum. In that regard, the Court referred to a previous decision made by the Supreme Court which dictates that the College is responsible for personal data made available on the VGN forum. Secondly, the Court determines whether the College should

have provided the appellant with a list of the recipients of his personal data. The Court followed the CJEU's reasoning in *Holstein* that joint responsibility does not mean that both parties have the same responsibility, as the parties may be involved in different stages of the data processing. Thus, the level of responsibility must be assessed in light of all the relevant circumstances of the case. The Court then goes on to cite the CJEU's reasoning in *Fashion ID* that parties only have the same responsibility under Article 2(d) of Directive 95/46 if they jointly determine the purpose of the processing of the data. A party is not responsible for operations which took place later or earlier in the processing chain. In light of these judgments, the Court considers that the College had the authority to post messages on the forum, as well as delete them. VGN managed access and provided the general accounts and passwords. The College did not have the requisite control over the forum and did not have insight into the recipients of the applicant's data. The Court concludes that for these reasons the College does not have the responsibility to provide a list of recipients to the applicant; he should instead submit a request VGN for this list.

Decisions and opinions of the supervisory authorities, also in light of the GDPR

Working Party Article 29 and EDPB

With regard to the interpretation of information duties the supervisory authorities seem to adopt a broad interpretation, which takes into account its importance in order to grant the effectiveness of data subject's rights. Within the WP29's *Guidelines on Transparency under Regulation 2016/679*, endorsed by the EDPB on 25 May 2018, the principle of transparency has been interpreted as a concretisation of the principle of fairness, enshrined in Article 8(2) CFREU. Moreover, the Working Party Article 29, also on the basis of recital 39 EU Regulation 2016/679 states that on the basis of the information provided, the data subject should be able to understand in advance what the scope of the processing is and what its consequences are, and they should not be surprised by the way personal data concerning them are used.

In relation to the "right to an explanation" in case of automated decision making (Article 22, 13 and 14 GDPR) the *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted by the Working Group Article 29 and endorsed by the EDPB*, provides, with regard to the information on the logic involved, that the data controller must find easy ways to communicate to the data subject the logic or criteria on which the decision is based, without necessarily proving a complex explanation of the algorithms used or the disclosure of the complete algorithm. The information should, however, enable the data subject to understand the reasons for the decision. According to the interpretation of recital 63 EU Regulation 2016/679 given by the Article 29 Working Party, there is no need to explain a particular decision, but rather its consequences. Furthermore, the data controller should provide to the data subject general information useful to contest the decision based on the processing.

With regard to the application of the criterion of the "**disproportionate effort"** set forth in Article 14 EU Regulation 2016/679, according to the WP29's *Guidelines on Transparency under Regulation 2016/679*, endorsed by the EDPB on 25 May 2018, the "disproportionate effort must be directly connected to the fact that the personal data was obtained other than from the data subject", because of the absence of such a criterion in the case of data collected from the data subject (Article 13 GDPR). With regard to the parameters according to which proportionality is to be assessed, the guidelines provide for a comparison, on the one hand, of the effort which the data controller would involve informing the data subject and, on the other hand, of the impact and effects of the failure to inform the data subject.

Italy

With regard to the importance of the information provided to the data subject, the Italian Data Protection Supervisor in several decisions where EU Regulation 2016/679 is applied (GPDP, 19 July 2018, n. 9039945; Decision, 22 February 2018 *Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento UE 2016/679,* n. 8080493) stated the need to inform the person

concerned about the methods of data processing, also in application of the principle of fairness and transparency as per Article 5, paragraph 1, letter a) EU Regulation 2016/679.
With regard to the application of the concept of "**disproportionate effort**", the Italian data protection supervisor (GPDP) referred to its precedents. The GPDP, before the entry into force of the GDPR, had identified some elements to be considered in assessing the existence of a "disproportionate effort" of the data controller. Firstly, the data subject's awareness of the processing is to be considered (GPDP, 26 November 1998, n. 39624). Other elements to be take into account are the nature of the processing (GPDP, 4 April 2001, n. 40763), its purpose (GPDP, 7 February 2001, n. 40967, GPDP, 12 February 2004, n. 634369; GPDP, 24 April 2013, n. 2404305), the nature of data (GPDP, 12 January 2017, n. 6033934), the manner in which the processing is carried out, the number of data subjects (GPDP, 5 July 2017, n. 6845231; GPDP, 31 May 2017, n. 6531135; GPDP, 16 November 2017, n. 7490004; GPDP, 19 January 2017, n. 6093240), the activities necessary to trace them, the date of collection, and the particular high costs for the data controller (GPDP, 26 November 1998, n. 39624; GPDP, 5 July 2017, n. 6845231; GPDP, 12 January 2017, n. 6033934; GPDP, 18 December 2014, n. 3716039).
In practice, the measures taken by the Italian Data Protection Authority focus in most cases on the assessment of the burden of the data controller, and not on the impact on the position of the data subject. In some cases, Italian Data Protection Authority has applied publication as an appropriate measure to protect the data subject.

France
The French data protection authority (*Commission Nationale de l'Informatique et des Libertés,* CNIL) identified some elements to be considered in assessing the existence of a "disproportionate effort", both before and after the entry into force of EU Regulation 2016/679. The CNIL considered the number of data subjects involved (CNIL, délib. 2018-300, 19 July 2018; CNIL, delib. n. 2017-106, 13 April 2017), the technical difficulty (CNIL, délib. n. 2018-151, 3 May 2018), the cost of the measures (CNIL, delib. n. 2018-151, 3 May 2018; CNIL delib. 2016-047, 25 February 2016) and the purposes of processing (CNIL, delib. n. 2011-423, 15 December 2011; CNIL, delib. 2014-301, 10 July 2014). The French authority also considers publication on the data controller's website, even in addition to publication by other means, to be an appropriate measure to protect data subjects (CNIL, delib. n. 2018-360, 13 December 2018; CNIL, delib. 2018-300, 19 July 2018; CNIL, delib. n. 2017-305, 7 December 2017; CNIL, delib. 2015-073, 26 February 2015).

7.4. BOX: Impact of fundamental rights on automated decision-making and profiling

Automated decision-making and profiling may pose a serious risk to fundamental rights (primarily: privacy and data protection, right to an effective remedy and right to a fair trial and due process[64] and prohibition of discrimination), especially due to the lack of transparency and the likelihood of discrimination. As a result, the GDPR sets forth a protective framework which is aimed at minimising a negative impact automated decision-making and profiling might have on the fundamental rights of data subjects.
The GDPR protection mechanisms cover: transparency and fairness requirements, specific accountability obligations, specified legal bases for the processing, rights for individuals to oppose profiling (specifically

[64] See box: : AI, the black box and data subjects' rights: the role of Article 47 CFR

profiling for marketing), and, if certain conditions are met, the need to carry out a data protection impact assessment.

In order to assure lawfulness, fairness and transparency the controller is obliged to provide data subjects with concise, transparent, intelligible and easily accessible information about the processing of their personal data (Article 12(1) GDPR). However, especially in the online environment, the practical efficiency of the safeguards based on the protection by information model is limited due to the information overload effect. Information is likely to be disregarded, unless it is highly specific and corresponds with the interests of the particular data subject. Yet, in light of the Article 13 and 14 GDPR, the catalogue of data that must be provided is lengthy. Thus, the obligation is probable to create a fiction of the data subject knowing and understanding the whole context of data processing instead of *e.g.,* enabling the data subject to make an informed choice in regard to consenting to profiling (Article 6(1) GDPR). In addition, the process of both automated decision-making and profiling are difficult to comprehend by a non-professional and are likely to constitute company's trade secret. Nevertheless, as the Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 suggests, *the controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision.* In this context, the right of access (Article 15 GDPR) might also play a significant role, as it allows data subject to effectively learn about the scope and quantity of personal data which is being processed by the controller.

In addition, use of big data-empowered tools increases the risks of objectionable or illegal discrimination (both direct and indirect).[65] The first obstacle, when aiming at limiting these risks, is the fact that the process of profiling and automated decision-making is opaque which hinders detection of discriminatory patters. Also, their emergence can be caused by different factors: definition of the "target variable" as well as the "class labels", the content and scope of training data, collecting these data, selection of the indicators on which the decision of the AI is based, and proxies. Finally, AI systems can intentionally be used for a discriminatory purpose.[66] Another issue is that the discrimination cannot be easily eradicated with i.a. eliminating certain factors (e.g., ethnicity), as there are usually other indicators, supposedly non-discriminatory (such as home address) which incorporation is likely to lead to the same effect.

As a result, when assessing the impact of fundamental rights on regulation of automated decision-making and profiling, it seems that a key role is played by the automatic and objective safeguards, namely, processing and purpose limitation (Article 5(1) GDPR), data minimisation (Article 5(1) (c) GDPR), storage limitation (Article 5(1)(e) GDPR). They supplement the individual protective toolset (right to rectification, to erasure, to restriction of processing, and right to object) which requires the data subject to actively exercise his rights. Finally, Article 22 of GPDR prohibits decision-making based solely on automated processing in cases where the decision has a legal effect on or similarly significantly affects someone, unless specific requirements are met. It is argued that this provision should be interpreted as encompassing the right to explanation, so that the data subject can learn about the reasoning behind certain decision, and, effectively challenge it in the due procedure (an aspect of the right to an effective remedy and to a fair trial, once the automated decision-making and profiling is used in judicial proceeding).

[See also: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)].

[65] For in-depth analysis see: Jon Kleinberg, Jens Ludwig, Sendhil Mullainathany and Cass R. Sunstein, Discrimination in the age of algorithms, Journal of Legal Analysis 2018, Vol. 10, 113.

[66] Frederik Zuiderveen Borgesius, Discrimination, artificial intelligence, and algorithmic decision-making, https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73.

7.5. BOX: AI, the black box and data subjects' rights: the role of Article 47 CFR

The opaqueness of the automated decision-making (so-called AI black box) may endanger the individual's right to an effective remedy and to a fair trial stipulated in Article 47 CFR. The lack of transparency in this regard is observed on different levels and may equally regard the basis for a decision, factual background taken into account during the decision-making process, the data subject's consent, and the effect of the decision.[67]

Thus, it becomes crucial to interpret Article 22(3) GDPR as granting the data subject a right to explanation. Under Article 22(3) GDPR the data controller is obliged 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*. However, without understanding the reasons behind a decision, it might be impossible to effectively challenge the outcome of the automated decision-making process. Thus, in order to be able data subject to, first, present one's view, and then, to contest a decision which was taken solely automatically, the data subject must know the rationale behind the decision as well as the argumentation and facts upon which it was based. As a result, the data subject should be provided with the concise, transparent, intelligible information on the process of decision-making carried out automatically as only in then they dispose of the data crucial for exercising data subject's rights. As a result, without providing the justification of the decision taken automatically, the guarantees provided for in Article 47 CFREU could be endangered. This issue becomes especially pressing as the application of AI and automated decision-making is being considered not only within private sphere but also in the judicial system.[68]

7.6. BOX: Balancing multiple individuals' rights under article 47 of the Charter. The example of the right to access

The cases where data concerns several data subjects are becoming more and more frequent. An example consists in credit-related data: the information that Mr. Smith owes a sum to Mrs. White concerns both of them. Another case is that of genetic data which concern several individuals, as also recognized by the ECtHR in the case *Marper v. United Kingdom*, 4 December 2008, Rec. n. 30562/04 and 30566/04 and by the Working Group Article 29 in the *Working Document on Genetic Data* of 17 March 2004. Another example is provided by the CJEU in the *Nowak* case, C-434/16, 20 December 2017 where the Court qualified the notes to a written examination test made by an examiner as personal data concerning both the candidate and the examiner.

Personal information in these hypotheses concerns a relationship, for this reason that it seems impossible or highly problematic to distinguish the data concerning each data subject from the information on the relationship. For example: communicating to a bank who is the creditor, but not who is the debtor, is certainly less useful than communicating both names.

The right to access protected by Articles 8(2) CDFUE and 15 GDPR is an example for showing the issue related to the interplay of data subjects' entitlements which have the same data as an object. The

[67] Study on the Human Rights Dimensions of Automated Data Processing Techniques (In Particular Algorithms) And Possible Regulatory Implications Prepared by the Committee of Experts on Internet Intermediaries (MSI-NET) 2018, https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5, 23-26.

[68] In regard to criminal justice see i.a.: Aleš Završnik, Criminal justice, artificial intelligence systems, and human rights, ERA Forum 20, 567–583 (2020). https://doi.org/10.1007/s12027-020-00602-0; and to civil proceeding: *Maria Dymitruk, The right to a fair trial in automated civil proceedings, Masaryk University Journal of Law and Technology 2019,* 13(1), 27.

GDPR already gives account to this issue: the last paragraph of Article 15 (right to access and to copy) states: "the right (...) must not infringe the rights and freedoms of others".
The question arises of how the right to access can be exercised, taking into account the right to access and the right to data protection of each data subject. In this respect, the exercise of the right to copy or portability that does not include relational information, which are personal to various data subjects, would be very weakened, because the information is relational, as seen in the examples above. Furthermore, a risk of veto emerges with respect to the reciprocal exercise of rights, which could put in nothing — or at least significantly weaken — the exercise of the right to access. This may result in the difficulty to take legal action based on the information obtained through the exercise of this right. Article 47 comes into play.
Therefore, in order to coordinate the right to access with the right to data protection to other data subjects, the last paragraph of Article 15 EU Regulation 2016/679 could be interpreted in light of Articles 8 and 47 CDFUE. From this perspective, if the collection of data by a data subject, necessary to the exercise of the right to access falls within the scope of application of the GDPR and data are not of sensitive nature, it could be argued that the data subject exercising the right to copy pursue a legitimate interest in the collection of data that also concerns other data subjects (Article 6(1)(f) GDPR).

8. Data protection and procedural rules: the impact of the Charter

8.1. Introduction

The right to a fair trial enshrined in Article 47 of the Charter has several consequences for the conduct of national proceedings, and it is relevant to compare these consequences with those attached to the right to data protection. It has been shown, for instance, how these principles impact the lawfulness of a national rule according to which a judicial remedy may be sought only once all administrative remedies have been exhausted (see the analysis of *Puškár* in Chapter 4, question 1).

This chapter will focus on several issues concerning the conduct of proceedings:

- the admissibility of evidence concerning a breach of data protection in court;
- the impact of the principles of proportionality and effectiveness, Article 8 and Article 47 CFREU on the regulation on access to personal data which are necessary for initiating civil proceedings
- the use of evidence derived from an unlawful processing in proceedings

Moreover, it is provided an informative box on collective redress under the GDPR.

Main questions addressed:

1. Can a list held by a financial authority of a Member State, which contains the claimant's personal data and the inaccessibility which has been secured against unauthorised disclosure or access, be regarded as unlawful evidence by virtue of the fact that it was obtained by the claimant without the lawful agreement of the relevant financial authority? Should the referring court refuse to admit this evidence in accordance with the requirements of EU law on a fair hearing in the second paragraph of Article 47(2) of the Charter?

2. With observance of principles of proportionality and of effectiveness, do Articles 8 and 47 of the Charter might be interpreted in a way that one has a granted right to have access to personal data which enables instituting civil proceedings?

3. In light of the right to a fair hearing laid down by Article 47 (2) of the Charter, can evidence derived from an unlawful processing be produced and used in court?

Cluster of relevant CJEU cases

➢ Judgment of the Court (Fourth Chamber) of 11 December 2014, *František Ryneš v. Úřad pro ochranu osobních údajů*, Case C-212/13 (**Ryneš**)

➢ Judgment of the Court (Second Chamber) of 27 September 2017, Peter Puškár v Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy, Case C-73/16, (***Puškár***)

➢ Judgment of the Court (Second Chamber) of 4 May 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA, Case C-13/16, (***Rīgas satiksme***)

➢ Judgment of the Court (Third Chamber) of 25 January 2018, Maximilian Schrems v Facebook Ireland Limited, Case C-498/16 (***Schrems II***)

➢ Judgment of the Court (Second Chamber) of 29th July 2019, Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV, Case C-40/17, (***Fashion-ID***)

➢ Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 15 July 2020 — *Facebook Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände — Verbraucherzentrale Bundesverband e.V*, Case C-319/20 (**Facebook Ireland Limited**) [pending]

Relevant legal sources:

EU Level

Charter of Fundamental Rights of the EU:

Article 6 (right to security of the person), Article 7 (right to private life), Article 8 (right to the protection of data), Article 47 (right to an effective remedy and to a fair trial) and Article 52 (scope of guaranteed rights).

Directive 95/46 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 (no longer in force)

Article 3 – Scope; Article 7 Criteria for making data processing legitimate; Article 8 – The processing of special categories of data; Article 9 – Processing of personal data and freedom of expression; Article 12 - Right of access

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)

Article 17 – Right to erasure ('right to be forgotten'); Article 80 – Representation of data subjects; Article 6 – Lawfulness of processing; Article 15 Right of access by the data subject

8.1.1. Question 1: Right to have access to personal data which enables instituting civil proceedings in light of Articles 8 and 47 of the Charter and of the principles of proportionality and effectiveness.

With observance of principles of proportionality and of effectiveness, might Articles 8 and 47 of the Charter be interpreted in a way that one has a granted right to have access to personal data that enables instituting civil proceedings?

Within the cluster of cases, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts on the question being considered:

➢ Judgment of the Court (Second Chamber) of 4 May 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde v Rīgas pašvaldības SIA, Case C-13/16, (***'Rīgas satiksme'***)

Relevant legal sources:

National Level

Latvian Law on the protection of personal data, of 23 March 2000 (Law No 123/124)

Article 7 of that law, which seeks to transpose Article 7 of Directive 95/46, provides that the processing of personal data is to be authorised only if that law does not provide otherwise and if at least one of the following requirements is met:

'[...] (3) processing is necessary for compliance with a legal obligation to which the controller is subject; [...]

(5) 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 in a third party to whom the data are disclosed;

(6) processing is necessary for the purposes of the legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.'

The case

In December 2012, a road accident occurred in Riga. A taxi driver parked his vehicle on the side of the road with a passenger in the rear. He opened the door to leave the car right when a trolleybus belonging to *Rīgas satiksme* was approaching. The door scrapped against and damaged the trolleybus. Administrative proceedings were initiated resulting in imposing sanctions. In order to compensate its damage, *Rīgas satiksme* sought payment from the insurance company that initially declined to pay any compensation, stating that responsibility for the incident would be held by a passenger who opened the door, not the taxi driver. It recommended *Rīgas satiksme* to bring civil proceedings against the passenger.

Rīgas satiksme applied then to national police for providing the following details of a passenger (who was earlier sanctioned by an administrative penalty) so that civil proceedings would be initiated: first name and surname, identity document number, and address. National police only partially responded to the request, having disclosed only the name and surname of the passenger. The decision of the police was based on the fact that under Latvian law, only parties to administrative proceedings leading to sanctions might be granted access to information in the case file. Moreover, Latvian Administrative Infringements Code entitles a person to be given the status of a victim in an administrative proceeding leading to sanctions by the body or official responsible for examining the case only upon such person's prior expressed request. And *Rīgas satiksm*e did not exercise that right.

Rīgas satiksme brought an administrative law action before the District Administrative Court against the decision issued by the national police. By judgement of 16 May 2014, the court upheld the action and ordered the national police to provide *Rīgas satiksme* with the information relating to the identity document number and place of residence of the taxi passenger. But the national police brought a cassation before the Administrative Division of the Supreme Court. That court asked for an opinion from the National Data Protection Agency,. The Agency responded that Article 7(6) of the Law on the Protection of Personal Data does not serve as a legal basis for providing personal data in the case, as the Latvian Administrative Infringements Code enumerates persons to which the national police may disclose the information relating to a case. Instead, as the relevant legal basis the Agency identified paragraphs 3 and 5 of that article. Above all, Article 7 does not oblige the data controller (national police in this case) to process the data, but merely permits him to do so.

Additionally, the Agency explained to *Rīgas satiksme* how the latter one might acquire demanded data, identifying two possible options:

(a)submitting a reasoned request to the Civil Registry; or
(b)applying to the court for the production of evidence; as a result a court would issue an injunction obliging the national police to reveal the personal data of a passenger subsequently used by *Rīgas satiksme*

in civil action against the passenger.
However, the referring court expressed doubts on the means of obtaining the personal data indicated by the Agency. First of all, it stated that the application made to the Civil Registry mentioning only the name and surname of the taxi passenger would be insufficient to identify the person, as many others would share the same name. Secondly, it affirmed that in order to bring a civil action, under national law on the provision of evidence, the applicant (*Rīgas satiksme* in that case) would need to know at least a place of residence of the defendant.

Preliminary question(s) referred to the Court:

In the first question, the referring court essentially asks whether Article 7(f) of Directive 95/46 must be interpreted as imposing the obligation to disclose personal data to a third party in order to enable him to bring an action for damages before a civil court for harm caused by the person concerned by the protection of that data.

Reasoning of the Court:

The Court underlines in its reasoning that it lays within the competences of Member States to provide the conditions determining, with the observance of the limits of the Directive 95/46, when the processing of personal data is lawful. Crucial here is its Article 7 laying down an exhaustive list of situations in which such processing is permitted. The case is relevant to point (f) of the Article which allows the processing if it is necessary for the purposes of the legitimate interests pursued by the controller (national police) or by the third party to whom the data are disclosed (*Rīgas satiksme*), except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (passenger of the taxi). The Court affirmed that from the wording of Article 7(f) of the Directive stems no obligation of data controller to process such data, but barely a possibility to provide the data to an interested entity, such as a third party having an interest in familiarising themselves with the data. That reasoning stands in line with the Opinion of AG (points 43-46) and in consequence leads to the statement that *no right is granted for persons that ask for access to data* (see: Opinion of AG, point 41). Such interpretation of the Directive's provisions is analogical to one featured also *inter alia* in the case *Promusicae*, C-275/06. However, a sole existence of possibility for the data controller to process the data would not preclude providing such data to interested entities under national law, with the observance of conditions laid down in Article 7(f). The structure of the provision itself indicates the existence of three cumulative conditions:

- the pursuit of a legitimate interest;
- the need to process personal data for the purposes of the legitimate interests pursued;
- fundamental rights and freedoms of the person concerned by the data protection do not take precedence.

As for the condition of the pursuit of a legitimate interest, the Court well stated that if a third person (in that case – *Rīgas satiksme*) demands access to personal data of a subject that damaged their property for the purpose of bringing civil action, then doubtlessly the condition is absolutely fulfilled.

With regard to the condition of need, the Court recalled, having invoked previously issued judgements (*i.e., Ryneš*, C-212/13), that derogations and limitations to the right of protection of data (guaranteed by Article 8 of the Charter) must apply only when they are strictly necessary. In that way, it supported the opinion of the AG who evoked the principle of proportionality in relation to aim and chosen means (see: Opinion of AG, points 70 and subs.). Accordingly, the Court claimed that in the situation when obtaining data consisting of place of residence and identity card number of a subject for the purpose of bringing civil action and in consequence, defending own rights seems necessary.

And finally, in reference to the last condition, the Court simply admitted that when balancing the opposing rights and interests at stake, into account must be taken the specific circumstances of the particular case. In other words, there is no universal mechanism of deciding whose interests – those of data subject or those of data controller/third party prevail, and therefore such balancing of opposing rights must be made "case-by-case".

Conclusion of the Court:

The Court ruled that under Article 7(f) of the Directive 95/46 there is no obligation to disclose personal data to third party in order to enable them to bring an action for damages before a civil court for harm caused by the person concerned by the protection of that data. However, Article 7(f) of that directive does not preclude such disclosure on the basis of national law.

By such a conclusion, the Court in fact confirmed that no person has a "right" to access personal data that is necessary for them to institute civil proceedings, as relevant data controller has only a "possibility" under certain circumstances to provide such data, and no such "obligation". However, the Court did not exclude an option for a person who seeks to defend their legal claims to obtain such data (and therefore exercise their right guaranteed by Article 47 of the Charter). In that case it is necessary that cumulatively exist three conditions laid down in Article 7(f) of the Directive (see: *supra*). The Court by its ruling made clear that decisive in conflict of rights and interests of two persons — data subject and data controller/third party asking for access to data is principle of proportionality. On one hand, concerned must be rights of data subjects stemming from Articles 7 and 8 of the Charter. On the other hand, bared in mind should also be a right enshrined in Article 47 of the Charter of a person whose property was damaged. In relation to that, an appropriate balancing must be made on the case-by-case basis.

Last but not least, the conclusion of the Court assures the observance of the principle of effectiveness, as it clarified that national law principles, in accordance with provisions of the Directive 95/46, should enable (but not oblige) data controller to provide personal data to a third party if the latter one has justified interests. In that way, national law would provide accurate level of protection of fundamental rights.

Elements of judicial dialogue:

The Court frequently evoked its previous decisions in relation to three conditions of lawfulness of personal data processing (under Article 7(f) of the Directive 95/46) in the case. When relating to the first condition on the pursuit of a legitimate interest, the Court underlines importance of interest of person whose property was damaged or infringed in general similarly in line with the judgement in case *Promusicae* (C-275/06), that also featured conflict between an interest of person who suffered damage and protection of data from disclosure.

When recalling the second condition, the Court evoked several cases (*Volker und Markus Schecke* and *Effert*, C-92/09 and C-93/09, *IPI*, C-473/12) the most recent being *Ryneš*, C-212/13 in which it literally repeated that derogations and limitations to right of protection of data might be applied only when it is absolutely necessary.

And regarding the last condition on precedence of rights and freedoms of data subject (stemming from Article 7 and 8 of the Charter), the Court repeated its reasoning established in a handful of cases (*ASNEF* and *FECEMD*, C-468/10 and C-469/10, *Breyer*, C-582/14).

The judgement in *Rigas Satiksme* also stands in line with the one issued in *Puškár* case (C-73/16) in question of balancing access to justice and to one's personal data (see: *supra*).

Impact on national case law in Member States different from the state of the court referring the preliminary question to the CJEU:

Poland

The issue of processing personal data for the purpose of instituting civil action against data subject has been frequently evoked before Polish Courts, both before and after adoption of the new GDPR. An act that served as a basis for claims was Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Personal Data Protection Act from 29 August 1997, hereinafter "PDPA") transposing the Directive 95/46 that stipulated in its Article 23(1) point 5 that processing of data is permitted for the *purpose of the legitimate interests pursued by the controllers or data recipients, provided that the processing does not violate the rights and freedoms of the data subject.*

The interpretation of the above mentioned provision by national courts in Poland leads to conclusion that it allows interested entities obtention of personal data of third parties for the purpose of instituting civil action that would defend their rights. Such view was expressed *inter alia* by Naczelny Sąd Administracyjny (Supreme Administrative Court) in its judgement I OSK 454/16. The Court rejected the action brought by the A S.A. on the judgement of the Wojewódzki Sąd Administracyjny w Warszawie (Provincial Administrative Court in Warsaw) in the case concerning action brought by H.R. on the decision of data protection authority. H. R. requested from the data protection authority to order A S. A. (operator of the forum) to disclose some pieces of data of internet users who had published comments on public forums insulting her. H. R. explained in the request that she needed the data (consisting of names, surnames, IP addresses) to institute legal proceedings against data subjects. Although the initial decision of the authority was negative (which was based *inter alia* on the statement that H. R. no longer had legal interest), the Provincial Administrative Court affirmed in its judgement that a mere fact that a requesting person needs the data to bring a civil action constitutes the legitimate interest and therefore should be accepted by the data protection authority.

The interpretation of the above mentioned provision by national courts in Poland leads to conclusion that it allows interested entities obtention of personal data of third parties for the purpose of instituting civil action that would defend their rights. Such view was expressed *inter alia* by Naczelny Sąd Administracyjny (Supreme Administrative Court) in its judgement I OSK 454/16. The Court rejected the action brought by the A S.A. on the judgement of the Wojewódzki Sąd Administracyjny w Warszawie (Provincial Administrative Court in Warsaw) in the case concerning action brought by H.R. on the decision of data protection authority. H. R. requested from the data protection authority to order A S. A. (operator of the forum) to disclose some pieces of data of internet users who had published comments on public forums insulting her. H. R. explained in the request that she needed the data (consisting of names, surnames, IP addresses) to institute legal proceedings against data subjects. Although the initial decision of the authority was negative (which was based *inter alia* on the statement that H. R. no longer had legal interest), the Provincial Administrative Court affirmed in its judgement that a mere fact that a requesting person needs the data to bring a civil action constitutes the legitimate interest and therefore should be accepted by the data protection authority.

8.1.2. Question 2: Admissible evidence of a violation of data protection

Can a list held by a financial authority of a Member State, which contains the claimant's personal data and the inaccessibility of which has been secured against unauthorised disclosure or access, be regarded as unlawful evidence by virtue of the fact that it was obtained by the claimant without the lawful agreement of the relevant financial authority? Should the referring court refuse to admit this evidence in accordance with the requirements of EU law on a fair hearing in the second paragraph of Article 47(2) of the Charter?

Within the cluster of cases, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts on the question being considered:

➢ Judgment of the Court (Second Chamber) of 27 September 2017, Peter Puškár v Finančné riaditeľstvo Slovenskej republiky, Kriminálny úrad finančnej správy, Case C-73/16, (***Puškár***)

Presentation of the case and national legal sources:

The facts of the case and the relevant national legal sources have been fully presented in Chapter 6 (question 1&2). It shall simply be recalled that Mr. Puškár managed to obtain a list established by the Slovak Finance Directorate, the content of which was not meant to circulate beyond the administrative offices. Several items of personal data relating to him were on the list, and he requested their removal. Mr. Puškár never claimed or proved that he had obtained the list with the consent, legally required, of the Finance Directorate or the Financial Administration Criminal Office.

The Najvyšší súd Slovenskej republiky (Supreme Court of the Slovak Republic) decided to refer several questions to the CJEU for a preliminary ruling. Among these, question 3 is directly related to the issue in the box.

Preliminary question(s) referred to the Court:

In the third question, the referring court asked, in essence, whether Article 47 of the Charter must be interpreted as meaning that a national court cannot reject, as evidence of an infringement of the protection of personal data conferred by Directive 95/46, a list drawn up by a public authority, submitted by the data subject and containing personal data relating to him, if that person had obtained that list without the consent, legally required, of the person responsible for processing that data.

Reasoning of the Court:

The Court started its reasoning by stating outright that the rejection of the list as evidence of an infringement of the rights conferred by Directive 95/46 constitutes a limitation on the right to an effective remedy before a court within the meaning of Article 47 of the Charter. In accordance with Article 52(1) of the Charter, such a restriction is justified only if it is provided for by law, if it respects the essence of that right and, subject to the principle of proportionality, if it is necessary and genuinely meets objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others.

The court consequently urged the referring court to verify if these conditions are met. Concerning, more particularly, the condition whether such a rejection affects the essential content of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter, the Court specified that it will be necessary for the referring court to ascertain whether the existence of the contested list or the fact that it contains personal data relating to Mr Puškár are being challenged in the context of the dispute in the main proceedings and, where appropriate, if he has other evidence in that regard. In other words, is the piece of evidence relevant, and crucial, to the claimant's case? The principle of effective access to justice underlies the Court's analysis, since it prompts national courts to weigh the role of the disputed piece of evidence in the proceedings.

Concerning the condition that the rejection of the contested list as evidence must be necessary and does in fact satisfy objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others, the Court leaved this appreciation to the national court, subject to clear guidelines. The purpose of protecting the right of the persons whose data appears in these documents might justify a refusal to allow the unauthorized internal documents to be produced in judicial proceedings. However,

the Court stressed that the referring court should ascertain whether such a rejection ***does not disproportionately affect the right to an effective remedy*** before a court referred to in Article 47 of the Charter.

Then, the Court stated that if the person whose personal data is on the list enjoys a right of access to that data, such rejection appears disproportionate to those very objectives. Since Article 12 of Directive 95/46 guaranteed everyone a right of access to the data collected relating to him, and that such right might be limited only under certain conditions by the Member States, the referring court should assess the proportionality of a rejection of the disputed list as evidence, by examining whether its national legislation limits, in relation to the data included in the list, the rights to information and access laid down in Articles 10 to 12 of Directive 95/46 and, where appropriate, if such a limitation is justified. In any case, the Court stressed that a case- by-case examination must be undertaken to verify whether the objectives pursued by national legislation through such limitation, take precedence over the interest in protecting the rights of the individual and whether, in the proceedings before that court, other means exist to ensure that confidentiality, in particular regarding the personal data of other natural persons included on that list.

Conclusion of the Court:

Article 47 of the Charter must be interpreted as meaning that a national court cannot reject, as evidence of an infringement of the protection of personal data conferred by Directive 95/46, a list drawn by a public authority, submitted by the data subject and containing personal data relating to him, if that person had obtained that list without the consent, legally required, of the person responsible for processing that data, unless such rejection is laid down by national legislation and respects both the essential content of the right to an effective remedy and the principle of proportionality.

To some extent, the right of access to justice enshrined in Article 47 could be interpreted in conjunction with the data subject's right to access to personal data concerning him as encompassing a right to produce evidence based on documentation including personal data of the person having the right of access to justice.

As a consequence, the role of the court becomes more complex, because it may not only ascertain whether evidence is lawfully produced but, in case of unauthorized evidence, it should also consider whether the legal restriction infringed represents a disproportionate burden for the party providing that evidence, in fact violating her right to access to justice.

Elements of judicial dialogue:

The Court relies on several previous decisions to justify its finding that the objective of avoiding the unauthorised use of internal documents in judicial proceedings is capable of constituting a legitimate general interest objective (*Austria v Council, C-445/00*; *Stadtgemeinde Frohnleiten and Gemeindebetriebe Frohnleiten*, C-221/06, *Donnici v Parliament*, C-9/08, not published).

Furthermore, the CJEU considered that any restrictions on the right of access of a person to data related to him, even when intended to safeguard the prevention, investigation, detection and prosecution of criminal offences or an important economic or financial interest of a Member State, have to be imposed by legislative measures (*Bara and Others* v Commission, C-201/14).

The reasoning of the Court in *Puškár* is directly in line with the approach endorsed by the Court in its case law analysed in Chapter 3, under question 2 (*Lindqvist, ASNEF and FECEMD, Promusicae, Scarlet Extended, Google Spain, Ryneš, Breyer, Rigas Satiksme*) since the issue of the admissibility of evidence must be solved in light of the balance of the conflicting interests at stake, including the right to effective access to justice and to a fair trial. In particular, there is a clear link, on the question being considered, between *Puškár* and *Rigas Satiksme*, although the latter does not expressly refer to the former, since in *Rigas Satiksme*

the issue at stake is whether data protection should prevail over effective access to justice, when the disclosure of data is a pre-condition to enable the victim of a road accident to identify the person responsible for the accident and thus bring civil proceedings against that person (the data subject).

Unlike in *Puškár*, where the right of access to justice finds an ally in the right to access one's own personal data, in *Rigas Satiksme* the right of access to justice represents a limitation on the data subject's protection, the latter being a potential defendant in the court case. Unlike in *Puškár*, Article 47 is not referred to. However, the national court is again requested to strike a similar balance to the one defined in *Puškár*: a balance in which, provided that access to a third party's personal data is strictly necessary to access the court to defend one's own rights, the nature and the scope of such data protection is weighed against the scope of judicial protection sought by the other party.

Impact on national case law in Member States different from the state of the court referring the preliminary question to the CJEU:

Italy

From the Italian perspective, *Puškár* can be expected to have a different impact in criminal and civil cases. With regard to the former, Article 191 of the Italian Criminal Procedure Code provides that unlawfully acquired evidence may not be used by the court, and this violation may be ascertained by the judge *ex officio* at any stage of the proceedings. A recent judgement of the Criminal Court applied this provision strictly, ruling that the right to defence could not be a sufficient ground for an accused to access telephone records beyond the time limit established by law (*Corte di cassazione penale*, no. 15613/2015).

No similar provision to Article 191, cited, exists in the civil procedural code and, proceeding from this consideration, civil courts hold that no (automatic) limitation may be applied to evidence brought before the judge in violation of data protection. Whereas such violation may be relevant in other respects (e.g., for a separate claim in tort by the aggrieved person), the evidence may be assessed by the judge, whether it is gathered lawfully or unlawfully (Tribunal of Bari, 16.2.2007). At the same time, civil courts hold that a balancing is needed between the right to a defence and the right to privacy, and this balancing must be based on concrete criteria (Court of Cassation, no. 18279/2010). In a recent judgement concerning child custody, the Tribunal of Rome endorsed this approach and dismissed a father's argument, based on data protection, against the use of video-recorded images showing him taking drugs on a day on which the child was in his custody. The balance was definitively found to be in favour of the mother's right to defend the minor's rights in such a dangerous context.

The Netherlands

ECLI:NL:GHSHE:2018:166 (Court of Appeal in 's-Hertogenbosch)

This case concerned the cost of a request based on the Dutch law on the protection of personal data. After referring to the *Puška´r* case (C-73/16) as an example, the Court explained that the CJEU has consistently held that it is for the courts of the Member States to ensure judicial protection of the rights which individuals derive from EU law, thereby providing for the necessary legal means to ensure effective legal protection in the fields covered by EU law. This obligation is linked to the right laid down in Article 47 of the Charter, under which anyone whose rights and freedoms guaranteed by Union law are violated is entitled to an effective remedy. Member States must, when they lay down the procedural provisions for legal actions instituted to safeguard the rights conferred by Directive 95/46, respect the guarantees of the right to effective judicial remedy provided for in Article 47 of the Charter. The principle of effectiveness means that national procedural rules must not, in practice, render the exercise of the rights

conferred by Community law impossible or excessively difficult. The Court then stated that the levying of court fees can be seen as a financial restriction on access to justice. However, such a restriction is permitted, provided that at least a number of requirements are met, namely that the restriction is set by law, that access to justice is not fundamentally compromised, that there is a legitimate purpose and that the principle of proportionality is respected (cf. Article 52 (1) of the Charter).

8.1.3. Question 3: Evidence obtained through unlawful processing of data

3. In light of the right to a fair hearing laid down by Article 47 (2) of the Charter, can evidence derived from an unlawful processing be produced and used in court?

Within the cluster of cases, identification of the main case that can be presented as a reference point for judicial dialogue within the CJEU and between EU and national courts on the question being considered:

➢ Judgment of the Court (Fourth Chamber), 11 December 2014, *František Ryneš* v. *Úřad pro ochranu osobních údajů*, Case C-212/13 (***Ryneš***), read in light of the subsequent decision of the Court in ***Puškár***

➢ Judgment of the Court (Grand Chamber) of 6 October 2020, *La Quadrature du Net and Others v Premier ministre and Others*, Joint Cases C-511/18, C-512/18 and C-520/18 (***La Quadrature du Net***)

Relevant legal sources:

National Level

Czech Law No 101/2000 Sb. on the Protection of Personal Data and the Amendment of Various Laws ('Law No 101/2000'), implementing Directive 95/46

Paragraph 3(3): 'This Law does not cover the processing of personal data carried out by a natural person solely for personal use.'

Paragraph 44(2), which governs the liability of the personal data controller, who commits an offence if he processes that data without the consent of the data subject, or if he does not provide the data subject with the relevant information or if he does not comply with the obligation to report to the competent authority.

Paragraph 5(2)(e) of Law No 101/2000, according to which the processing of personal data is in principle only possible with the consent of the data subject. In the absence of such consent, personal data may be processed where doing so is necessary to safeguard the legally protected rights and interests of the data controller, recipient or other data subjects. However, such processing must not adversely affect the data subject's right to respect for his private and family life.

The case(s):

For around 6 months, Mr Ryneš, whose home and family had suffered several attacks, installed and used a camera system located under the eaves of his family home. The camera, installed in a fixed position, recorded the entrance to his home, the public footpath and the front door entrance to the house. The system allowed only a visual recording, which was stored on recording equipment in the form of a continuous loop, that is to say, on a hard disk drive. As soon as it reached full capacity, the device would record over the existing recording, erasing the old material. No monitor was installed on the recording equipment, so the images could not be studied in real time. Only Mr Ryneš had direct access to the system and the data.

On the night of 6 to 7 October 2007, a further attack took place. One of the windows of Mr Ryneš's home was broken by a shot from a catapult. The video surveillance system at issue made it possible to identify two suspects. The recording was handed over to the police and relied on in the course of the subsequent criminal proceedings. One of the suspects lodged a request for confirmation that Mr Ryneš's surveillance system was lawful.

The *Úřad pro ochranu osobních údajů* (Czech Office for Personal Data Protection; 'the Office'), found that Mr Ryneš had infringed Law No 101/2000, since:

– as a data controller, he had used a camera system to collect, without their consent, the personal data of persons moving along the street or entering the house opposite;
– he had not informed those persons of the processing of that personal data, the extent and purpose of that processing, by whom and by what means the personal data would be processed, or who would have access to the personal data; and
– as a data controller, Mr Ryneš had not fulfilled the obligation to report that processing to the Office.

Mr Ryneš' action challenging that decision was dismissed by the *Městský soud v Praze* (Prague City Court), and Mr Ryneš appealed. The *Nejvyšší správní soud* decided to stay proceedings and refer a question to the CJEU for a preliminary ruling.

Preliminary question(s) referred to the Court:

In its question, the referring court essentially asked whether, on a proper construction of the second indent of Article 3(2) of Directive 95/46, the operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, amounts to the processing of data in the course of a purely personal or household activity, for the purposes of that provision.

Reasoning of the Court:

This question of the material scope of the protection, in relation to the exception to its application laid down in article 3 (2) of Directive 95/46, has been dealt with in Chapter 2. The Court concludes that video surveillance even partially covering a public space is not a 'purely personal or household activity' and thus falls under the regime of data protection. However, as mentioned in Chapter 4, the Court implicitly invites national authorities, in the implementation of national law, to follow the methodology described in Chapter 4 in order to the balance the right to data protection and to privacy, with the legitimate interests of the controller to protect his home and family.

The Court does not deal, either expressly nor implicitly, with the question in the box, whether evidence allegedly obtained through an unlawful processing of personal data may be used in courts. However, it

may be inferred from its decision, combined with the subsequent decision given in *Puškár*, that in order to answer the question, the following reasoning is to be undertaken by national judges. Generally speaking, judges should rely on the principle of proportionality to balance the right to protection of private life and data protection of the data subject with conflicting rights of the controller, such as the right to protect his home and safety as stressed in *Ryneš*.

Although not mentioned by the court, the right of the controller to effective access to justice which is at stake, where the admissibility of evidence is in question could also be balanced with the rights of the data subject, since the use of data is in that case a decisive condition for the conviction of the defendants. It is only after making such assessment in light of the principle of proportionality, with due consideration given to the right to a fair trial, that judges should decide if evidence obtained in violation of the protection of personal data may be produced in court. In *Puškár*, the Court implicitly considers that the mere fact that the document unlawfully obtained includes other persons' data, subject to protection, does not preclude its production in court if such a production proves to be crucial to guarantee the holder of the document effective access to justice.

Conclusion of the Court:

As mentioned above, the Court's conclusion, according to which video surveillance even partially covering public space is not a 'purely personal or household activity' and thus falls under the regime of data protection, does not directly answer the question being considered. However, by clustering this case with the above decisions adopted in the *Puškár* and *Rigas* cases, scope can be seen for a similar balancing based on the principle of proportionality.

Impact on the follow-up case:

On 25 February 2015, the referring court made a final judgement on the case. It repealed the decision of the Office, stating that the Czech law on protection of data did not give a clear indication whether installation of a security surveillance camera falls under its provisions (hence the decision to refer to the Court). Moreover, the Office, whose task is to clarify vague wording of legal provisions failed to do so, having issued different decisions in similar cases. Therefore, it was not possible to punish those who installed a camera system on their own family house until December 2014, when the issue of the exception to the applicability of the Personal Data Protection Act was definitively enacted. In view of the referring court, the Office's decision in consequence breached Article 7 §1 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

Elements of judicial dialogue:

As mentioned above, the question requires a joined analysis of *Puškár* and *Rigas*.

Furthermore, recently the CJEU in *La Quadrature du Net* (C-511/18; C-512/18: C-520/18) has stated that a national court may not apply a provision of national law empowering it to limit the temporal effects of a declaration of illegality, which it is bound to make under that law, in respect of national legislation imposing on providers of electronic communications services — with a view to, *inter alia*, safeguarding national security and combating crime — an obligation requiring the general and indiscriminate retention of traffic and location data that is incompatible with Article 15(1) of Directive 2002/58, read in light of Articles 7, 8 and 11 and Article 52(1) CFR. Moreover, the CJEU stated that Article 15(1), interpreted in light of the **principle of effectiveness**, requires national criminal courts to disregard information and evidence obtained by means of the general and indiscriminate retention of traffic and location data in breach of EU law, in the context of criminal proceedings against persons suspected of having committed criminal offences, where those persons are not in a position to comment effectively on that information

and that evidence and they pertain to a field of which the judges have no knowledge and are likely to have a preponderant influence on the findings of fact.

Impact on national case law in Member States different from the state of the court referring the preliminary question to the CJEU:

France

The French *Cour de cassation* had to decide on several occasions whether an employer could produce evidence collected against employees through a data processing system in court, whereas the employer had not fulfilled its obligation to declare the existence of such processing to the French data supervisory authority (CNIL).

Before *Rynes*, in 2014, the French Court had decided:

- that evidence collected through a data processing system which had not been previously declared to the French data protection authority was to be considered as unlawfully obtained and could not be admissible in civil proceedings (Employment Chamber, 8 October 2014, no 13-14.991);

- but that the dismissal of an employee, based on evidence collected through a data processing system, was lawfully founded even if the processing had not been properly declared to the French data protection authority, as long as the implementation of the data processing system constituted a legal obligation of the employer, subject to criminal sanctions (Employment Chamber, 14 January 2014, no 12-16218).

After *Rynes*, in 2017, the French Court reached a more balanced solution: the fact that the employer has not fulfilled its obligation to declare data processing to the French CNIL does not prevent him from producing in court evidence collected against the employee through that system, if the judge finds that the system does not violate the employee's right to private life and the employee must have known that his emails were stored in the system (Employment Chamber, 1 June 2017, n°15-23522).

8.2. Guidelines emerging from the analysis

Enforcement of data protection law for the sake of forthcoming civil proceedings

Domestic courts are not obliged to force disclosure of personal data for the sole purpose of bringing an action for damages before a civil court for harm caused by the person whose data is at stake. There is no particular right to obtain such data that could be enforceable before a domestic court.

Article 47 CFREU may create a ground for claiming such data only in an exceptional situation where three premises are satisfied independently:

- the pursuit of a legitimate interest;
- the need to process personal data for the purposes of the legitimate interests pursued;
- fundamental rights and freedoms of the person concerned by the data protection do not take precedence.

It is for the domestic court to establish whether these three premises have been satisfied in the case.

Evidence obtained illegally

It is impossible for a domestic court to reject a document issued by a public authority that was obtained unlawfully by a data subject whose data this document concerns. The duty to reject may stem only from domestic law — and as long as it respects both the essential content of the right to an effective remedy and the principle of proportionality.

Article 47 CFREU must be read together with the right to access one's own personal data. Such right encompasses a right to produce evidence that is based on documents that include personal data of such an individual.

In this way, the domestic court should carry out a two-tier test:

- In the first step, it is necessary to established whether data has been obtained in a lawful way.
- At a second stage — providing that the evidence has been produced or obtained unlawfully — the domestic judge must assess whether the legal restriction infringed represents a disproportionate burden for the party providing that evidence, in fact violating her right to access to justice.

9. Effective data protection and consumer law: the intersections

9.1. Introduction

Both the case law and EU legislation show the existence of areas of intersections between data and consumer protection. In this chapter the relationship between them is addressed assuming the data protection perspective. **The general question addressed is whether the application of consumer law can ensure the application of the right to an effective remedy (Article 47 CFR) and the right to data protection (Article 8. CFR),** where a natural person is to be qualified both as a consumer and as a data subject.

In this analysis, the fact that the number of data subjects who are not consumers in the online context is increasing should be taken into account. The relationship between users and online platforms is a good example: generally speaking, all users are data subjects *vis à vis* the online platform, but not all of them are consumers. Some of the data subjects cannot be qualified as consumers, but as professionals (e.g., a natural person sells for profit and in an organised manner tablecloths on an online platform, and personal data concerning her are processed by the online platform). The following table shows this relationship (without considering the relationship between users, not relevant for our purposes).

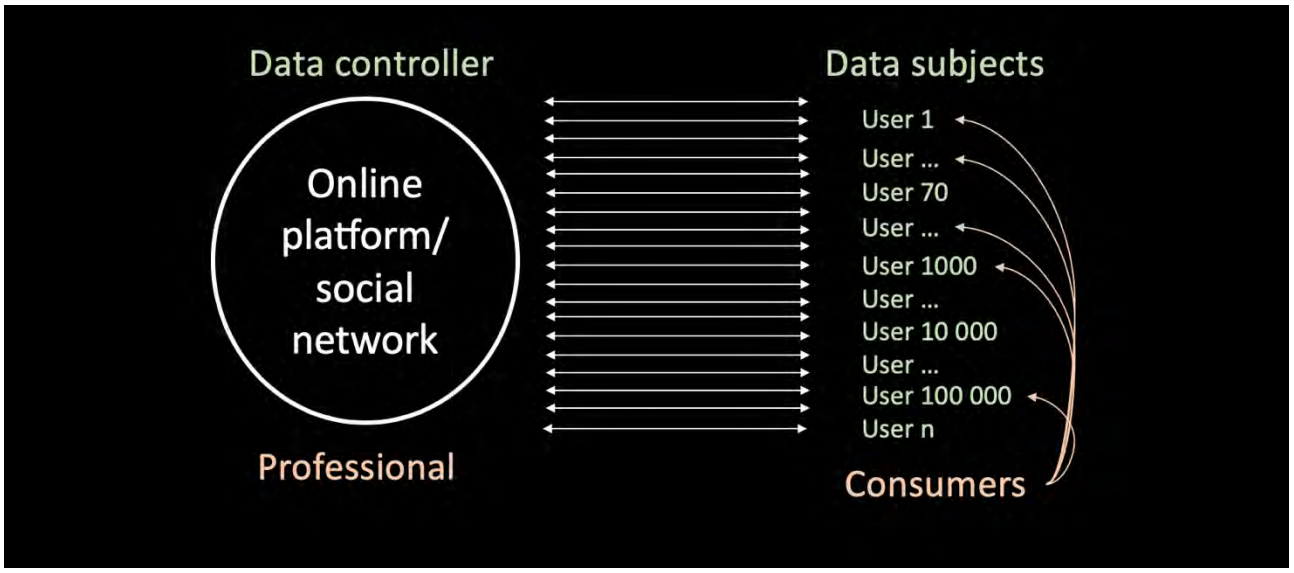


Figure 1. The interplay between the qualification of data subject and consumers in the relationship between natural persons and online platforms.

Main question addressed:

1. In light of the principle of effectiveness and of Article 47 CFREU and Article 8 CFR, can a consumer protection association seek an action in case of violations of data protection law?

1. A) Shall, in light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, the Unfair Commercial Practices Directive (2005/29) be applied in case of a **violation of the duty of information on data processing** provided by Articles 13 and 14 of the General Data Protection Regulation (2016/679)?

In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the Charter of Fundamental Rights, could the Unfair Commercial Practices Directive (2005/29) be **used to**

extensively interpret the duty of information provided in the General Data Protection Regulation (2016/679)?
b) Which authority **is competent**? How should authorities coordinate in light of principles of effectiveness, good administration and duty of cooperation?
2. In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, could the **UCTD** (93/13) (hereinafter UCTD), and the **Consumer Rights Directive** (2011/83) be applied in case of missing or wrongful information to be provided to the data subject?

3. In light of the principle of effectiveness, proportionality, equivalence, dissuasiveness and Article 47 of the CFR, what is the **relationship between the information duties provided in Articles 5 and 6 of the Consumer Rights Directive** (2011/83) and in **Articles 13 and 14 of the GDPR** (2016/679)? Could the information duties provided in the Consumer Rights Directive be interpreted, in certain cases, as covering also the ones of the GDPR? What are the consequences on remedies available under the Consumer Rights Directive?

4. In light of Articles 41 and 47 of the CFR, what is the relationship between the administrative authorities and judicial ones? Is there an impact of the principles of effectiveness, proportionality and dissuasiveness in organising the coordination between data protection authorities ascertaining a data protection violation and judicial authorities in proceedings concerning the ascertainment of a consumer law violation?

5. In light of the principle of effectiveness, dissuasiveness and of Article 47 and Article 8 CFR, could the consumer remedies against a lack of conformity of a digital content/service provided by Directive 2019/770 be used against a violation of data protection law?

9.2. Collective redress in data protection. The (possible) role of consumer protection associations

9.2.1. Collective redress in data protection and its comparison with consumer law

In the field of data protection, the GDPR repealed Directive 95/46/EC (the Data Protection Directive) and introduced a new collective redress mechanism. Article 80 GDPR introduced three new innovations for collective redress in the field of data protection: the data subject has the right to mandate a not-for-profit body (*opt-in*), organisation or association with regard to the protection of their personal data:
- to lodge the complaint on her behalf,
- to exercise on rights on their behalf
- to i) lodge a complaint with a supervisory authority (Article 77 GDPR), ii) an effective judicial remedy against a supervisory authority (Article 78 GDPR) iii) an effective judicial remedy against a controller or processor (Article 79 GDPR).

That not-for-profit body must
- have been properly constituted in accordance with the law of a Member State
- have statutory objectives which are in the public interest,
- be active in the field of the protection of data subjects' rights and freedoms

Furthermore, Article 80 GDPR states that Member States **may** provide that:
- the data subject has the right to mandate a not-for-profit body, organisation or association with the above mentioned characteristics to exercise the right to receive compensation referred to in Article 82 on her behalf (*opt-in*)

- any body, with the above mentioned characteristics independently of a data subject's mandate, has the right to lodge a complaint with the competent supervisory authority in that Member State,(Article 77 GDPR) and to exercise the rights to an effective judicial remedy against a supervisory authority (Article 78 GDPR) and against a controller or processor (Article 79 GDPR) if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing (*opt-out*).
However, the major weakness of this article is that it does not oblige Member States to act for providing an *opt-out* action. Member States are free to choose whether to implement such collective redress mechanisms in their national legislation. The initial Commission proposal included an obligation for Member States to provide for such a mechanism, but the Council amended the text to remove that obligation, despite the fact that the Parliament had approved it. The fact that Member States seem reluctant to implement collective redress mechanisms in general is reflected in their national legislations since, as explained below, only six of them adopted a functioning and efficient collective redress system (Belgium, France, Italy, Portugal, Spain and Sweden).[69]
Data subjects who are also consumers, are already taking advantage of this new possibility at national level. In **France,** consumer group UPF-Que Choisir brought a collective claim on 26 June 2019 before the *Tribunal de grande instance de Paris* (Tribunal of First Instance of Paris) to obtain an injunction against and claim compensation from Google for violation of the GDPR. The association wants to obtain an injunction against Google for stopping the illegal use by its Android system of the users' personal data and for obtaining their express consent before collecting and treating their data. The association claims a compensation of €1000 for any user of Google's Android system and who has a Google account. Consumers who believe their rights have been violated will be able to join the case once the first instance judge has decided on Google's liability.

9.2.2. Question 1: The role of consumer protection associations in ensuring an effective data protection

Relevant CJEU cases:

❖ Judgment of the Court (Second Chamber) of 29 July 2019, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, Case C-40/17 ("**Fashion ID**")

❖ Judgment of the Court (Third Chamber) of 25 January 2018, *Maximilian Schrems v Facebook Ireland Limited*, Case C-498/16 ("**Schrems**")

❖ Judgment of the Court (Third Chamber) of 22 of April 2022 and Opinion of Advocate General delivered on 2 December 2021, *Meta Platform Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, Case C-319/20, ("**Meta Platforms Ireland Ltd**")

In light of the principle of effectiveness and of Article 47 CFREU and Article 8 CFR, can a consumer protection association seek an action in case of violations of data protection law?

The analysis is mainly based on the *Fashion ID* case (C-40/17).

The case

Fashion ID, an online clothing retailer, embedded the 'Like' social plugin from the social network Facebook ('the Facebook "Like" button') on its website. When a visitor consults the website of Fashion ID, that visitor's personal data are transmitted to Facebook Ireland as a result of that website including

[69] BEUC, *Why we need collective redress at EU level: a compelling collection of cases*, October 2019, accessible at: https://www.beuc.eu/publications/beuc-x-2019-062_why_we_need_collective_redress_at_eu_level.pdf.

that button. It seems that that transmission occurs without that visitor being aware of it regardless of whether or not they are a member of the social network Facebook or has clicked on the Facebook 'Like' button.
Verbraucherzentrale NRW, a public-service association tasked with safeguarding the interests of consumers, criticises Fashion ID for transmitting to Facebook Ireland personal data belonging to visitors to its website, first, without their consent and, second, in breach of the duties to inform set out in the provisions relating to the protection of personal data. Verbraucherzentrale NRW brought legal proceedings for an injunction before the Landgericht Düsseldorf (Regional Court, Düsseldorf, Germany) against Fashion ID to force it to stop that practice.
By decision of 9 March 2016, the Landgericht Düsseldorf (Regional Court, Düsseldorf) upheld in part the requests made by Verbraucherzentrale NRW, after having found that it has standing to bring proceedings under Paragraph 8(3)(3) of the UWG.
Fashion ID brought an appeal against that decision before the referring court, the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany). The referring court asked the following question to the CJEU because it had doubts whether Directive 95/46 gave public-service associations the right to bring or defend legal proceedings in order to defend the interests of persons who have suffered harm.

Preliminary questions referred to the Court

(1) Do the rules in Articles 22, 23 and 24 of Directive [95/46] preclude national legislation which, in addition to the powers of intervention conferred on the data-protection authorities and the remedies available to the data subject, grants public-service associations the power to take action against the infringer in the event of an infringement in order to safeguard the interests of consumers?
By its first question the referring court asks, in essence, whether Articles 22 to 24 of Directive 95/46 must be interpreted as precluding national legislation which allows consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the laws protecting personal data.

Reasoning of the Court

As a preliminary point, the Court noted that, under Article 22 of Directive 95/46, Member States are required to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.
Article 28(3) of Directive 95/46 provides that the supervisory authority responsible for monitoring the application of the transposing measures within each Member State has the power to engage in legal proceedings where the national provisions adopted pursuant to that directive have been violated or to bring those violations to the attention of the judicial authorities.
However, no provision of that directive obliges Member States to provide, or expressly empowers them to provide, in their national law that an association can represent a data subject in legal proceedings or commence legal proceedings on its own initiative against the person allegedly responsible for an infringement of the laws protecting personal data.
Nevertheless, nothing in Directive 95/46 precludes national legislation allowing consumer-protection associations to bring or defend legal proceedings against the person allegedly responsible for such an infringement.
The Court then recalled that Member States are required, when transposing a directive, to ensure that it is fully effective in accordance with the objective which it seeks to attain, but they retain a broad discretion as to the choice of ways and means of ensuring that it is implemented. In this regard, one of the underlying objectives of Directive 95/46 is to ensure 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 fact that a Member State provides in its national legislation that it is possible for a consumer protection association to commence legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data in no way undermines the objectives of that protection and, in fact, contributes to the realisation of those objectives.
Since Directive 95/46 lays down rules that are relatively general and have a degree of flexibility, Member States have a margin of discretion in implementing that directive. Although Article 22 of that directive requires Member States to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the personal data processing in question, that directive does not, however, contain any provisions specifically governing the conditions under which that remedy may be exercised. In addition, Article 24 of the directive provides that Member States are to adopt 'suitable measures' to ensure the full implementation of its provisions, without defining such measures.
The Court then explained that a provision making it possible for a consumer protection association to commence legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data may constitute a suitable measure, within the meaning of that provision, that contributes to the realisation of the objectives of that directive.
Finally, the fact that Regulation 2016/679 (the GDPR), which repealed and replaced Directive 95/46 and has been applicable since 25 May 2018, in Article 80(2) thereof, expressly authorises Member States to allow consumer-protection associations to bring or defend legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data does not mean that Member States could not grant them that right under Directive 95/46, but confirms, rather, that the interpretation of that directive in the present judgment reflects the will of the EU legislature.

Conclusion of the Court

Articles 22 to 24 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 must be interpreted as not precluding national legislation which allows consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the protection of personal data.

Impact on the follow-up case

The referring court (*Oberlandesgericht Düsseldorf*) still has to deliver its decision.

Elements of judicial dialogue

The ***Schrems II*** **case** (C-498/16) is also relevant to answer the question of whether a consumer protection association can seek an action in case of violations of data protection law.
In that case, the plaintiff (Mr Schrems) had founded an association which sought to uphold the fundamental right to data protection. Firstly, the qualification of the applicant as a consumer should be considered: in the *Schrems* case (C-498/16) the referring court asked the question whether, in order to apply Regulation No 44/2001, the activities of publishing books, lecturing, operating websites, fundraising and being assigned the claims of numerous consumers for the purpose of their enforcement do not entail the loss of a private Facebook account user's status as a 'consumer'. The CJEU, recalling its previous case law, stated that the concept of consumer is distinct from the knowledge and information that the person concerned actually possesses. Therefore, neither the expertise which that person may acquire in the field covered by those services nor his assurances given for the purposes of representing the rights and interests of the users of those services can deprive him of the status of a 'consumer' with regard to the application of Regulation No 44/2001.

However, the applicant brought the action against Facebook on the basis of his own rights and similar rights of seven other contractual partners of the defendant, who are also consumers in Austria, Germany and India. Austrian law indeed allows that one applicant brings different claims against the same defendant and that these claims be heard jointly in the same proceedings. The plaintiff claimed that the defendant had committed numerous infringements of data protection provisions. After his actions were dismissed by the lower courts, Mr Schrems brought an appeal before the *Oberster Gerichtshof* (Supreme Court, Austria), which referred a question to the CJEU.

In its question, the referring court asked, in essence, whether Article 16(1) of Regulation No 44/2001 (related to jurisdiction over consumer contracts) must be interpreted as meaning that it does not apply to the proceedings brought by a consumer for the purpose of asserting, in the courts of the place where he is domiciled, not only his own claims, but also claims assigned by other consumers domiciled in the same Member State, in other Member States or in non-member countries. In other words, as AG Bobek puts it in his opinion of the case, can Article 16(1) of Regulation No 44/2001 establish an additional special jurisdiction in the domicile of the assignee, thus effectively opening up the possibility of collecting consumer claims from around the world?

The Court did not depart from its settled case law and held that the assignment of claims cannot, in itself, have an impact on the determination of the court having jurisdiction. It follows that the jurisdiction of courts other than those expressly referred to by Regulation No 44/2001 cannot be established through the concentration of several claims in the person of a single applicant.[70]

By holding that the special rules of jurisdiction over consumer contracts do not allow consumers to seek redress jointly for their own claims and for claims assigned to them by consumers domiciled in the same Member State, in other Member States or in non-member countries, the Court interpreted Article 16(1) of Regulation 44/2001 strictly. Although the claim in these proceedings related to violations of data protection laws, the Court's conclusion applies to any claims related to consumer contracts.

While the Court in *Schrems* denied collective redress through the assignment of rights by consumers, it held in *Fashion ID* that Member States could allow consumer protection associations to seek redress for violation of data protection laws. Consequently, if Austria had allowed such claims by consumer protection associations and if Mr Schrems had filed suit with his association, it is likely that he would have had standing to bring those third-party claims as well. In any event, it is worth noting that the Court does not generally exclude the possibility of collective redress for violations of data protection provisions. However, the issue in *Schrems* was rather specific, as it concerned the assignment of rights by consumers to a single plaintiff (a possibility under Austrian law). Therefore, the Court did not hold that consumers victims of violations of data protection law cannot obtain collective redress, but rather that multiple plaintiffs cannot circumvent the European rules on international jurisdiction by concentrating their claims in the person of a single applicant.

Meanwhile, the GDPR entered into force and now provides in its Article 80 that data subjects have the right to mandate a not-for-profit body, organisation or association to lodge complaints and to exercise the right to receive compensation, where provided for by Member State law (see below). As explained below, the major drawback of Article 80 is that Member States are free to implement it or not, which leaves consumer protection associations upholding the fundamental right to data protection with unharmonised collective redress mechanisms in the EU.

Moreover, with regard to the application of Article 80 GDPR for protecting (also) economic interests, the case **C-319/20, *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen***

[70] On 28 February 2018, the Austrian Supreme Court upheld the Higher Regional Court's decision dismissing the appeal. Given the CJEU's preliminary ruling, the Austrian Supreme Court explained that the plaintiff could only rely on his personal claim and not on the other claims assigned to him. The Austrian Court did not depart from the CJEU's ruling and dealt with the issue rapidly.

und Verbraucherverbände is of particular interest. In this preliminary reference, the German Federal Court of Justice asked to the CJEU as to whether the rules in Chapter VIII of the GDPR, in particular in its Article 80 concerning collective redress, and Article 84 concerning sanctions preclude national rules which — alongside the powers of intervention of the supervisory authorities responsible for monitoring and enforcing the Regulation and the options for legal redress for data subjects — empower, on the one hand, competitors and, on the other, associations, entities and chambers entitled under national law, to bring proceedings for breaches of Regulation (EU) 2016/679, independently of the infringement of specific rights of individual data subjects and without being mandated to do so by a data subject, against the infringer before the civil courts on the basis of the prohibition of unfair commercial practices or breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions. In its **opinion** delivered **on 3 December 2021, the Advocate General**, relying, *inter alia,* on the principle of dissuasiveness (§65) affirmed that Article 80(2) GDPR must be interpreted as meaning that it does not preclude national legislation which allows consumer protection associations to bring legal proceedings against the person alleged to be responsible for the infringements of the protection of personal data, on the basis of the prohibition of unfair commercial practices, the infringement of a law relating to consumer protection or the prohibition of the use of invalid general terms and conditions, provided that the objective of the representative action in question is to ensure observance of the rights which the persons affected by the contested processing derive directly from that regulation.

The **CJEU, in its decision of 22 of April 2022**, stated that Article 80(2 GDPRP does not preclude national legislation which allows a consumer protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects, against the person allegedly responsible for an infringement of the laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions, where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that regulation.

Impact on national case law in Member States other than the one of the court referring the preliminary question to the CJEU

France

The decision of the Paris First Degree Court, of 9 April 2019 No 14/07298 is of particular interest. In that case, the association UNION FÉDÉRALE DES CONSOMMATEURS – QUE CHOISIR (hereinafter UFC – QUE CHOISIR) has brought an action before the Paris First Degree Court against Facebook for the purpose of establishing the unfair or unlawful nature of clauses in the platform's "General Terms and Conditions of Use" in the 2013, 2015 and 2016 versions, to have them deleted or deemed to be unwritten and to repair the damage caused to the collective interest of consumers. UFC QUE CHOISIR has requested that all the contractual conditions proposed by Facebook be declared abusive and illegal on its internal website with regard to the Consumer Code in particular Articles L 111-1, L. 211-1 and L. 212-1. The applicant argued that Facebook terms of use were not accessible, clear and understandable and did not comply with the provisions of the Law No. 78-17 of 6 January 1978 on information technology, data files and civil liberties.

In line with previous decisions (TGI Paris, 7 August 2018, No. 14/07300, UFC Que Choisir v. Twitter ; TGI Paris, 12 February 2019, No. 14/07224, UFC Que Choisir v. Google) and the recommendation on social networking contracts of the Commission on Unfair Terms, the qualification of a consumer contract was retained even though Facebook noted that social network access was free. Thus, the contract concluded between the company Facebook and the member of its social network is a consumer contract, subject to all the provisions of consumer law, subject only that the member does not use the network for professional purposes (CJEU 25 January 2018, C-498/16, Schrems). The Court applied consumer law

(see par. XX of this Chapter and condemned Facebook to pay 30 000 euros to the association UFC-QUE CHOISIR in compensation for the moral prejudice caused to the collective interest of consumers. (for further information on that case, see the FRiCoRe database at this link).

9.2.3. The role of consumer associations in the field of data protection in light of new Directive EU, 2020/1828, on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, adopted on 25 November 2020

In the field of data protection, as explained above, Article 80 of the GDPR notably allows non-profit organisations to bring actions on behalf of data subjects whenever Member States provide for this possibility. However, as a study requested by the European Parliament's Committee on Legal Affairs duly noted, the article's "wording is rather unclear and by including a reference to national law, the EU legislator made it clear it was not ready to recognise a European collective action mechanism yet".[71]
Against this backdrop, on 11 April 2018, the European Commission published a legislative proposal for the adoption of a new directive on representative actions for the protection of the collective interests of consumers.[72] The new directive EU 2020/1828, on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC was adopted on 25 November 2020.
With regard to the role of consumer protection associations in the field of data protection, Article 2 of the directive states that:
"This Directive applies to representative actions brought against infringements by traders of the provisions of Union law referred to in Annex I, including such provisions as transposed into national law, that harm or may harm the collective interests of consumers".
Regulation UE 2016/679 and Directive 2002/58 are included in Annex I.
According to its recital 14, the directive should cover infringements of the provisions of EU law referred to in Annex I *to the extent that those provisions protect the interests of consumers*, regardless of whether those consumers are referred to as consumers, travellers, users, customers, retail investors, retail clients, **data subjects** or something else. **However, this Directive should only protect the interests of natural persons who have been harmed or may be harmed by those infringements if those persons are consumers under this Directive. Infringements that harm natural persons qualifying as traders under this Directive should not be covered by it** (see also recital 16).
Furthermore, according to Recital 15 the directive should be without prejudice to the legal acts listed in Annex I and therefore it should not change or extend the definitions laid down in those legal acts or replace any enforcement mechanism that those legal acts might contain. In addition, recital 15 of the directive expressly provides that *the enforcement mechanisms provided for in or based on Regulation (EU) 2016/679 (…) could, where applicable, still be used for the protection of the collective interests of consumers.*
The directive at certain extent encourages the role of consumer protection associations in data protection cases. The coordination between collective redress in consumer and data protection cases will be an important issue for Member States in the implementation of the new directive, also in light of Article 47, Article 8 CFREU and of the principle of effectiveness.

---

[71] Study requested by the JURI committee of the European Parliament, *Collective redress in the Member States of the European Union*, October 2018, p. 44, accessible at: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/608829/IPOL_STU(2018)608829_EN.pdf.
[72] Proposal for a Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, COM/2018/0184 final - 2018/089 (COD). The Commission proposal was published on 11 April 2018.

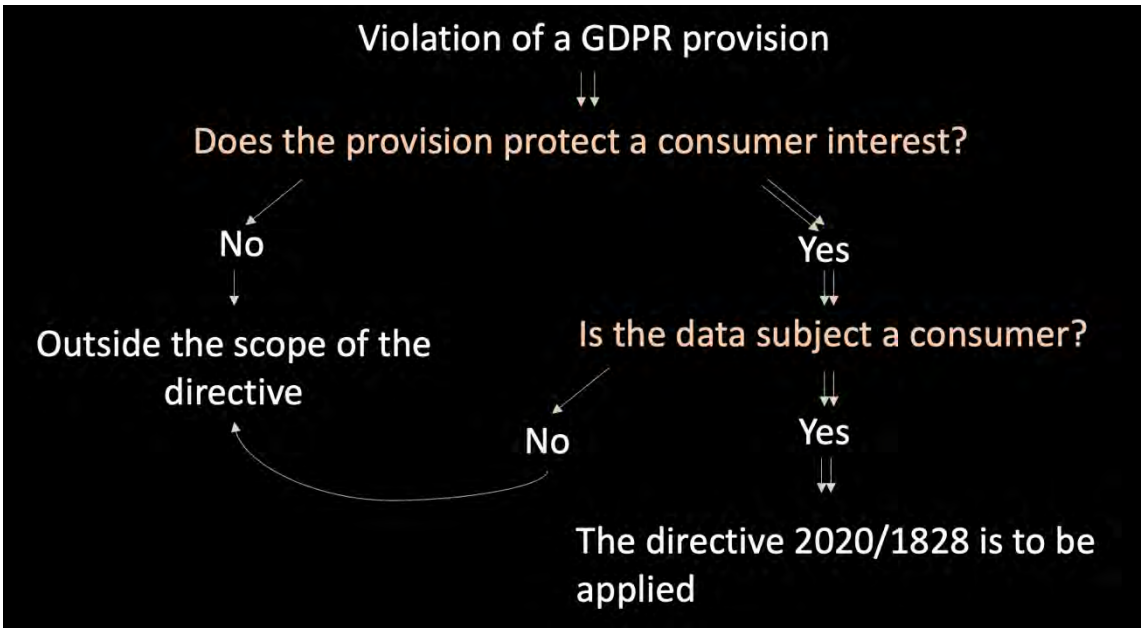


Fig. 2 The application of the directive in case of violations of data protection law

The directive creates a different protection against violations of data protection law if the infringed provisions are protecting also the interests of consumers, and the victims can be qualified as consumers. In this respect, the following question arises:

If the data subject is also a consumer, can Article 47 CFREU lead to a concurrence of remedies that combines data protection and consumer law remedies?

Furthermore, the comparison between the legislation on collective actions in consumer law and in data protection law shows that within the latter the collective redress system is less developed. In this respect, it should be noted that both the relationships between, on the one hand, the data subject and the data controller and on the other hand, the consumer and the professional, are characterized by an imbalance of power, although — at least partially — different in nature. The weaker position of the consumer *vis-à-vis* the seller or supplier, concerns the consumer's level of knowledge and her bargaining power (e.g., *Costea,* 3 September 2015, C-110/14; *Siba,* C-537/13, 15 January 2015; *Pouvin*, C-590/17, 21 March 2019; *Vapenik,* C-508/12, 5 December 2013). The data subject's weaker position is due at least to the knowledge concerning the data subject that the data controller acquires in processing data, and to the fact that the ways and timing of processing are put in place by the controller, with the consequence of an information asymmetry concerning the operations of processing.

9.3. Unfair commercial practices and information provided to the data subject

a. Shall, in light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, the Unfair Commercial Practices Directive (2005/29) be applied in case of a **violation of the duty of information on data processing** provided by Articles 13 and 14 of the General Data Protection Regulation (2016/679)? In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, could the Unfair Commercial Practices Directive (2005/29) be **used to interpret extensively the duty of information provided in the General Data Protection Regulation** (2016/679)?

b. Which authority **is competent**? How should authorities coordinate in light of principles of effectiveness, good administration and duty of cooperation?

Relevant national cases in cluster:

➢ Italian consumer protection Authority (Autorità Garante per la Concorrenza e il Mercato – AGCM), decision n° 26597, 11 May 2017, *Whatsapp-Trasferimento dati a Facebook*

➢ Italian consumer protection Authority (Autorità Garante per la Concorrenza e il Mercato – AGCM), decision n° 27432, 29 November 2018, *Facebook- condivisione dati con terzi*

➢ Administrative court (T.A.R.) of Rome, 10 January 2020, n. 260 (judicial review of Italian consumer protection Authority, decision n° 27432, 29 November 2018)

➢ Administrative court (T.A.R.) of Rome, 10 January 2020, n. 261 (judicial review of Italian consumer protection Authority, decision n° 27432, 29 November 2018)

➢ Council of State, decisions No. 2631 and 2630, 29 March 2021

Introduction: coordination and existence of parallel systems and authorities regulating the digital economy

Although unfair commercial practices linked to infringements of data protection laws are not limited to the digital economy, such practices frequently occur online. The most relevant cases do involve online platforms, online traders and connected objects. Digital markets are characterized by a lack of informed consent by data subjects, leading to a lack of transparency in the way their data are collected and processed. These characteristics lead to situations where a single conduct can potentially constitute infringements of data protection, consumer and/or competition law.

Another issue is to determine which regulator is competent to investigate and sanction infringements of data protection law that also constitute infringements of consumer law and potentially restrict competition on the market. In February 2019, the German Competition Authority (*Bundeskartellamt*) issued a decision against Facebook for abusing its dominant position on the German market for social networks, based on the extent of collecting, using and merging data in user accounts. Similarly, the Italian Competition Authority (*Autorità Garante della Concorrenza e del Mercato*), also in charge of consumer protection, fined WhatsApp in May 2017 for violating consumer law because it shared its users' personal data with Facebook and forced its users in accepting its new terms and conditions.

Both cases are discussed below as they involve conducts prohibited under a mix of consumer, data protection and/or competition law. These cases illustrate the existence of parallel systems and authorities regulating the digital economy. Each system has its own legal bases, goals, procedures and remedies. But can those systems overlap, and to what extent? This section will focus on the interplay between the General Data Protection Regulation (the ***GDPR***) and Directive 2005/49 (the ***Unfair Commercial Practices Directive***). In particular, it aims to answer the question whether violations of information duties provided by the GDPR can also constitute unfair commercial practices under the Unfair Commercial Practices Directive, and whether this directive could be used to interpret extensively the duty of information provided in the GDPR. This section also tries to determine which authority is competent, and how they should coordinate.

9.3.1. Question 2a: Unfair commercial practices and information provided to the data subject

In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, shall the Unfair Commercial Practices Directive (2005/29) be applied in case of a **violation of the duty of information on data processing** provided by Articles 13 and 14 of the General Data Protection Regulation (2016/679)?

In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, could the Unfair Commercial Practices Directive (2005/29) be **used to interpret extensively the duty of information provided in the General Data Protection Regulation** (2016/679)?

With regard to the question, there are no CJEU judgements. This sub-section will thus focus on EU legal instruments and on national cases in Italy and Germany.

EU law perspective

The European Commission **Guidance on the implementation/application of the Unfair Commercial Practices Directive**[73] provides that:

- A trader's violation of Data Protection rules will not, in itself, always mean that the practice is also in breach of Directive 2005/29, but such **data protection violations should be considered when assessing the overall unfairness of commercial practices**, particularly in the situation where the trader processes consumer data in violation of data protection requirements, (*i.e.,* for direct marketing purposes or any other commercial purposes like profiling, personal pricing or big data applications).
- Personal data, consumer preferences and other user generated content, have a "de facto" economic value. Depending on the circumstances, this could also be considered a violation of the EU data protection requirements to provide the required information to the individual concerned as to the purposes of the processing of the personal data.

Furthermore, the European Commission in the Guidance affirmed that:

"According to its Article 51(1), the EU Charter of fundamental rights applies to the Member States when they implement Union law, thus also when they implement the provisions of the UCPD. The Charter contains provisions, among others, on the **protection of personal data (Article 8)**, the rights of the child (Article 24), consumer protection (Article 38) and the **right to an effective remedy and a fair trial (Article 47)**. The Court has stressed the significance of Article 47 of the Charter on access to justice in relation to remedies available to consumers in connection with consumer rights granted under EU directives. **The principle of effectiveness**, as referred to by the Court, means that national rules of procedure may not make it excessively difficult or impossible in practice for consumers to exercise rights conferred by EU law."

The statement on the economic value of certain uses of personal data, such as the ones for commercial purposes should be coordinated with the impossibility of their qualification as "mere commodities". In this respect, **recital (24) of Directive 2019/770** states:

"Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. (…) While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies".

According to the **EDPB' s Opinion 4/2017 on the Proposal for a Directive** on certain aspects concerning contracts for the supply of digital content, personal data cannot be regarded as a commodity. In this Opinion, the EDPB states:

"The EDPS warns against any new provision introducing the idea that people can pay with their data the same way as they do with money. Fundamental rights such as the right to the protection of personal data cannot be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity".

[73] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016SC0163&from=IT

National case law

Italy

In two decisions the Italian consumer protection Authority (*Autorità Garante per la Concorrenza ed il Mercato,* hereinafter: ***AGCM***) has considered the conduct of professionals concerning the information of the data subject in light of Directive 2005/29 on unfair commercial practices.

In both **decisions** (dec. n° 27432, 29 November 2018 and n° 26597, 11 May 2017), the AGCM affirmed that **the unfair commercial practices discipline is to be applied** where **personal data** concerning Facebook's users acquire economic value because are **used for commercial purposes**, also in absence of a price payed for the commercial use of these data.

Furthermore, in the decision n° 27432, 29 November 2018 the AGCM considered:

a) as **a misleading commercial practice,** the professional's conduct consisting in not providing a clear, complete and immediate **information concerning his activity of collecting and using, for commercial purposes, the data of its users** during the first registration phase of the user on Facebook Platform. The AGCM considered that the information provided by Facebook is generic and incomplete and that it does not adequately distinguish between, on the one hand, the use of data for the customisation of the service with the aim of facilitating socialisation with other users ("consumers"), and on the other hand, the use of data to carry out targeted advertising campaigns. **The misleading character of the practice is aggravated by the circumstance that, in the use of Facebook, the commercial purposes are mixed and presented as confused with the social and cultural purposes typical of the social network.**

b) as an **aggressive commercial practice** the professional's conduct according to which the professional applies, in relation to its registered users, a mechanism that, through various steps, involves the **transmission of user data from the platform of the social network to third party websites/apps and *vice versa*,** without the prior express consent of the person concerned, for the use of the same for profiling and commercial purposes. In the case, the option available to the user to authorise or not this method is pre-set on the consent to the technical integration between Facebook and third party websites/apps (so-called "Platform activation"), which implies, by default, a generic predisposition to the reciprocal transmission (Facebook/third parties) of Facebook users' data, and users' right to opt-out. Moreover, Facebook affirms that the deactivation of the above mentioned integration produces for the users penalising consequences, both in the use of Facebook, and in the accessibility and use of third-party websites and apps**. <u>The AGCM considered that this practice, by means of undue influence, is to be considered suitable to considerably restrict the freedom of choice or conduct of the average consumer, thus inducing them to take a decision of a commercial nature that they would not otherwise have taken, in particular, the decision to integrate the functionalities of Facebook with those of third party websites/apps, including games, and to transfer, consequently, his data from Facebook to third parties and vice versa</u>**. According to the AGCM decision, the professional exercises undue influence over registered consumers, who, without express and prior consent, therefore unconsciously and automatically, suffer the transmission and use by Facebook/third parties, for commercial purposes, of the data concerning them (information deriving from the use of Facebook and from their own experience on third party websites and apps). Undue conditioning derives from the application of the pre-selection system of the widest consent to the transmission of one's own data from/to third parties, described above, together with the description of significant limitations in the usability of the social network and of the websites/apps of third parties due to the deselection of the transmission option.

With regard to **decision n° 26597, 11 May 2017**, the proceeding concerns WhatsApp's conduct towards its customers (consumer users), which has led users to accept in full the changes made to the Terms of Use of the WhatsApp Messenger application, which provided the option, pre-selected, of sharing certain personal data from their WhatsApp with Facebook for the company's use of such data for commercial

profiling and advertising purposes. In the event of non-acceptance of that changes, the information provided to the user/consumer suggested that the service would be discontinued. It should be noted also that for those who were already users of the application at the time of the update, WhatsApp allowed them to accept its contents even "partially". The existence of such an option was not represented in the main screen dedicated to the acceptance of the new Terms of Use. Only on the next screen, which was accessed by clicking on the link that referred to the reading of the Terms and Privacy Policy, the user would have realised that he had an alternative choice that was, however, pre-set, by checking in the box provided, to consent to the sharing of data. If the user had wanted to continue to use the application, without sharing their data with Facebook, he would have to uncheck the checkbox.

The commercial practice is qualified by the AGCM **as aggressive in that, through undue influence, it is likely to significantly restrict the average consumer's freedom of choice or conduct, thereby causing him to take a transactional decision that he would not have taken otherwise**. This undue influence stems from the fact that WhatsApp Messenger users were in fact forced to accept the new contractual terms in full, in particular with regard to the sharing of data with Facebook, making them believe that it would otherwise have been impossible to continue using the application where those who were already users at the date of the amendment of the Terms, instead, had the opportunity to "partially" accept its contents.

In July 2019 the **Italian consumer protection Authority (AGCM), the Italian Data protection Authority (GPDP) and the Media Authority (AGCOM) issued a joint statement "Big Data. Joint Investigation, Guidelines and Policy Recommendations"**, in which they elaborated some shared guidelines and policies, which states that it is necessary (point n. 10):

"To strengthen the powers of AGCM and AGCom to acquire information outside the investigation procedures and to increase the maximum level of sanctions in order to ensure an effective deterrent effect of the consumer protection rules".

In this respect the Authorities affirm that **consumer protection** can affect a variety of profiles related to the relationship between operators and users in the acquisition, processing and processing of data. According to that statement, the fact that the **legislation on the protection of personal data** is applicable to the conduct of companies does not exempt them from complying with the rules **on unfair commercial practices**; **the two disciplines are seen as complementary and not alternative**. The authorities considered that consumer protection and privacy protection are undoubtedly important components of a fair competition.

The **Italian administrative court of Rome in the judgement n. 260, 10 January 2020**, which constitute the judicial review of the AGCM decision n° 27432/2018, stated that the economic value of person data of the users requires the professional to inform the consumer that the information obtained from such data will be used for commercial purposes that go beyond its use in the "social network". The practice may be qualified as misleading in case of lack of adequate information, or in the case of misleading statements. In the present case, the court confirmed the AGCM's decision, stating that the claim used by Facebook in the registration page in order to encourage users to subscribe ("Subscribe. It's free and it will be forever") suggested the absence of a counter-performance required from the consumer in exchange for the use of the service. Therefore, according to the court's judgement, the practice is to be sanctioned because of the incompleteness of the information provided, where the claim of gratuitousness of the service did not allow the consumer to understand that the professional would use the users data for remunerative and commercial purposes.

The Council of State, in its decisions no. 2631 and 2630 of 29 March 2021 confirmed the decision of the Tribunal. In its reasoning, the Council of State considered that the special EU discipline of personal data protection has a very broad scope also due to the broad concept of "processing" (Article 4 GDPR), but that the application of data protection rules does not exclude the application of other disciplines, such as consumer law. Therefore, according to the Council of State, there is not a principle of the

speciality of data protection law that excludes the application of other provisions. In this vein, the Council of State considered that when the processing involves behaviours and situations regulated by other legal sources for the protection of other values and interests, the legal system — first at EU level and then at a national level — cannot exclude the application of other sectoral disciplines, such as that of consumer protection, to reduce the protection guaranteed to natural persons. Accordingly, the Council of State affirmed the need to ensure "multi-level protections" that can enhance the protection of individuals' rights. As to the merit of the case, the Council of State affirmed that in the present case is not at stake the commercialisation of personal data by the data subject, but the exploitation of personal data made available by the data subject in favor of a third party who will use it for commercial purposes, without the data subject is fully aware of the data uses.
Considering the above mentioned litigation, in light of the principle of effectiveness and dissuasiveness, the following questions can be raised:

In light of Article 47 of the CFR, when there is a violation of data protection law and the conduct is qualified also as a commercial practice, taking into account Article 8 of the CFR, what are the cases in which the practice is not to be considered unfair? Could a decision of the Data Protection Authority declaring a violation of data protection rules be relevant in the Consumer Authority's assessment concerning the existence of an unfair practice? If so, is it decisive in that assessment?

The application of unfair commercial practices directive could lead to focus on the importance of the information related to the use of personal data for profit also in the interpretation of the information duties of the data controller (Article 13 GDPR). In this respect,

In light of Article 8 and 47 CFR, could an extensive interpretation of Article 13 GDPR, including the duty to inform about the commercial and remunerative use of personal data be applied where the data subject is not a consumer?

9.3.2. Question 2b: Competent administrative authorities and their coordination

National cases

Italy
The consumer protection authority examined the question of its **competence** in the decisions 27432, 29 November 2018 n° 26597, 11 May 2017. The AGCM affirmed that the data protection and the commercial practices disciplines have different material scopes and pursue different interests. As a result, the Authority affirmed that there is no conflict between the two disciplines, but rather they are complementary. On this ground the authority stated that the conducts analysed in the proceeding are considered in light of the unfair commercial practices' rules. Therefore, the Italian consumer protection Authority affirmed its competence.
It should be noted that in both proceedings (related to decisions 27432, 29 November 2018 and decision n° 26597, 11 May 2017) the Italian consumer protection Authority required an **opinion to the Italian media Agency** (*Autorità per le Garanzie nelle Comunicazioni*, AGCOM), in accordance with **Article 27(6) consumer code**, which states that when a commercial practice has been or is intended to be disseminated in the periodical or daily press, or by radio or television or any other telecommunications medium, before issuing a decision, the consumer protection Authority shall request the opinion of the Communications Regulatory Authority.
In July 2019 the **Italian consumer protection Authority (AGCM), the Italian Data protection Authority (GPDP) and the Media Authority (AGCOM) issued a joint statement titled "Big Data. Joint Investigation, Guidelines and Policy Recommendations"**, in which they elaborated some

shared guidelines and policies, and according to which (point n° 11) **it is necessary to create a permanent coordination between the three authorities.** In particular, the authorities considered that:
"The challenges posed by the development of the digital economy and Big Data require full use to be made of the synergies between ex ante and ex post instruments for protecting privacy, competition, consumers and pluralism.
AGCM, AGCom and the GPDP, each within their own sphere of competence, can best guarantee their own institutional objectives, insofar as they will be able to take full advantage of the opportunities offered by fruitful cooperation.
To this end, the three Authorities, in the exercise of the complementary competences assigned to them and which contribute to tackling the critical issues of the digital economy, are committed to close forms of collaboration in interventions that affect the digital markets, including through the signing of a memorandum of understanding."

The Authorities considered also that in order to allow a full understanding of the new phenomena in the digital economy, it seems appropriate to strengthen the powers of acquisition of information by AGCM and AGCOM outside the investigative procedures (investigations, pre-instructive activities), including the possibility to impose administrative sanctions in case of refusal or delay in providing the information.
In the judgment of the **Italian administrative court of Rome n. 260, 10 January 2020**, which constitutes the judicial review of the AGCM decision 27432/2018, the court addressed the question of the consumer protection authority's competence, which was denied by the claimant. In this respect, the court stated that the plaintiff's arguments presuppose that the protection of personal data only concerns fundamental rights. The national court considered that this approach does not take into account the economic value of personal data. The court stated that personal data are to be protected as an expression of an individual's right to privacy, and as such subject to specific and not renounceable forms of protection, such as the right to revoke consent, access, rectification, erasure.
In the court's view, a different kind of protection of personal data is to be developed, because of the economic value of personal data. The court affirmed that the existence of an economic value of the personal data, typical of the new economies of the digital markets, requires the operators to respect, in the relative commercial transactions, those obligations of clarity, completeness and not deceptiveness of the information provided for by the legislation for the protection of the consumer, which must be made aware of the exchange which is related to the adhesion to a contract for the fruition of a service, such as the use of a "social network". The court recalled the *Guidance on the implementation/application of directive 2005/29/ec on unfair commercial practices* released by the EU Commission on 25 Mary 2016, where the economic value of personal data and the possible relevance of Directive 2005/29 is affirmed.
Moreover, the Italian administrative court stated that the omission of information about the exploitation for commercial purposes of user data is not a matter entirely regulated and sanctioned within data protection law. The court recalled also *Wind Tre* (C-54 and C-55/17), concerning the coordination among multiple administrative bodies competent in relation to the same conduct.
Then, according to the court, in the present case there is no incompatibility or antinomy between the provisions of data protection and consumer law, since they are complementary, imposing, in relation to the respective purposes of protection, specific information obligations, in one case functional to the protection of personal data, understood as a fundamental right, and in the other to the correct information to be provided to the consumer in order to allow her to make an informed economic choice.
Furthermore, the court highlights that there is no risk of over-deterrence consisting in a double sanction for the same conduct, considering that the object of investigation by the competent authorities concerns different conduct of the operator, the correct processing of personal data and the clarity and completeness of the information about the exploitation of the data for commercial purposes

Similar arguments and the same conclusion were adopted by the **administrative court of Rome in the judgment 10 January 2020, n. 261**.

Germany

On 6 February 2019, the German Competition Authority (*Bundeskartellamt*), which was also granted competences in the area of consumer protection, issued a decision against Facebook for abusing its dominant position on the German market for social networks, based on violations of data protection law. In its summary of the decision,[74] the Authority explains that the GDPR does not rule out the possibility for authorities other than the national data protection authorities (including competition and/or consumer protection authorities) to apply substantive data protection law.

The Authority also explains that the GDPR explicitly states that data protection law can also be enforced under civil law, i.e., that full consistency is not aspired to. More importantly, the Authority explains that:

"This applies in particular to consumer protection organisations and competitors and their associations. These entities can enforce data protection based on stipulations of the Act Against Unfair Competition (UWG) or regulations on business terms linked to data protection and also based on Section 19 GWB. A large part of the ECJ's case law which data protection authorities and the data protection board have to consider has been obtained from civil law proceedings. Civil law proceedings promote rather than threaten the consistent implementation of data protection law, especially as the ECJ can be involved at an early stage as part of the preliminary ruling procedure".

The *Bundeskartellamt* explained that, in the course of its proceedings against Facebook, it maintained regular contact with data protection authorities, none of which considered they had exclusive competence. This is consistent with the approach taken by the Italian competition, data protection and telecom authorities in their joint statement.

EU law perspective

The AGCM decision fining WhatsApp for data transfer to Facebook of May 2017 came three years after the European Commission approved the merger between the two companies.[75] In its merger decision, the Commission had concluded that the merged entity would be unable to establish reliable automated matching between Facebook users' accounts and WhatsApp users' accounts. However, in August 2016, WhatsApp announced updates to its terms of service and privacy policy, including the possibility of linking WhatsApp users' phone numbers with Facebook users' identities. This led the Commission to fine Facebook €110 million for providing misleading information during the merger process.[76]

Therefore, the Italian authority issued a decision against WhatsApp based on consumer law, but the problem originates in the Commission's decision not to oppose to the merger. The Commission has been criticised for not taking enough into account data protection concerns in its review of the merger. In its decision, the Commission indeed stated that:

"For the purposes of this decision, the Commission has analysed potential data concentration only to the extent that it is likely to strengthen Facebook's position in the online advertising market or in any sub-segments thereof. Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules".

---

[74] https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3

[75] European Commission, Case COMP/M.7217 Facebook/Whatsapp 3 October 2014.

[76] https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369

The Commission's decision suggests that it has not coordinated its investigation with national data or consumer protection authorities. This suggests that there is the need of more coordination between the different national and European authorities in the field of consumer, data protection and competition enforcement. In this respect, the following question arises:

In light of the principles of effectiveness and good administration, is it necessary to provide a system of coordination between data protection and consumer authorities at national and European level? Could the documents and the investigations made by an authority be used in proceedings of another authority?

9.4. Information to be provided to the data subject, consumer rights directive, and unfair terms directive

Main questions addressed

3. In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, could the **UCTD** (93/13) and the **Consumer Rights Directive** (2011/83) be applied in case of missing or wrongful information to be provided to the data subject? 4. In light of the principle of effectiveness, proportionality, equivalence, dissuasiveness and Article 47 of the CFR, what is the **relationship between the information duties provided in Articles 5 and 6 of the Consumer Rights Directive** (2011/83) and in **Articles 13 and 14 of the General Data Protection Regulation** (2016/679)? Could the information duties provided in the Consumer Rights Directive be interpreted, in certain cases, as covering also the ones of the GDPR? What are the consequences on remedies available under the Consumer Rights Directive? 5. In light of Articles 41 and 47 of the CFR, what is the relationship between the administrative authorities and judicial ones?

Relevant national cases in cluster:

- LG Berlin, 30/04/2013, (2013) Neue Juristische Wochenschrift 2605, 2606 – Apple
- LG Berlin, 19/11/2013, (2014) MultiMedia und Recht 563, 565 – Google
- LG Frankfurt a.M., 10/06/2016, (2016) Beck Rechtsprechung (BeckRS) 10907 – Samsung

9.4.1. Question 3: Unfair contractual terms and information provided to the data subject

In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, could the **UCTD** (93/13) and the **Consumer Rights Directive** (2011/83) be applied in case of missing or wrongful information to be provided to the data subject?

With regards to this question, there are no European cases. This sub-section with thus focus on German cases.

National case law

Germany

On **30 April 2013**, the **Landgericht Berlin** (District Court of Berlin) issued a decision against **Apple**.[77] The plaintiff is a consumer protection association and requests an injunction against non-transparent clauses of the defendant's terms and conditions. The defendant sells computer hardware and communication devices. They also operate a telemedia service which is available in German at 'www.apple.com/de'. On this website, the defendant publishes their terms and conditions as well as their 'Apple privacy policy'. The plaintiff regards clauses of the privacy policy and the terms and conditions as problematic under §307 BGB and requests an injunction against their use.

[77] Registration No. 15 O 92/12.

The district court held that the clauses of a privacy policy also constitute terms and conditions. Under §305 German Civil Code, terms and conditions are pre-formulated conditions for numerous contracts which one party stipulates to the other. On the basis of the presentation of the privacy policy as part of the order process (as one click-wrapping option with the terms and conditions), the court adopted the least consumer-friendly interpretation of that clause. It held that consumers would assume the privacy policy to be part of the terms and conditions of the order. Consequently, the privacy policy forms part of the terms and conditions and is subject to the same control.

On **19 November 2013**, the **Landgericht Berlin** (District Court of Berlin) issued a decision against **Google**.[78] The defendant offers numerous services on their website, i.e., a well-known internet search engine, specialised search engines for images, maps, books, movies, e-mail and calendar services. Many of these services can be used without registration and free of charge, whereas some services (i.e., the email service) require registration and some are chargeable.

The plaintiff, a registered consumer protection association, first successfully requested an injunction regarding the terms of use and its privacy policy against the defendant in 2008.[79] In the current case, the plaintiff requests an injunction against the defendant's updated Terms of Use and privacy policy (used on the website in July 2012).

One of the issues dealt with by the District Court of Berlin is the extent of the possibility to control privacy policies and terms of services, and whether certain clauses of the terms and conditions are void.

First, the court decides that the defendant's terms of use and privacy policy constitute terms and conditions and are, thus, subject to the same level of control. It is decisive that the defendant's conditions of contract are pre-formulated for a multitude of contracts and stipulated in a one-sided manner. Adopting the least consumer friendly interpretation of the website, the privacy policy is included in the analysis as it is impossible to sign up for the defendant's services without consenting to it and the terms of use through a single click-wrapping link. Consequently, the terms of use and the privacy policy constitute terms and conditions. In addition, the defendant's services do not constitute 'gifts' but a reciprocal relationship as the defendant makes use of collected information in exchange for the offered services.

Second, the court determines several clauses of the defendant's terms and conditions void. Regarding the terms and conditions, the court determines that the clauses are worded too broadly and that some clauses are too one-sided. For example, it is unclear to the consumer how the defendant examines the uploaded content and what constitutes infringements, because the clauses are worded too broadly and do not contain restrictions regarding conduct entailing criminal responsibility. The defendant also assumes continuing obligations although it needs to be possible to terminate the relationship in case of misconduct of either party. The privacy policy is similarly void as the consumer cannot understand from it in which ways his data is processed. Lastly, the clauses regarding 'android market' are illegal as far as the defendant is authorised to access the devices owned by the consumer, to unilaterally change the conditions of the contract and to terminate the use of services. Therefore, the court stresses that it does not matter whether the clauses are currently in use. Due to the abstract danger of re-offending, an official court injunction is necessary.

On **10 June 2016**, the **Landgericht Frankfurt** (District Court of Frankfurt) issued a decision against **Samsung Electronics**.[80] The plaintiff is the consumer protection association of North Rhine-Westphalia. It acquired a 'smart TV' produced by the defendant Samsung Electronics. These smart TVs feature the user surface 'Smart Hub' where the consumer can access third party applications, but also upload their own movies and receive recommendations regarding the TV programme. In the assembly

[78] Registration No. 15 O 402/12.

[79] LG Hamburg, judgment of 19.05.2011 - 10 U 32/09.

[80] Registration No. 2-03 O 364/15.

instructions, there was neither reference to the terms and conditions, nor to the privacy policy. The terms and conditions related to the privacy policy could be accessed after the assembly of the TV. During the first use of the TV, the TV uses the consumer's IP address to download and present the terms and conditions, as well as the appropriate privacy policy according to the region of the plaintiff. The plaintiff can then read the terms and conditions and the privacy policy displayed without sub-sections or headings, and then issue a blanket approval regarding them. The plaintiff complains that the HbbTV function was activated without the consent of the consumer, and that this function transfers data to the producer without previously informing or obtaining the consumer's consent.

Addressing the points raised by the plaintiff, the district court Frankfurt concludes that there is no duty for the defendant to inform the consumer about the activated HbbTV function, and the possible transfer of information. While this function transmits IP-addresses, §13(1) TMG is aimed at service providers who use data collected during the provision of the service. The defendant is not in a position where they have active knowledge of the data or the authority to dispose about the collected data, hence, §13(1) TMG is not applicable to the defendant.

While the district court Frankfurt addresses the points raised by the plaintiff, its focus is on controlling the terms and conditions, including therein also the privacy policy without explicit discussion. The district court raises this issue on its own motion and decides that the privacy policy lacks transparency. Due to its length and unclear presentation (56 TV pages in running text without sections or headings), the district court finds that the privacy policy is not a suitable basis for agreeing to the collection and use of data. Furthermore, the court does not deem the phrasing of the privacy policy suitable. The provider has to inform the consumer at the beginning of the use of the product, regarding the form, extent and purpose of collecting and using the data in an understandable manner.

Therefore, it is necessary to inform the consumer of which kind of data is collected. By using phrases including 'for example' and 'possibly' regarding the used data, the provider does not present an exhaustive list of what kind of data is collected and the consumer cannot validly agree.

France

The decision of the Paris First Degree Court, of 9 April 2019 No 14/07298 is of particular interest. In that decision, the Paris Hight Court noted that "by collecting data submitted free of charge by the user when accessing the platform and by marketing them for a fee, the company Facebook, which, acting for commercial purposes, makes a profit from its activity, is a professional within the meaning of the introductory article of the Consumer Code" (TGI Paris, 7 August 2018, No. 14/07300, UFC Que Choisir v. Twitter; TGI Paris, 12 February 2019, n°14/07224, UFC Que Choisir c/ Google). Thus, the Court affirmed that the contract concluded between the company Facebook and the member of its social network is a consumer contract, subject to all the provisions of consumer law, subject only that the member does not use the network for professional purposes (CJEU 25 January 2018, C-498/16, Schrems). French consumer law and the regulations relating to distance contracts, consumer information, unfair terms, form and interpretation of the contract are applicable. The relevant clauses relating to the definition of the purpose of the service provided by the company Facebook can be assessed on the basis of the regulations on unfair terms.

Two articles of the Consumer Code were used to support the judges' reasoning. Article L. 211-1 imposing an obligation of clarity in the drafting of clauses, which implies in particular the use of French, and Article L. 111-1 imposing a general obligation of pre-contractual information. The underlying idea was that the social network can neither collect nor share the personal data of its users without having clearly informed them about the economic value of their data, just as it can neither suggest that its social network is disinterested, nor suspend/delete an account without justification or recourse, nor modify the general conditions without the users' information or agreement, nor exclude any liability on its part. The judges also relied on the Law No. 78-17 of 6 January 1978 on information technology, data files and civil liberties

and justified its application with regard to Article 4§1(a) of the Directive 95/46/CE and to Article 5 1° of the referred Law No. 78-17. Indeed, the simultaneous display on the home page of the Facebook social network site of the user's personal data (surname, first name, date of birth) and advertisements related to the user's activities on the internet confirm that the sale of advertising space, conducted by the company Facebook, the data controller's establishment on French territory, constitutes processing of personal data within the meaning of Article 2(b) of Directive 95/46/EC and Article 2 of the Law No. 78-17 of 6 January 1978. The judges have used the Law No. 78-17 of 6 January 1978 in order to assess the illegality of the clauses and thus forbid the social network to use for free or to resell without time limit the contents created by its users, to indefinitely keep the data of its users even after the deletion of their account, or to remove a published content without warning its author.
Facebook has been convicted by the Paris First Degree Court for having inserted 430 abusive or illegal clauses in the Terms and Conditions of its social network with regard to Articles 6, 32-I, 32-II, 32-II of the Law No. 78-17 of 6 January 1978 on information technology, data files and civil liberties, the law of 4 August 1994, and article L. 211-1 of the French Consumer Code. They will therefore be deemed to be unwritten. Moreover, the judges order Facebook to allow all of its French members to read the entirety of this judgment by means of a hypertext link in an exclusively dedicated banner that must appear on the home page of its Internet site as well as on those of its tablet and telephone applications for a period of three months (for further information on that case, see the FRiCoRe database at this link).

EU law perspective

Article 3(1) of the ***UCTD*** provides that terms that have not been negotiated individually should be considered as unfair "if it causes a significant imbalance in the parties' rights and obligations arising under the contract". This provision leaves courts the possibility to consider if violations of information requirements under the GDPR cause a significant imbalance in the parties' rights and obligations.
Nevertheless, **in case of conflict between the UCTD and the GDPR**, the latter should be considered the *lex specialis* because it regulates the specific sector of data protection. Indeed, one could argue that Recital 42 of the GDPR provides indications on how to apply the UCTD in the area of data protection, (and therefore has *lex specialis* value) by providing that, "in accordance with Council Directive 93/13/EEC a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".
In July 2019, the Commission adopted a **Guidance Notice on the interpretation and application of the UCTD**.[81] The Guidance is remarkably silent about the interplay of transparency requirements under the directive and similar information duties under data protection provisions. However, concerning the interplay of transparency requirements under the directive and those in other EU instruments in general, the Guidance provides the following:

- "Where other EU provisions apply in addition to the UCTD, one will, in general, favour an interpretation that preserves as much as possible the *effet utile* of the UCTD and of a potentially conflicting provision. For instance, rules of procedure should not jeopardise the effectiveness of the protection against unfair contract terms under the UCTD" (p. 16).
- "Various EU acts regulate in a detailed fashion the pre-contractual information that traders have to provide to consumers in general or with regard to specific kinds of contracts. […] The UCTD is

[81] Commission notice — Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts, OJ C 323, 27.9.2019, pp. 4–92.

without prejudice to such provisions and the consequences of the failure to comply with them as set out in such specific instruments" (p.28).

- "Insofar as specific pre-contractual and contractual information requirements apply, they will also have to be taken into account for the transparency requirements under the UCTD, on a case-by-case basis, and in light of the purpose and scope of those instruments" (p. 28).
- "The fact of whether a seller or supplier has complied with sector-specific requirements is an important element when assessing compliance with the transparency requirements under the UCTD. However, given the parallel applicability of the UCTD with sectorial legislation, compliance with such instruments does not automatically indicate compliance with all transparency requirements under the UCTD" (p. 29).

Since this guidance was published after the entry into force of the GDPR, it is reasonable to assume that the Commission foresaw the interaction of then transparency requirements provided for in the UCTD and the GDPR when drafting these guidelines.

Regarding the relationship between information duties under the Consumer Rights Directive and the GDPR, see Section 9.4.2 below.

9.4.2. Question 4: Relationship between information duties under the Consumer Rights Directive and the GDPR

In light of the principle of effectiveness, proportionality, equivalence, dissuasiveness and Article 47 of the CFR, what is the **relationship between the information duties provided in Articles 5 and 6 of the Consumer Rights Directive** (2011/83) and in **Articles 13 and 14 of the GDPR**? Could the information duties provided in the Consumer Rights Directive be interpreted, in certain cases, as covering also the ones of the GDPR? What are the consequences on remedies available under the Consumer Rights Directive?

EU law perspective

In this area, the principle *lex specialis derogat legi generali* is confirmed by Article 3(2) of the **Consumer Rights Directive**, which provides that in case of conflict with another Union act governing specific sectors, the provision of that other Union act shall prevail and shall apply to those specific sectors.

In June 2014, the Commission adopted a **Guidance document concerning the Consumer Rights Directive.** This guidance states that, in case of conflicts about information requirements provided for in Directive 95/46/EC (the Data Protection Directive) or Directive 2002/58/EC (the ePrivacy Directive), these sector-specific requirements prevail. This is especially relevant in online sales for issues such as information about data processing and data subjects' consent to the tracking and use of personal data supplied. By extension, this could also hold true for the GDPR. Therefore, information duties from both the Consumer Rights Directive and the GDPR apply in parallel, but the ones from the latter prevail in case of conflict. This is consistent with the fact that the GDPR contains more detailed transparency requirements than the Consumer Rights Directive.

It is true that both consumer protection and data protection share **common purposes**, such as the free moments of goods and services in the internal market, transparency and fair treatment.

In that regard, it should be recalled that the under Article 13 of Directive 2011/83, as modified by Directive 2019/2161, that directive applies where the trader supplies or undertakes to supply digital content which is not supplied on a tangible medium or a digital service to the consumer and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content which is not supplied on a tangible medium or digital service or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose.

Furthermore, according to Article 6 of Directive 2011/83, as modified by Directive 2019/2161, before the consumer is bound by a distance or off-premises contract, or any corresponding offer, the trader shall provide the consumer with the information in a clear and comprehensible concerning, where applicable, that the price was personalised on the basis of automated decision-making. This provision may contribute to ensuring the effectiveness of data protection, by reinforcing information duties provided within data protection legislation.
Hence, the **remedies** available under the Consumer Rights Directive cannot be used against violations of information duties provided in the GDPR alone. Violations of information duties under the GDPR can only be remedied with the Consumer Rights Directive if they also constitute violations of information requirements under that directive.

9.4.3. Question 5: Relationship between the administrative and judicial authorities

In light of Articles 41 and 47 of the CFR, what is the **relationship between the administrative authorities and judicial ones**?

This question aims at analysing the possible impact of an administrative decision issued by a data protection authority which ascertains a data protection violation on a judicial proceeding concerning the ascertainment of a consumer law violation. In this respect, the new directive 2020/1828, on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC was adopted on 25 November 2020, and the new **Directive on the better enforcement and modernisation of Union consumer protection rules** should be considered.

EU law perspective

As explained in Section 9.1.2, Directive EU 2020/1828, on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC was adopted on 25 November 2020. With this new directive, the EU legislator set out rules to ensure that representative actions aimed at the protection of the collective interests of consumers are available in all Member States.
It should first be noted that the directive allows Member States to decide whether the representative action can be brought in judicial or administrative proceedings. Recital 19 of Directive 2020/1828 provides:
"Since both judicial proceedings and administrative proceedings could effectively and efficiently serve to protect the collective interests of consumers, it is left to the discretion of the Member States whether a representative action can be brought in judicial proceedings, administrative proceedings, or both, depending on the relevant area of law or the relevant economic sector**. This should be without prejudice to the right to an effective remedy under Article 47 of the Charter, whereby Member States are to ensure that consumers and traders have the right to an effective remedy before a court or tribunal, against any administrative decision taken pursuant to national measures transposing this Directive. This should include the possibility for a party in an action to obtain a decision ordering the suspension of the enforcement of the disputed decision, in accordance with national law.**"
The directive further deals with the coordination between administrative and judicial authorities. In particular, Article 15 of Directive 2020/1828 states:
"Member States shall ensure that the final decision of a court or administrative authority of any Member State concerning the existence of an infringement harming collective interests of consumers can be used by all parties as evidence in the context of any other action before their national courts or administrative authorities to seek redress measures against the same trader for the same practice, in accordance with national law on evaluation of evidence.".

On 27 November 2019, the European Parliament and the Council also adopted the new **Directive on the better enforcement and modernisation of Union consumer protection rules**, 2161/2019. The amending directive modernises Directive 2005/29/EC (unfair commercial practices), Directive 93/13/EEC (unfair contract terms), Directive 2011/83/EU (consumer rights) and Directives 98/6/EC (indication of prices).

The new directive provides that consumers will have the right to bring individual actions if they are harmed by unfair commercial practices, such as aggressive marketing. Member States shall provide for contractual and non-contractual remedies. At a minimum, contractual remedies shall include the right to obtain a price reduction or to terminate the contract. Non-contractual remedies shall, as a minimum, include the right to compensation for damages. To that effect, the new directive inserts a new Article 11a titled 'Redress' to Directive 2005/29/EC, which provides:

1. "Consumers harmed by unfair commercial practices, shall have access to proportionate and effective remedies, including compensation for damage suffered by the consumer and, where relevant, a price reduction or the termination of the contract. Member States may determine the conditions for the application and effects of those remedies. Member States may take into account, where appropriate, the gravity and nature of the unfair commercial practice, the damage suffered by the consumer and other relevant circumstances.
2. Those remedies shall be without prejudice to the application of other remedies available to consumers under Union or national law".

This right to individual remedies is being introduced in Directive 2005/29/EC because the Commission considered that consumers harmed by unfair commercial practices did not have access to effective remedies.

Taken together, both directives would allow consumers, which in some cases may be also data subjects, harmed by unfair commercial practices to initiate representative actions and seek the new remedies available for infringements of unfair commercial practices. While individual consumers should not be able to interfere with the procedural decisions undertaking by the qualified entities allowed to initiate the action, the consumers concerned by a representative action should be entitled to benefit from that representative action. In representative actions for redress measures, the benefits should come in the form of remedies, such as compensation, repair, replacement, price reduction, contract termination or reimbursement of the price paid. In representative actions for injunctive measures, the benefit for the consumers concerned would be the cessation or prohibition of a practice that constitutes an infringement (recitals 36 and 37).

9.4.4. Question 6: Lack of conformity of digital content or services and the GDPR compliance

In light of the principle of effectiveness, dissuasiveness and of Article 47 and Article 8 CFR, could the consumer remedies against a lack of conformity of a digital content/service provided by Directive 2019/770 be used against a violation of data protection law?

New Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services

Directive 2019/770 (the ***Digital Content Directive***) was published in May 2019.[82] As part of the EU's Digital Single Market strategy, this directive fully harmonises certain key contractual rules for the supply of digital content or services. Member States have until 1 July 2021 to adopt and publish the measures necessary to comply with this directive. They shall apply those measures from 1 January 2022.

Among the measures that Member States must transpose there are remedies for lack of conformity of the digital content or service offered by a trader. In this respect, Article 14 of the directive provides for

[82] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *O.J.E.U.*, 22.5.2019, L 136/1.

three options for the consumer: (i) have the digital content or service brought into conformity; (ii) receive a proportionate reduction in price; or (iii) terminate the contract, in accordance with the conditions established by the directive.[83] When it comes to compensation, Article 3(10) of the directive provides that Member States are free to regulate the right to damages in case of violations of their national legislation transposing the directive. However, it is beyond the scope of this Casebook to detail these remedies extensively. Instead, the question at hand is whether these remedies for lack of conformity of a digital content or service can be used for violations of data protection law.

The scope of the directive is rather broad, as it applies to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price.[84] **Furthermore, Article 3(1) of the directive, which provides that it applies *"where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader".***

In this regard, Recital 24 of the directive provides the following:

"*Such business models are used in different forms in a considerable part of the market. While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies. This Directive should, therefore, apply to contracts where the trader supplies, or undertakes to supply, digital content or a digital service to the consumer, and the consumer provides, or undertakes to provide, personal data. The personal data could be provided to the trader either at the time when the contract is concluded or at a later time, such as when the consumer gives consent for the trader to use any personal data that the consumer might upload or create with the use of the digital content or digital service. Union law on the protection of personal data provides for an exhaustive list of legal grounds for the lawful processing of personal data. This Directive should apply to any contract where the consumer provides or undertakes to provide personal data to the trader. For example, this Directive should apply where the consumer opens a social media account and provides a name and email address that are used for purposes other than solely supplying the digital content or digital service, or other than complying with legal requirements. It should equally apply where the consumer gives consent for any material that constitutes personal data, such as photographs or posts that the consumer uploads, to be processed by the trader for marketing purposes. Member States should however remain free to determine whether the requirements for the formation, existence and validity of a contract under national law are fulfilled".*

Taking into account the possibility of processing personal data for commercial purposes, Directive 2019/770 extends some contractual remedies where the professional provides a digital content, or a service and the consumer/data subject "provides" personal data. With regard to the wording « the consumer provides or undertakes to provide personal data », the interpretation of similar wording in the GDPR is relevant. Article 20 GDPR on the right to data portability refers to personal data that, "have been provided" by the data subject, and the WP29 (the *Guidelines on the right to data portability*, 2017) interpreted it in an extensive way, including both data actively provided by the consumer or «observed data». Directive 2019/770 could be interpreted in the same way, also considering that the interpretation allows to better apply the directive in the online context, where most of personal data are collected through the observation of data subject's activity.

The directive also provides that Union law on the protection of personal data, especially the ***GDPR***, shall apply to any personal data processed in connection with such contracts.[85] In case of conflict between Directive 2019/770 and data protection law, the latter prevails.[86]

In the same vein, Recital 48 of the directive explicitly mentions that the lack of compliance with the GDPR may constitute a lack of conformity in the sense of the Digital Content Directive:

---

[83] Article 14 of Directive (EU) 2019/770.

[84] Article 3(1) of Directive (EU) 2019/770.

[85] Article 3(8) of Directive (EU) 2019/770.

[86] Article 3(8) of Directive (EU) 2019/770.

"Facts leading to a lack of compliance with requirements provided for by Regulation (EU) 2016/679, including core principles such as the requirements for data minimisation, data protection by design and data protection by default, may, depending on the circumstances of the case, also be considered to constitute a lack of conformity of the digital content or digital service with subjective or objective requirements for conformity provided for in this Directive. One example could be where a trader explicitly assumes an obligation in the contract, or the contract can be interpreted in that way, which is also linked to the trader's obligations under Regulation (EU) 2016/679. In that case, such a contractual commitment can become part of the subjective requirements for conformity. A second example could be where non-compliance with the obligations under Regulation (EU) 2016/679 could, at the same time render the digital content or digital service unfit for its intended purpose and, therefore, constitute a lack of conformity with the objective requirement for conformity which requires the digital content or digital service to be fit for the purposes for which digital content or digital services of the same type would be normally used".

Therefore, if there is an infringement of data protection law in processing the personal data collected by a trader and the directive applies, the consumer would be able to seek remedies available under the Digital Content Directive if that mishandling of personal data also constitutes a lack of conformity and all conditions laid down in the directive are fulfilled. Recital 48 of the directive confirms this finding:

"Where the facts leading to non-compliance with requirements under Regulation (EU) 2016/679 also constitute a lack of conformity of the digital content or digital service with subjective or objective requirements for conformity as provided for in this Directive, the consumer should be entitled to the remedies for the lack of conformity provided for by this Directive, unless the contract is already void or voidable under national law".

In this respect, the **principle of effectiveness, Article 47 and Article 8 CFREU** should be taken into account by Member States in the implementation of Directive 2019/770 and by courts in its interpretation. In particular, it raises the question whether the compliance with data protection law of the service and of the digital content is to be qualified as an objective requirement for conformity, regulated by Article 8 of that directive. Another issue is the relationship between the information provided to the data subject in accordance with Regulation 2016/679 and Article 7 of Directive 2019/770, which regulates the subjective requirements for conformity of digital content or service. It should also be considered that in several cases traders which enter in a contract with the economic operator, such as an online platform, or a social network are data subjects (See figure 1) which are active on digital environments. In this respect, the following question raises:

In light of Article 47 and 8 CFR, does the remedy consisting in the brought into conformity of a service with regard to data protection compliance could be applied by analogy, in order to grant the right to data protection also in cases in which the data subject is not a consumer, and operates in a digital environment which is not compliant with data protection requirement?

Furthermore, consumers are not the only ones who can seek remedies for lack of conformity. In order to guarantee effective enforcement of the directive's provisions, Member States shall include in their legislation the possibility for either public bodies, consumer organisations, professional organisations or not-for-profit bodies active in the field of data protection to take action under national law before courts or administrative bodies.[87] Member States are free to choose which of these types of organisations (one or more) will be able to take action.

When implementing the Digital Content Directive, Member States must therefore take into account the articulation between the two sets of laws: not only the remedies provided for in the directive, but also the

[87] Article 21(2) of Directive (EU) 2019/770.

collective redress mechanism foreseen in the GDPR. Indeed, the combination of both schemes is currently the best way to ensure effective consumer protection in the data protection space.

9.5. Guidelines emerging from the analysis

The general issue addressed in this chapter concerns the role of the application of consumer law in ensuring effective data protection (Article 8 and Article 47 CFR).

Collective redress between collective and data protection

With regard to collective redress, national legislation could allow consumer protection associations

a) to bring or defend legal proceedings against a person allegedly responsible for an infringement of the protection of personal data (*Fashion ID,* C-40/17);
b) to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects, against the person allegedly responsible for an infringement of the data protection laws, on the basis of consumer protection law infringment, where the data processing concerned is liable to affect data subjects rights provided for by the GDPR (*Facebook Ireland Limited,* C-319/20).

Furthermore, when a violation of the GDPR violates the interests of consumers, and the person harmed is a consumer, Directive 2020/1828 on representative actions for the protection of the collective interests of consumers, which repeals Directive 2009/22 is to be applied. In any case, the relationship between collective redress in consumer and data protection should be carefully assessed; the existence of collective redress in consumer law, applicable to consumers who seek action for a data protection claim may not be sufficient for ensuring effective data protection, especially within the digital context (e.g., where the parties are a small professional and an online platform).

Unfair commercial practices and information provided to the data subject

In light of the EU Commission's *Guidance on the implementation/application of the Unfair Commercial Practices Directive,* although a trader's violation of Data Protection rules will not, in itself, always mean that there is an unfair commercial practice, data protection violations should be considered when assessing the overall unfairness of commercial practices, particularly in the situation where the trader processes consumer data in violation of data protection requirements. The Italian decisions of the Consumer protection authority, of the Administrative Tribunal of Rome and of the Council of State are examples of the interplay between data protection rules and Directive 2005/29.

Information to be provided to the data subject and consumers rights (Directive 2011/83)

The amendments of Directive 2011/83 provided in Directive 2019/2161 show the importance of the relationship between data and consumer law. In fact, the directive applies where the trader supplies or undertakes to supply digital content which is not supplied on a tangible medium or a digital service to the consumer and the consumer provides or undertakes to provide personal data to the trader, except in some specific cases (Article 3 Directive 2011/83). Moreover, before the consumer is bound by a distance or off-premises contract the trader shall provide the consumer with the information concerning the fact that the price was personalised on the basis of automated decision-making. This provision may contribute to ensuring the effectiveness of data protection, by reinforcing information duties provided within data protection legislation.

However, the **remedies** available under the Consumer Rights Directive cannot be used against violations of information duties provided in the GDPR alone. Violations of information duties under the GDPR can only be remedied with the Consumer Rights Directive if they also constitute violations of information requirements under that directive.

Information to be provided to the data subject and unfair contractual terms

National case law (especially French and German one) shows the importance of the interplay, with regard to information duties, of the GDPR and the UCTD directive. There are no EU case law or documents in that regard. Nevertheless, the principle of effectiveness and Article 47 and 8 CFREU may be of important guidance in order to interpret the relationship between the concept of unfairness under Directive 1993/13 and breaches of data protection law.

Competent administrative authorities and their coordination

As explained in a joint statement by the Italian consumer, telecom, and data protection authorities of July 2019, **data protection and consumer protection are seen to be complementary and not exclusive from one another**.
The same conduct can constitute an infringement of consumer, data protection, and competition law; the **coordination between the national and European authorities** in charge of consumer, data protection, and competition enforcement is a key issue, as the lack of such coordination may have negative consequences on the principles of effectiveness, good administration and the duty of cooperation.

Lack of conformity of digital content or services and the GDPR compliance

In light of Article 47 8 CFR, and of recital 48 of Directive 2019/770 on digital contents and services, the remedy consisting in the brought into conformity of a service with regard to data protection compliance could be a mean for granting to consumers the right to data protection.