RE-JUS CASEBOOK

EFFECTIVE JUSTICE IN DATA PROTECTION

THE RE-JUS PROJECT IS CO-FUNDED BY THE JUSTICE PROGRAMME OF THE EUROPEAN UNION
(JUST/2015/JTRA/AG/EJTR/8703)
A collection of case law on the application of EU principles of effectiveness, proportionality and dissuasiveness and of Article 47, Right to an effective remedy, of the Charter of Fundamental Rights of the European Union, in matters related to data protection.

Published in October 2018

Published in the framework of the project:

Roadmap To European Effective Justice (Re-Jus):
Judicial Training Ensuring Effective Redress To Fundamental Rights Violations.

Coordinating Partner:
University of Trento (Italy)

Main Partners:
University of Versailles Saint Quentin-en-Yvelines (France)
Institute of Law Studies of the Polish Academy of Sciences (Poland)
University of Amsterdam (The Netherlands)

Associate Partners:
Scuola Superiore della Magistratura (Italy)
Consejo General del Poder Judicial (Spain)
Institutul National al Magistraturii (Romania)
Pravosudna Akademija (Croatia)
Ministrstvo za pravosodje Republika Slovenije (Slovenia)
Judicial Studies Committee of the Irish Judiciary (Ireland)
Scientific Coordinator of the Re-Jus Project:

Fabrizio Cafaggi

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

Sandrine Clavel

Project Manager:

Chiara Patera

Coauthors of this Casebook (in alphabetical order):

Federica Casarosa
Sandrine Clavel
Mélanie Clément-Fontaine
Paola Iamiceli
Célia Zolynski

Note on national experts and collaborators:

The Re-Jus team would like to thank all the judges, experts and collaborators who contributed to the project and to the casebook by suggesting national and European case law (in alphabetical order):

Roberta Brusco  Carmen Domocos  Romain Perray
Luigi Cannada Bartoli  Lorette Dubois  Gianmatteo Sabatino
Francesca Capotorti  Malte Engeler  Wojciech Sawczuk
Stefano Caramellino  Martina Flamini  Chiara Tea Antoniazzi
David Castillejos Simon  Florence Gaullier  Lavinia Vizzoni
Jaroslaw Czarnota  Fabienne Jault  Margaux Voelckel
Silvia Dalle Nogare  Karin Kieffer  The students of Master PIDAN
Fiorella Dal Monte  Maria Teresa Leacche  (UVSQ/Saclay)
Nicole Di Mattia  Isabella Oldani
Introduction: a brief guide to the casebook

In line with the methodology developed in Re-Jus and the related judicial training projects, the Re-Jus Casebook on Effective Data Protection has been drafted based on collaboration between academics and judges of various European countries. This collaboration permits the combination of rigorous methodologies with judicial practices, and provides the trainers with a wealth of comparative material.

The Casebook was enriched thanks to the work done during the training seminars. Training included not only the transfer of knowledge but the creation of a learning community composed of different professional skills. This Casebook is the result of this work; it has evolved both in content and method over time with additional suggestions coming from its use in training events.

Judicial dialogue is another key dimension of the approach in this Casebook. The development of EU law is driven by the dialogue between CJEU, the ECtHR and national courts and, increasingly, by the dialogue among national courts of different Member States (MS). In preliminary ruling procedures, the Casebook investigates the full life cycle of a case, from its origin with the preliminary reference, to its impact in different MS. The Casebook examines the upstream phase and analyses why and how the preliminary reference is made, and whether and how the questions referred are reframed by the Advocate General and by the Court. We then analyse the judgments, distinguishing between them in terms of the degree of detail, where they provide guidance both to the referring court and to the other courts that have to apply the judgments in the various MS. The CJEU clearly signals the degree of specificity of the question and answers it accordingly. Sometimes it gives a very context-specific answer, not easy to generalize and to apply to other legal systems; sometimes it defines general principles that can be flexibly applied to different legal systems.

Data protection is characterized by a strong dialogue between administrative authorities, which interact, and judicial authorities. Hence judicial dialogue is complemented by administrative dialogue. This dialogue is set to develop further through the European Data Protection Board established by Article 68 of 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, hereinafter GDPR). Important tools will be the guidelines, recommendations and best practices to be issued by supervisory authorities for enhancing their own cooperation and the consistent application of EU law. Pursuant to the new Regulation, these regulatory instruments will also specifically address the application of enforcement measures and the setting of administrative fines pursuant to article 83 GDPR. Additional forms of coordination among courts are envisaged in case of cross-border infringements (see article 81). While national procedural autonomy is indeed acknowledged and preserved in the new legal framework, the role of general principles establishing procedural safeguards, including fair trial and access to justice, is expressly identified as a limitation on that autonomy. Such principles themselves call for stronger coordination among multiple enforcers, including supervisory authorities and courts, as is shown in the mechanisms envisaged for the imposition of fines (see article 83 GDPR).

While alive to future developments, the Casebook provides information on the current interaction at
state and EU level between data protection authorities and courts. Fundamental rights play an important role both in judicial and administrative enforcement and article 47 offers guidance on the overall enforcement architecture (see CJEU Puškár).

By contrast with the organization of training material in previous projects (JUDCOOP and ACTIONES) we have decided to cluster European judgments around common issues, instead of focusing on a single judgment. Often, CJEU judgments touch on many questions depending on how the preliminary references are framed, and it seems more effective to choose a subset of complementary issues and examine them in sequence across several cases, rather than focus on a single judgment. This approach may add a degree of complexity, but it reflects the problem-solving approach, rather than the conventional perspective. The internal coordination of the chapters makes it possible to reconstruct the judgment from the different chapters.

The casebook aims to offer a comparative perspective of the impact the judgment, or a cluster of judgments addressing the same issue (for example, the impact of data protection on access to justice when the rules on burden of proof may conflict with data protection) has on the case-law of MS other than the state of the referring court. In some cases, the impact can be examined through judgments expressly referring to the CJEU’s decisions; in others, 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 in countries other than the referring one. The efforts they make to interpret and adapt the judgment to their national legal context is often underestimated. While, formally, the CJEU judgments are binding on MS courts, their application requires a careful analysis of which substantive and procedural rules may be affected by them, in particular the application of article 47 of the Charter and the principle of effectiveness.

The judgments and their impact show that the application of the Charter, and in particular article 47, is promoting substantive and procedural changes in data protection. Some of these changes have been incorporated into the GDPR. Some remain part of a long-standing judicial dialogue involving the ECtHR, the CJEU and national courts.

Despite the fact that article 47 CFREU is not directly applicable to administrative enforcement and that the scope of article 41 CFREU is limited, it is likely that similar principles such as the right to proper administration will emerge in order to coordinate the different forms of data protection, including administrative, judicial and non-judicial mechanisms. In the absence of EU legislation on the point, it is likely that the CJEU will continue to play a leading role in devising coordination tools, as recently shown in the Puškár case. Judicial dialogue can be usefully deployed to promote homogeneity across MS in order to ensure that effective data protection is not undermined by too high a variation in procedural rules concerning individual and collective remedies.

The Casebook is complemented by a Database that endorses the methodological approach of judicial dialogue. It is organized 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 under a preliminary reference procedure, and those that apply or take into consideration the CJEU case-law in national cases outside of any referral procedure. Hence, the database is specific, and it reflects the idea that judicial dialogue is a pillar of EU data protection.

We would like to encourage training courses organized by national judicial schools to use both the Casebook and the Database, which will be subject to constant updating during the course of the
project thanks to contributions from the Schools of the Judiciary and the workshops’ participants.

The Casebook comprises six Chapters, all focused, from different angles, on the impact of the Charter of Fundamental Rights on enforcement of data protection law by administrative authorities and courts. Indeed, articles 7-8 CFREU (and before it article 8 ECHR), on the one hand, and the general principles of effective judicial protection, on the other, now reinforced and complemented by article 47 CFREU, have contributed through judicial dialogue to defining the scope of data protection in terms of both its territorial scope (see Chapter 1 of this Casebook) and material scope (see Chapter 2). In most cases this impact emerges from a balancing exercise carried out by administrative authorities and courts facing the – often conflicting – dynamics between data protection and the protection of other fundamental rights or legitimate interests (see Chapters 3 and 5). The relation between administrative and judicial enforcement in data protection is examined in Chapter 4, showing how judicial dialogue triggered through preliminary references complements the rules of coordination in multiple enforcement systems, with some additional limitation on national procedural autonomy. Chapter 5 is focused on enforcement procedures and on the role of the principle of effectiveness in striking the balance between data protection and access to justice. More particularly, the analysis focuses on the burden of proof and the extent to which data protection may (or may not) limit access to the kinds of evidence that are necessary to go to court: a new balancing act to challenge the courts and administrative authorities. The choice and the modes of application of remedies and sanctions are at the core of Chapter 6. As in other fields (see the Re-Jus Casebooks on Effective Consumer Protection and on Effective Protection in the field of Asylum and Migration Law), general principles such as effectiveness, proportionality and dissuasiveness play a major role in shaping the path of judicial dialogue and leading national enforcers towards effective data protection. Within a still rather fragmented legal framework across MS where systems of sanctions and remedies are concerned, the use of remedies remains a difficult challenge for supervisory authorities and courts, and judicial-administrative dialogue is a valuable resource.
# TABLE OF CONTENTS

INTRODUCTION: A BRIEF GUIDE TO THE CASEBOOK

## INTRODUCTION

Evolution of DP in EU law ................................................................. 8
The impact of the Charter on DP law ................................................... 8
EU legal sources .............................................................................. 9
Judicial dialogue dimension ............................................................. 11
Horizontal judicial dialogue and article 81 GDPR ............................... 13
New challenges emerging from GDPR ........................................... 14

## 1. IMPACT OF THE CHARTER ON THE TERRITORIAL SCOPE OF DATA PROTECTION

1.1. Introduction .................................................................................. 18
1.2. Intra-EU relations ................................................................. 19

*Question 1*: Interpretation of the connecting factor defining the territorial scope of a Member State’s law on data protection ................................................................. 20

*Question 2 & 3*: Coordination between national data protection authorities regarding intra- EU cross border processing ............................................................................. 29

*Question 2*: The competence of Member States’ data protection authorities in cross-border situations ................................................................. 30

*Question 3*: Impact of the territorial limitation of national data protection authorities: the duty of cooperation ................................................................. 35

3. a) – Duty of cooperation between MS Data protection authorities ................................................................. 35

3. b) - Absence of hierarchy between MS data protection authorities exercising competence over the same data processing ............................................................................. 40

*Questions 4 & 5*: Coordination between national courts regarding intra- EU cross-border processing ................................................................. 44

1.3. Relations with third countries .................................................. 51

*Question 6 & 7*: The scrutiny of third countries’ legislation in terms of EU law and its consequences ................................................................. 54

## 2. IMPACT OF THE CHARTER ON THE MATERIAL SCOPE OF DATA PROTECTION

2.1. Introduction .................................................................................. 59
2.2. The general scope of data protection ........................................... 60

*Question 1 (a) and 1 (b)* – Definition of the concept of “processing” of personal data ................................................................. 63

*Question 2*: Definition of the concept of “personal data” ................................................................. 70

*Question 3*: Definition of the concept of “controller” ................................................................. 77

*Question 4*: Definition of the concept of “data subject” ................................................................. 82

2.3. 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 ................................................................. 84

*Question 5*: The extension of the protection of data in the field of State security matters ................................................................. 84

## 3. IMPACT OF THE CHARTER ON THE ASSESSMENT OF THE LEGITIMACY OF DATA PROCESSING

3.1 Introduction .................................................................................. 97

*Question 1*: The balance between data subjects’ rights to the protection of privacy and personal data, and others legitimate private interests ................................................................. 101

## 4. EFFECTIVE DATA PROTECTION BETWEEN ADMINISTRATIVE AND JUDICIAL ENFORCEMENT

4.1. Introduction .................................................................................. 111

*Question 1*: The right to effective judicial remedy and the coordination of administrative and judicial enforcement ................................................................. 113

*Question 2*: Interaction between the CJEU and the ECHR ................................................................. 120

*Question 3*: Coordination between EU institutions and national authorities ................................................................. 122

*Question 4*: Duty of cooperation of national authorities regarding the possible invalidity of an EU act ................................................................. 124

*Questions 5 & 6*: Interaction between national administrative and judicial proceedings ..., 126
5. Impact of the Charter on the Conduct of Proceedings

5.1. Introduction

Question 1: Admissible evidence of a violation of data protection

Question 2: Evidence obtained through unlawful processing of data

6. Effective, Proportionate and Dissuasive Sanctions and Remedies

6.1. Introduction

Question 1: The use of “corrective remedies” and the right to be de-listed

Question 2: Effective remedies and the principle of full compensation

Question 3: Collective redress

Question 4: The sanctioning powers of national data protection authorities

Question 5: Proportionate and dissuasive remedies or sanctions in data protection

Question 6: The application of consumer protection to data subjects
Introduction

Evolution of DP in EU law

Since 1995, the EU legislator has addressed the need to protect citizens’ data across Member States with the aim of facilitating internal cross-border data transfers within the EU. The need to harmonise legislation across MS proved more compelling as different standards were applied under the different legislation in force, with different level of protection potentially hampering the free flow of personal data. As a result, 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 was adopted in order to harmonise the protection of fundamental rights of individuals with regard to data processing activities. The implementation at national level required by the Directive, however, failed to achieve the objective of harmonising data protection legislation within the EU.

In the meantime, several other legal instruments were adopted in order to resolve the issues emerging in those areas where data protection converged with technological developments and specific areas of law, such as Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, and Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data.

Faced with a level of fragmentation and divergence in MS data protection legislation that was no longer tolerable, the EU embarked on a wide-ranging reform in the field of data protection. Among the most compelling, though sensitive, needs to emerge was the updating of Directive 95/46 in order to remove the potential obstacles to the free flow of data and to keep pace with the technological developments that in twenty years had radically changed social and economic conditions in the market. The long negotiation process resulted in the adoption, in 2016, of the General Data Protection Regulation. The choice of a Regulation was designed to achieve harmonisation, as the regulation is directly applicable; however, it contains initial clauses that allow latitude for national specificities.

The impact of the Charter on DP law

Through the entry into force of the Lisbon Treaty, the Charter of Fundamental Rights became binding and the right to the protection of personal data enshrined in article 8 of the Charter acquired recognition and autonomy vis-à-vis the right to respect of private life. These fundamental rights require, on the one hand, detailed implementation by the enactment of data protection legislation at European and national level, and on the other impose the definition of remedies. Although the CJEU has explicitly addressed the coordination between the two Charter provisions only on a few occasions, in several other cases the Court has adjudicated on the basis of the principle of effectiveness, steering towards a high standard for data protection.

---

1 Drafted by Federica Casarosa with the collaboration of Chiara Tea Antoniazzi, Isabella Oldani and Gianmatteo Sabatino.
The clusters of cases that will be presented in the Casebook show that the application of the Charter by the CJEU is promoting substantive and procedural changes in the field of data protection. In particular, the principle of effectiveness has triggered innovation in the substantive rules addressing the definition of data processor and data treatment (see in particular Chapter 2), and also in the concept of ‘establishment’ allowing the national supervisory authority to exercise its competence in transborder cases and imposing a duty to cooperate with foreign supervisory authorities (see in particular Chapters 1 and 4). Article 47 CFREU has impacted both substantive law, being the yardstick for evaluating the validity of EU law that proves not to meet the demands of justice, and procedural law, being the basis for evaluating whether rules on admissibility of evidence affect effective access to justice (see in particular Chapter 5). Furthermore, based on the Charter, the CJEU has developed a very precise methodology relying on the principle of proportionality in order to balance conflicting fundamental rights and interests. That methodology is a recurring theme throughout the Casebook, particularly when dealing with the assessment of the legitimacy of data processing (Chapter 3), the admissibility of evidence (Chapter 5) or sanctions and remedies (Chapter 6).

**EU legal sources**

<table>
<thead>
<tr>
<th><strong>Primary Law</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Article 16 Treaty on the Functioning of the European Union</strong></td>
</tr>
<tr>
<td>1. Everyone has the right to the protection of personal data concerning them. 2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.</td>
</tr>
<tr>
<td><strong>Charter of Fundamental Rights of the European Union</strong></td>
</tr>
<tr>
<td><strong>Article 7 (Respect for private and family life):</strong> “Everyone has the right to respect for his or her private and family life, home and communications”</td>
</tr>
<tr>
<td><strong>Article 8 (Protection of personal data):</strong> “1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority”</td>
</tr>
<tr>
<td>International Agreements</td>
</tr>
<tr>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Agreement</strong> between the <strong>United States of America</strong> and the <strong>European Union</strong> on the Protection of Personal Information relating to the Prevention, Investigation, Detection, and Prosecution of criminal offenses signed on <strong>2 June 2016</strong> (Umbrella Agreement)</td>
</tr>
<tr>
<td><strong>Agreement</strong> between the <strong>United States of America</strong> and the <strong>European Union</strong> on the use and transfer of passenger name records to the United States Department of Homeland Security signed on <strong>14 December 2011</strong></td>
</tr>
<tr>
<td>Agreement between the <strong>European Union</strong> and the <strong>United States of America</strong> on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program signed on <strong>28 June 2010</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Secondary Law</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Commission Implementing Decision (EU) 2016/1250</strong> of <strong>12 July 2016</strong> pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield</td>
</tr>
<tr>
<td><strong>Regulation (EU) 2016/679</strong> of the European Parliament and of the Council of <strong>27 April 2016</strong> 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)</td>
</tr>
<tr>
<td><strong>Directive (EU) 2016/680</strong> of the European Parliament and of the Council of <strong>27 April 2016</strong> on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA</td>
</tr>
<tr>
<td><strong>Directive (EU) 2016/681</strong> of the European Parliament and of the Council of <strong>27 April 2016</strong> on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime</td>
</tr>
<tr>
<td><strong>Council Framework Decision 2008/977/JHA</strong> of <strong>27 November 2008</strong> on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters</td>
</tr>
</tbody>
</table>

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

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

European Convention on Human Rights

Art 8 ECHR
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, Convention 108, 8 November 2001

Judicial dialogue dimension

This Casebook focuses on the judicial dialogue emerging across European and national courts in the area of data protection. This methodology allows analysis of the full cycle of the case, starting from the preliminary reference (and potentially the conflicting national jurisprudence that triggered the emergence of the underlying legal question), through the preliminary ruling, to the follow up judgment and the impact of the European decision in different MS from the referring state.

This analysis provides for a wider picture regarding the interplay between European and national courts, showing whether and how the preliminary reference tool is used by courts strategically: for instance, the CJEU may reframe the question referred by the national court so as to address a more general question on the compatibility of national laws with EU law, in order to detach it from the specificity of the national case and provide guidance to all MS. Similarly, national courts may decide to present a preliminary ruling not only to solve a conflict in interpretation of the EU law provision, but also satisfy to an underlying objective of modifying the existing jurisprudence on the provision in question.

The follow up decision, then, is relevant as it allows verification of whether and how the referring court has interpreted the guidance provided by the CJEU, and, where available, the impact of the same decision in other jurisdictions where judges have undertaken the difficult exercise of interpreting the decision and adapting it to their own legal context.
A clear example is the case of Google Spain, where the CJEU addressed the request of the Audiencia national concerning a dispute between a Spanish citizen and Google Spain. The case was an appeal against the decision of the national DP authority to the effect that, as search engine operators subject to data protection legislation, Google should limit access to some personal data where the fundamental right to data protection is at stake. Given the ubiquitous use of search engines and the ongoing debate, also before national courts, regarding the balance between freedom of expression, data protection and freedom to conduct a business, the CJEU decision had a substantial impact not only in Spain, where the courts easily adapted the national jurisprudence to the CJEU decision, but also in other jurisdictions. For instance, in Italy, the CJEU decision affected the criteria governing the proportionality test involved in the balancing exercise between the right to information and the rights to respect for private life and to protection of personal data. As a matter of fact, the CJEU decision (and the guidance provided by the Article 29 Working Party after the decision) allowed the national courts to take into account not only the passing of time, which was crucial in the landmark decision of the Italian Supreme Court in 2012, but also the public role of the data subject, as the recent decisions of lower courts show (e.g. decision no. 10374/2016 by the Tribunale of Milan, Chapter 6, question 1). Moreover, the CJEU decision has affected the way in which national courts apply the proportionality test taking into account the specific context of Internet diffusion, in that the criteria have been adjusted so as to ensure a high level of protection for data subjects.\(^3\)

Judicial dialogue takes place vertically between the CJEU and the ECtHR and national courts, and horizontally between European and domestic courts. Vertical judicial dialogue among courts may also overlap with horizontal dialogue. In particular, this may occur when the European courts address similar issues in their decisions. This involves an additional layer of analysis, if not an additional interpretative effort for national courts. As a matter of fact, the effects of CJEU decisions differ from those of the ECtHR, the former being immediately binding not only on the national referring court, but also the other MS courts. The latter, however, may need a longer process in order to be implemented, even requiring the national courts to re-open a closed case, and the other contracting states have discretion as to the role of ECHR jurisprudence in their legal systems, ranging from countries where the ECtHR jurisprudence is legally binding to those where it is only an interpretative tool.\(^4\) However, in both cases, national courts have to be aware of, and consistent with, the standards laid down by the European courts.

One example of horizontal dialogue is the ECtHR decision in Satamedia Oy v. Finland, decided on 27 June 2017. Here again, the ECtHR engages in the balancing of freedom of expression and the right to respect for private life, already addressed in several previous judgments by the same court,\(^5\) bearing in mind that the case had already triggered a

---

\(^3\) See Italian Court of Cassation, decision no. 13161/2016; Italian Court of Cassation, decision no. 13151/2017.


preliminary reference to the CJEU, decided in 2008. The case concerned two companies that published data on the income of individual persons in a newspaper and, in 2003, also made them available through an SMS service. Although, under Finnish law, such data was accessible to the public, the companies were requested to stop publishing tax data in such a manner and to such an extent. The companies then claimed before the ECtHR that their right to freedom of expression had been violated, as the collection of tax information was not illegal and the information collected and published was in the public domain. The decision applied the standard already defined in previous jurisprudence on the fair balance between freedom of expression and the right to respect for private life, which included consideration of contribution to a debate of public interest; the degree to which the person affected was well-known; the subject of the news report; the prior conduct of the person concerned; the method of obtaining the information and its veracity; and the content, form and consequences of the publication. The Court’s decision engages extensively with the EU Data Protection Directive and the related jurisprudence of the CJEU. However, while the CJEU held that journalism must be interpreted broadly in light of the right to freedom of expression, the ECtHR affirmed that derogations and limitations on the right to protection of personal data enshrined in the Directive must be allowed only insofar as strictly necessary to achieve a balance between the competing rights. Thus, given that the Finnish court had applied the stricter test, no violation of article 10 was found.

**Horizontal judicial dialogue and article 81 GDPR**

Moreover, the increasingly transborder nature of data processing through technological means requires an additional element which is only addressed in passing by the GDPR in article 81, whereby in case of claims by data subjects located in different MS relating to the same conduct, there is the possibility for the court to suspend the proceedings, or possibly consolidate the claims. The rule governs simultaneous proceedings for the same infringement in various MS. Such cases will give rise to problems of coordination, and decisions either to stay proceedings or to continue them will require courts in different countries not only to be informed of the existence of such overlapping cases, but also to identify whether and how the decision of the foreign court might affect their own proceedings.

Similar issues apply to data protection authorities. No rules exist to regulate coordination between a data protection authority in country A and a court in country B. Coordination problems and the applicability of article 81 to these cases will likely generate preliminary references to the CJEU.

---

6 Case C-73/07 Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, EU:C:2008:727
7 Article 81 on Suspension of proceedings provides that:

1. Where a competent court of a Member State has information on proceedings, concerning the same subject matter as regards processing by the same controller or processor, that are pending in a court in another Member State, it shall contact that court in the other Member State to confirm the existence of such proceedings.

2. Where proceedings concerning the same subject matter as regards processing of the same controller or processor are pending in a court in another Member State, any competent court other than the court first seized may suspend its proceedings.

Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof.”
New challenges emerging from GDPR

DPAs enhanced powers – a shift towards stronger administrative enforcement?

In Directive 95/46, the powers of the national supervisory authorities and the sanctioning measures were left almost completely to MS, both in terms of institutional organisation and procedural autonomy. On the one hand, article 28 of Directive 95/46 provided only for a minimum standard as regards the powers allocated to the (required) national supervisory authority; on the other, article 22 of Directive 95/46 left MS the choice of introducing different types of sanctions (administrative fines or penalties) in case of data protection breaches.

The approach of GDPR is radically different: the GDPR allocates stronger enforcement powers to national supervisory authorities and provides for a more detailed definition of (administrative) fines in case of data protection breaches. In particular, article 58 GDPR requires national supervisory authorities to have an array of investigative, corrective, advisory and authorisation powers, among them in particular the possibility “to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case”. In article 83 GDPR, administrative fines are extensively defined, including a wide set of criteria to steer the decision of the enforcer in applying the proportionality test, ranging from the current (and previous) behaviour of the defendant to the level of collaboration with the national supervisory authority. Additionally, in order to ensure consistency and coordination across MS, article 70 GDPR includes among the tasks of the European Data Protection Board (the former article 29 Working Party) the possibility to draft guidelines concerning administrative fines.

---

8 Article 28 provides that MS shall ensure that national supervisory authorities shall have investigative powers, legal standing before courts, and effective powers of intervention, but with no specific reference to the power to impose fines or sanctions.

9 Article 22 on remedies provided that:

“Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall 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.”

10 Article 83 (2) includes the following criteria:

“(a) 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;
(b) the intentional or negligent character of the infringement;
(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
(e) any relevant previous infringements by the controller or processor;
(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
(g) the categories of personal data affected by the infringement;
(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.”
defined in article 83.

On the one hand, the GDPR aims to provide a solution to the perception emerging from several studies that there is a lack of effective remedies in data protection;\(^{11}\) on the other, it follows the steps of the Commission’s practice of administrative fines in Competition Law under article 23 paragraph 2 a) of Council Regulation (EC) No 1/2003, enhancing the coordination and harmonisation of sanctions across MS.

The modification of the institutional structure along the lines detailed by the GDPR will require several steps within each legal system, imposing a wider reframing of the institutional design between administrative and judicial enforcement. At the moment, almost all MS provide for two concurring enforcement mechanisms with partial overlap, giving scope for divergent results whereby national supervisory authorities may find a violation of data protection law, whereas the court may decide that the conduct is lawful. The preliminary references by national courts described in the following Chapters shows that forms and manners of coordination between administrative and judicial enforcement were already present in judicial discourse with the European courts, not only at national level but also in relation to transborder cases. In particular, the decision of the CJEU in case C-78/16 (see Chapter 4) addresses the compliance of a mandatory administrative procedure with effective judicial protection, whereas the decision in C-230/14 and the pending preliminary reference C-210/16 (see Chapter 2) focus on the powers of the national supervisory authorities in transborder cases.

The most challenging issues emerging are the following:

- Is a mandatory sequence between administrative and judicial proceedings compatible with the right to an effective remedy, and in particular with access to the courts?
  - If the answer is yes, what are the requirements for coordination between the administrative and judicial proceedings in order to guarantee effective judicial protection?
  - What is the impact of a specific institutional framework on the type of remedies available in each enforcement mechanism?
- What are the modes of coordination along the two dimensions of European-national level and administrative-judicial enforcement?
- What is the level of coordination among national supervisory authorities in case of transborder violation of data protection law?

**Individual and collective redress between judicial and administrative enforcement**

The GDPR provides for different possible enforcement mechanisms, involving both administrative and judicial proceedings.

**Under article 77 GDPR**, the data subject may claim breach of data protection before the supervisory authority where he or she has habitual residence, of the place of work or place of the alleged

infringement if the data subject considers that the processing of their personal data infringes the GDPR. In case of breach, the supervisory authority may impose several corrective measures on the data controller (see article, 58 GDPR), and, as said above, it may also impose administrative fines pursuant to article 83 GDPR. The specific amount of the fine will be determined by the Supervisory Authorities on a case-by-case basis and follow the principles of effectiveness, proportionality and dissuasiveness in each individual case.

Under article 78 GDPR, the data subject (and also the data controller) may appeal against a decision of the supervisory authority before the court where the supervisory authority is established. The right to an effective remedy also covers cases where the supervisory authority does not handle a complaint or does not inform the data subject within 3 months about the progress or outcome of their complaint. In this case, the court will exercise full jurisdiction, which should include its competence to examine all questions of fact and law relevant to the dispute before it.

Finally, under article 79 GDPR, the data subject may also claim breach of data protection provisions before the court where the controller/processor has an establishment or, alternatively, where the data subject has their habitual residence.

It should be noted that, pursuant to article 80 GDPR, the data subject can exercise their rights also by mandating a not-for-profit body, organisation or association, which will select the judicial or administrative enforcement mechanism. Although this provision does not explicitly provide for collective redress, it may trigger increased involvement by organisations or associations in collecting and coordinating claims by data subjects. This could increase the protection of data subjects, as the incentives to enforce individual rights may be higher where the intermediation of organizations allows for lower costs of litigation.

Given the lack of detailed indications in the GDPR, the MS will have discretion regarding the possibility of allowing coordinated claims before supervisory authorities and courts. In order to adapt the national framework and ensure effective application of the regulation two options are available: the legislation might identify existing national procedural rules that will be applicable to data protection (for instance extending the rules applicable to collective remedies, if any, to data protection), or introduce new rules covering data protection clarifying the effects of the decision (e.g. whether it is erga omnes or only binding on the parties to the claim), the coordination between individual and collective actions, and also the coordination between claims before the Data Protection authorities and national courts.

Even before that happens, the jurisprudence included in this Casebook includes cases where the national courts have already been confronted with questions related to aggregation of claims for breaches of data protection. In particular, the decisions of the CJEU in case C-194/16 (see Chapter 2) and case C-498/16 (see Chapter 6), and the pending preliminary reference C-40/17 (see Chapter 6), address the problem of jurisdiction in cases of multiple claims coming from different MS and thus (potentially) subject to different rules of jurisdiction depending on the type of claim.

---

12 Note that in the French legal system, the so called actions de groupe – which emerged in the consumer protection area - may also address claims by individuals in similar situations suffering from damage that results from a breach of statutory obligations by data controllers or subcontractors. Such collective actions may be filed before civil or administrative courts by (i) associations that have been exercising their statutory activities in the field of privacy and data protection for at least five years, (ii) accredited consumer associations that are representative at national level (if data processing affects consumers’ interests); or (iii) trade unions (if data processing affects employees or civil servants’ interests). Proceeding can be instituted only to request the court to order the cessation of the unlawful practices. See Law no. 2016-1547 of November 2016 on the Modernisation of Justice (Loi de modernisation de la justice du 21e siècle).
The current issues emerging are the following:

1. Is it possible to aggregate claims by different data subjects from different countries of data protection breaches based on the same conduct, (ie against the same defendant)?
   ○ Is there a difference where the data subjects are all located in single MS?

2. Is it possible to aggregate claims of data protection breaches made by a single data subject suffering damage in different countries based on the same conduct (ie against the same defendant)?

3. What are the effects of judicial remedies in the case of transborder aggregate claims (eg. may an injunction from a French court have effect in Poland)?

4. Is there a difference between the rules on aggregation of claims before the national supervisory authority and before judicial courts?

5. Is there a difference between the effects of remedies ordered by national supervisory authorities and those ordered by national courts in case of transborder aggregate claims?

6. What is the interplay between national supervisory authorities and courts from different MS in the case of transborder aggregate claims (eg. is it possible for a decision of the French CNIL to be used to claim damages before an Italian court?)
1. Impact of the Charter on the territorial scope of data protection

1.1. Introduction

Extraterritoriality is, at the moment, the subject of important debates in the field of data protection. Within the European Union, since 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. This chapter will analyse, in section 1.1., 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. In the future, the perspective of harmonization through the GDPR, which includes new provisions on the territorial scope of the protection, might bring 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 European Union 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 again, the Charter has been, for the CJEU, an essential instrument 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 questions addressed

1. (a) & (b): In the light of the principle of effectiveness, within the European Union, how should the concept be defined of data processing “carried out in the context of the activities of an establishment of the controller on the territory of” a Member State, which constitute the relevant criteria for defining the territorial scope of the law of that Member State implementing Directive 95/46?

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 on the territory of that Member State?

3. (a) Can a national data protection authority exercise the powers conferred upon it by its national law transposing Directive 95/46 against a data controller, when the data controller carries out its activities, fully or in part, on the territory of another Member State or a third country? If not, does the principle of effective access to justice impose a duty of cooperation between Member States’ supervisory authorities?

(b) Where different MS 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 MS where the entity mainly responsible for the processing is established have any priority or supremacy over other MS 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. In the relationships between online service providers and their customers concerning the processing of data, are the rules on international jurisdiction in consumer protection applicable?
Question 1: - Interpretation of the connecting factor defining the territorial scope of a Member State’s law on data protection

1 (a) & (b): In the light of the principle of effectiveness, within the European Union, how should the concept be defined of data processing “carried out in the context of the activities of an establishment of the controller on the territory of” a Member State, which constitute the relevant criteria for defining the territorial scope of the law of that Member State implementing Directive 95/46?

Question 1(a): For the determination of the territorial scope/applicability of a MS law on data protection, in the light of the principle of effectiveness, how should the concept of processing of data “carried out in the context of the activities of an establishment of the controller on the territory of that MS” be defined within the meaning of article 4 (1) (a) of Directive 95/46?

Question 1(b): For the determination of the territorial scope/applicability of a MS law on data protection, in the light of the principle of effectiveness, how should the “use of equipment, automated or otherwise, situated on the territory of the said Member State” be defined within the meaning of article 4 (1) (c) of Directive 95/46?

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 (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 (Holstein)

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)
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 – National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

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

Recital (10), (18), (19) and (20)

Recital (10): “... the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognised both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms [, signed in Rome on 4 November 1950,] and in the general principles of Community law; ... for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community”.

Recital (18): “… in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; … in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State”.

21
Recital (19): “… establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; … the legal form of such an establishment, whether simply [a] branch or a subsidiary with a legal personality, is not the determining factor in this respect; … when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities”.

Recital (20): “… the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; … in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice”.

The case(s):

In all referral cases, the general pattern is the same. 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 in the Member State where the data subject is domiciled, a branch or subsidiary 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 (Holstein GmbH, 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 on 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 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 in that Member State an office or subsidiary 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 to the parent company, located outside the European Union, requests and requirements addressed to it both 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 the light of Article 8 of the [Charter]? 

- In _Weltimmo_, in 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, in 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 Holstein, in circumstances where a parent company based outside the European Union (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 European Union and hence in the first Member State as well, 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, although not expressly referring to article 47 of the Charter, the Court relies on the principle of effectiveness to underline that given the objective of ensuring an effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, the words “carried out in the context of the activities” of an establishment cannot be interpreted restrictively.

The Court states that it is clear, from the EU legislation on data protection, that the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive, and to prevent that protection from being circumvented, by prescribing a particularly broad territorial scope.

Consequently, the Court decides that the processing of data is carried out ‘in the context of the activities’ of an establishment in a Member State even if it is “only” intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable, given that “the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed”. The fact that the display of results is accompanied, on the same page, by the display of advertising linked to the search terms, proves that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller’s establishment on the territory of a Member State, in this instance Spanish territory.

The Court concludes that in such circumstances, it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive’s effectiveness and the effective and complete protection of the fundamental rights and freedoms of
natural persons which the directive seeks to ensure, in particular their right to privacy, with respect to the processing of personal data, a right to which the directive accords special importance.

On the question related to the localization 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 on the territory of a Member State, within the meaning of within the meaning of article 4 (1) (a) of Directive 95/46:

- when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State (Google Spain),

- the controller exercises, through stable arrangements in the territory of a Member State, a real and effective activity — even a minimal one — in the context of which that processing is carried out. In order to ascertain whether that is the case, the referring court may, in particular, take account of the fact (i) that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State’s language and that it is, as a consequence, mainly or entirely directed at that Member State, 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).

Impact on the follow-up case:
Not available yet.

Elements of judicial dialogue:

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

In Weltimmo, the Court elaborates on the reasoning in Google Spain, to state that the concept of ‘establishment’ should be given a flexible definition, which departs 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 the
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, suffice 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, extends 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’ extends to any real and effective activity, even a minimal one, exercised through stable arrangements, such an establishment cannot exist in a Member State merely because the undertaking’s website is accessible there.

In Holstein, 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 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.

Possible further evolution in the light of the new GDPR:

With the GDPR, whose provisions are directly applicable in Member States, the issue of the territorial scope of Member States’ laws on data protection within the European Union should vanish. The same EU rules will apply everywhere on EU territory. But new issues will certainly arise, and might bring further interest in the Charter. We know for sure, 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 Charter of Fundamental Rights 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 nor established in the Union”. However, the reach 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.

It is certain that the implementation of these criteria will raise issues that will be referred to the CJEU, and the Charter will most certainly be a useful tool to solve these issues.

Impact on national case law in MS 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)
The Italian judge, 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, recalls the domestic and European laws as well as the European case law applicable in the case. Directive 95/46/CE, read in the 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 on the territory of that Member State.
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”. Having 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.
Question 2 & 3: 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 (Holstein)

Within this cluster, identification of the main cases 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 (Holstein)

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)

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

…

3. Each authority shall in particular be endowed with:

– investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

– effective powers of intervention, such as, for example, that of delivering opinions before
processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

– 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.

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

…

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

**Question 2 – The competence of Member States’ data protection authorities in cross-border situations**

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 on 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 the Hungarian Law on information, and imposed on that company a fine of approximately EUR 32 000.

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 pronounces 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 on the territory of another Member State. The Court judges 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, the Court, 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, **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).

**Impact on the follow-up case:**
Not available yet

**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 *Holstein*, 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 MS 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 on 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.”

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

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

Question 3. a) Can a national data protection authority exercise the powers conferred upon it by its national law transposing Directive 95/46 against a data controller, when the data controller carries out its activities, fully or in part, on 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?

Question 3. b) Where different MS 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 MS where the entity mainly responsible for the processing is established have any priority or supremacy over other MS data protection authorities, to decide on the lawfulness of the processing?

**3. a) – Duty of cooperation between MS Data protection authorities**

3. a) Can a national data protection authority exercise the powers conferred upon it by its national law transposing Directive 95/46 against a data controller, when the data controller carries out its activities, fully or in part, on the territory of another Member State? If not, does the principle of effective access to justice impose a duty to cooperation between Member States’ supervisory authorities?

*The case(s):*

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 were 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 penalize 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 on the territory of its own Member State in order to ensure, on 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.

**Impact on the follow-up case:**
Not available yet.

**Elements of judicial dialogue:**

In *Schrems I*, the Court considers, as regards 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 on a non-exhaustive basis 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 on 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 *Holstein*, 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 MS’ 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 MS 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 European Union.

**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.
2. 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.
3. 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.
4. 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.
5. 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.
6. Requested supervisory authorities shall, as a rule, supply the information requested by other supervisory authorities by electronic means, using a standardised format.
7. 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.
8. 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 on 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).
9. 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”. In this regard, article 60 (1) to (3) reads:

“All. 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.”

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

Not available yet.
3. b) - Absence of hierarchy between MS data protection authorities exercising competence over the same data processing

3. b) Where different MS 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 MS where the entity mainly responsible for the processing is established have any priority or supremacy over other MS 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 (Holstein)

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: quoted above
Article 28: quoted above

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 to 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 to 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?

It 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 to, 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 European Union (see above question 3.a.), the CJEU deals with the
issue of the concurring competence of several MS 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 Charter of Fundamental Rights of the European Union 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 Charter of Fundamental Rights 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 European Union has its seat in another Member State: there is no hierarchy between MS 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.

Impact of the follow-up case

Not available yet.

Elements of judicial dialogue

-Horizontal: Weltimmo and Schrems I are reference decisions on which the Court builds this new
Impact on national case law in MS different from the state of the court referring the preliminary question to the CJEU

Not available yet

Input of the GDPR

In the future, the solution adopted in Holstein must be read in the 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 MS 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 MS, is not assessed differently in each MS 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 Holstein, 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”.

rule.
Questions 4 & 5: Coordination between national courts regarding intra-EU cross-border 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?

Relevant CJEU decision

➢ 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)

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)

Relevant legal sources:

EU level


Recitals 15 and 16:

‘(15) The rules of jurisdiction should be highly predictable and founded on the principle that jurisdiction is generally based on the defendant’s domicile. Jurisdiction should always be available on this ground save in a few well-defined situations in which the subject matter of the dispute or the autonomy of the parties warrants a different connecting factor. The domicile of a legal person must be defined autonomously so as to make the common rules more transparent and avoid conflicts of jurisdiction.

(16) In addition to the defendant’s domicile, there should be alternative grounds of jurisdiction based on a close connection between the court and the action or in order to facilitate the sound administration of justice. The existence of a close connection should ensure legal certainty and avoid the possibility of the defendant being sued in a court of a Member State which he could not reasonably have foreseen. This is important, particularly in disputes concerning non-contractual obligations arising out of violations of privacy and rights relating to personality, including defamation.’
**Article 7 (2)**

‘A person domiciled in a Member State may be sued in another Member State:

(2) in matters relating to tort, delict or quasi-delict, in the courts for the place where the harmful event occurred or may occur…”

**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 appearing there, to pay Bolagsupplysningen the amount of EUR 56,634.99 as compensation for harm sustained 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 of 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 he or she 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 localization 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 his 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 its commercial reputation is most firmly established and must, therefore, be determined by reference to the place where it carries out the main part of its economic activities. While the centre of interests of a legal person may coincide with the place of its registered office when it carries out all or the main part of its activities in the Member State in which that office is situated and the reputation that it enjoys 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 his personal 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 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 consider separately 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 he may sue, with the defendant’s interest in reasonably foreseeing which court he 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 his personal 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 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.
Impact on the follow-up case:
Not available (case too recent).

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.

Impact on national case law in MS different from the state of the court referring the preliminary question to the CJEU:
Not available.

Input of the GDPR on the jurisdiction of courts:

The GDPR, which institutes 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 his claim before the courts of the Member State of his 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 the light of Recital 147 of the Preamble of the GDPR:

“Where specific rules on jurisdiction are contained in this Regulation, in particular as regards 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.

5. In the relationships between online service providers and their customers concerning the processing of data, are the rules on international jurisdiction in consumer protection applicable?

2.a - More specifically, are choice-of-forum clauses included in the service providers’ general terms and conditions applicable?

2.b - More specifically, can a consumer taking action, on the basis of Regulation 44/2001 (Brussels I revised), in the Member State where he is domiciled, also invoke at the same time as his own claims and before the same courts the claims of other consumers on the same subject, such consumers being domiciled in different Member States or in non-member States?

See the discussion in Chapter 6, question 6
1.3. Relations with third countries

Directive 95/46 dedicates 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 on its territory. However, the intangible nature of data is not strictly compatible with an approach relying on purely 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” (August 2016). And in the meantime, the CJEU has had to provide safeguards for EU citizens, using in particular the rights enshrined in the Charter.

Main question addressed:

1. Should Member States’ data protection authorities assess the adequacy of data protection in third countries, where personal data gathered in the European Union is to be transferred, in terms of European Union principles and/or legislation?

2. Should they find that the data protection offered in a third country is not adequate, should Member States oppose the transfer of personal data gathered in the European Union to that country?

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

1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of
2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

(…) 

4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.

6. The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. 

Member States shall take the measures necessary to comply with the Commission’s decision.

**Article 28 - Supervisory authority**

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals’ rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

   – investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
   
   – effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction
of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,

– 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.

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

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

(…)

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

**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.

**National Level**

**Irish Data Protection Act 1988**

**Irish Constitution**

*Articles 40 (personal rights, including the right to privacy) and 41 (protection of family life)*
Question 6 & 7: The scrutiny of third countries’ legislation in terms of EU law and its consequences

6. Should Member States’ data protection authorities assess the adequacy of data protection in third countries, where personal data gathered in the European Union is to be transferred, in terms of European Union principles and/or legislation?

7. Should they find that the data protection offered in a third country is not adequate, should Member States oppose the transfer of personal data gathered in the European Union 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 European Union, at the time he registered on Facebook, each user had to conclude a contract with Facebook Ireland, a subsidiary of Facebook Inc., which is itself 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 EU Charter of Fundamental Rights 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 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:

The Court reaffirms the role of national supervisory authorities in the 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, observes the Court in an implicit application of the principle of effectiveness, 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 scrutinized according to EU standards.

The Court then engages in an analysis to define which authority within the European Union 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, the Court first of all observes that compliance with the safe harbor 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 European Union to 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, from the assessment made by the Court or by national authorities and/or courts, that the level of protection in a third country is not sufficient, Member State 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 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 Commission Decision 2000/520 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 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 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.

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:


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, among others, the national supervisory authorities and the European Parliament, 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 Holstein (C-210/16), for the ruling on the independence of MS 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 protection of data (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).
2. Impact of the Charter on the material scope of data protection

2.1. Introduction

The material scope of EU data protection was defined, at least until the coming into force of the GDPR in May 2018, 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”. However, article 3 (2) limits the material scope of the protection by expressly excluding its application to the processing of personal data realized: (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 European Union 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”.

This Chapter will analyze in section 2.1 how the CJEU has, based on the Charter and/or of the principles of effectiveness and proportionality, interpreted article 3 to define the general scope of the protection. Section 2.2 will focus on the important exception to the scope of the protection of personal data, applying to processing operations concerning public security, defence and State security, considering the safeguards imposed by the CJEU on the basis of the Charter. Ultimately, each section puts in perspective the developments that might be expected with the coming into force of the GDPR, although the GDPR does not seem to introduce major changes as far as the material scope of the directive is concerned.
2.2. The general scope of data protection

Notwithstanding the definitions, enshrined in article 2 of the Directive, of concepts such as ‘personal data’, ‘processing’, or ‘data subject’ – concepts important for the delimitation of the scope of the protection, questions and disputes have arisen regarding the precise meaning of such concepts. When asked for preliminary rulings, the CJEU has progressively refined these definitions. This section analyses how the Court has carried out this task of interpretation, and to what extent the Charter has been a tool for fulfilling this task.

Main questions addressed:

1. (a) In the light of the principle of effectiveness of data protection, how should the concept of “processing of personal data” be interpreted within the meaning of article 2 (b) of Directive 95/46?
   (b) In the light of the principle of effectiveness of data protection, how should the limits to the scope of the protection be implemented, as defined in article 3 (2) of Directive 95/46?

2. In the light of the principle of effectiveness of data protection, how should the concept of “personal data” be interpreted within the meaning of article 2 of Directive 95/46?

3. In the light of the principle of effectiveness of data protection, how should the concept of “controller” of the processing of personal data be interpreted within the meaning of article 2 of Directive 95/46?

4. In the light of the principle of effectiveness of data protection, how should the concept of “data subject” be interpreted within the meaning of article 2 of Directive 95/46?

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 Markkinapörssy Oy, Satamedia Oy, Case C-73/07 (Satamedia)
➢ Judgment of the Court, 20 May 2003, Österreicher Rundfunk, Case C-465/00, C-138/01 et C-139/01 (Österreicher Rundfunk)
➢ Judgment of the Court (Grand Chamber), 16 December 2008, Heinz Huber v. Bundesrepublik Deutschland, Case C-524/06 (Heinz Huber)
➢ 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, Worten – 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, 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, 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 (Second Chamber), 19 October 2016, Patrick Breyer v. Bundesrepublik Deutschland, Case C-582/14 (Breyer)

➢ Opinion of the Court, (Grand Chamber), 26 July 2017, Opinion 1/15 (PNR Canada)

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

➢ 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 (Holstein)

➢ Request for a preliminary ruling from 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), 10 July 2018, Tietosuojavaltuutettu / Jehovan todistajat — uskonnollinen yhdyskunta, Case C-25/17 (Jehovan)

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

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or
combination, blocking, erasure or destruction;

(c) …

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean 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.

Article 3 - Scope

1. 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.

2. This Directive shall not apply to the processing of personal data:

   - 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 European Union 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,

   - by a natural person in the course of a purely personal or household activity.
Question 1 (a) and 1 (b) – Definition of the concept of “processing” of personal data

1. (a) In the light of the principle of effectiveness of data protection, how should the concept of “processing of personal data” be interpreted within the meaning of article 2 (b) of Directive 95/46?

1. (b) In the light of the principle of effectiveness of data protection, how should the limits to the scope of the protection be implemented, as defined in article 3 (2) of Directive 95/46?

Cluster of CJEU cases, particularly relevant with respect to question 1

➢ 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, 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, 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), 10 July 2018, Tietosuojavaltuutettu / Jehovan todistajat — uskonnollinen yhdyskunta, Case C-25/17 (Jehovan)

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)

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 2 and article 3 (see full quotation above)

In particular article 2 (b): “processing of personal data' ('processing') shall mean any
operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction”

Article 25 'Transfer of personal data to third countries' (see quotation in Chapter 1, under questions 6 & 7)

National level
Personuppgiftslag (SFS1998:204) (Swedish law on personal data, 'the PUL')

The case(s):

Mrs. Lindqvist was charged with breach of the Swedish legislation on the protection of personal data for publishing on her internet website personal data (such as names, phone numbers, jobs and hobbies, and in one case health information) on a number of people working with her on a voluntary basis in a parish of the Swedish Protestant Church. 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 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 authorization (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 stay 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, the facts and issues were quite similar with regard to the question here considered. A data controller alleged that its activity could not be regarded as “processing of data” within the meaning of Directive 95/46 since it did not strictly fall under the directive’s definition. 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*, 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*, 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.

**Preliminary question(s) referred to the Court:**

In *Lindqvist*, the Court was asked several questions related to the scope of the directive and the concept of “processing of data”:

(1) Is the mention of a person — by name or with name and telephone number — on an internet home page an action which falls within the scope of [Directive 95/46]? Does it constitute “the processing of personal data wholly or partly by automatic means” to list on a self-made internet home page a number of persons with comments and statements about their jobs and hobbies etc.?

(2) If the answer to the first question is no, can the act of setting up on an internet home page separate pages for about 15 people with links between the pages which make it possible to search by first name be considered to constitute “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” within the meaning of Article 3(1)?

(3) Can the act of loading information of the type described about work colleagues onto a private home page which is none the less accessible to anyone who knows its address be regarded as outside the scope of [Directive 95/46] on the ground that it is covered by one of the exceptions in Article 3(2)?

(5) [Directive 95/46] prohibits the transfer of personal data to third countries in certain cases. If a person in Sweden uses a computer to load personal data onto a home page stored on a server in Sweden — with the result that personal data become accessible to people in third countries — does that constitute a transfer of data to a third country within the meaning of the directive? Would the answer be the same even if, as far as known, no one from the third country had in fact accessed the data or if the server in question was actually physically in a third country?
(7) Can a Member State, as regards the issues raised in the above questions, provide more extensive protection for personal data or give it a wider scope than the directive, even if none of the circumstances described in Article 13 exists?

In all the other cases referred, the Court was asked, in substance, the same general question: whether article 2(b) of Directive 95/46 is to be interpreted as meaning that the activities considered in the case must be classified as ‘processing of personal data’ within the meaning of that provision and, consequently, fall within the scope of application of the directive.

**Reasoning of the Court:**

Although not expressly referring to article 47 of the Charter or to the principle of effectiveness, the Court obviously relies implicitly on the principle of effectiveness to endorse a broad conception of the general scope of the directive. It is important to stress that the Court endorses a two-step reasoning. Firstly, it focuses on the “positive” material scope of the directive in the light of article 3 (1); and secondly, it verifies whether the disputed processing falls under the activities not covered by the protection, pursuant to article 3 (2) of the directive. In the latter case, the data subject would not be able to claim the protection awarded by the directive and/or national law.

**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, as regards 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* and *Ryneš*, 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, the Court observes, first, 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.
4. 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.

6. Measures taken by the Member States to ensure the protection of personal data must be consistent both with the provisions of Directive 95/46 and with its objective of maintaining a balance between freedom of movement of personal data and the protection of private life. However, nothing prevents a Member State from extending the scope of the national legislation implementing the provisions of Directive 95/46 to areas not included in the scope thereof provided that no other provision of Community law precludes it.

**Impact on the follow-up case:**
Not available yet.

**Elements of judicial dialogue:**

-**Horizontal dialogue:**

  **Lindqvist, Satamedia, Google Spain, Rynes, and Weltimmo** include numerous cross-references.

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.
**Perspectives in the light of the coming into force of the GDPR:**

**General analysis of the material scope of the Regulation**

Article 2 of the Regulation, titled “Material scope”, defines the scope of the Regulation in its first paragraph as follows:

“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”.

This provision is identical to article 3(1) of Directive 95/46, which means that the Regulation should not bring about major changes in the scope of the Regulation.

However, it might be asked whether some of the Recitals of the Preamble shed new light on the scope of the protection. That could be the case, in particular, with Recitals (1) to (4), as well as Recital (14).

**Specific analysis on the concept of “processing”**

Concerning, specifically, the concept of “processing” of personal data, article 4(2) provides for the following definition:

‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”.

That definition is very much in line with the one available in Directive 95/46, with the result that CJEU case law should be transposable for the interpretation of the Regulation.

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

Not available yet.
Question 2 – Definition of the concept of “personal data”

2. In the light of the principle of effectiveness of data protection, how should the concept of “personal data” be interpreted within the meaning of article 2 of Directive 95/46?

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. Satammin 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, Worten – 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, 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, Peter Nowak v Data Protection Commissioner, Case C-434/16 (Nowak)

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)

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

Recital 26

‘Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, 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; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible.’

Article 2 & Article 3 (see full quotation above)

In particular article 2 (a): ‘“personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

National level

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

Paragraph 3(1)

‘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’),

Paragraph 12:

‘(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:

‘(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 logfiles.

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 abovementioned 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 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 may qualify as “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*, 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* and *Satamedia*, 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.

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?

**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 the 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 gather 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 the 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 transmit directly to the online media services provider the additional data necessary for the identification of the data subject, it seems however, 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 her 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:**
Not available yet.

**Elements of judicial dialogue:**

- Horizontal (within the CJEU):
  See above the complementarity between the cases.

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 be 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 him or her as a person, since:

1) it reflects the extent of the candidate’s knowledge and competence in a given field and, in some cases, his intellect as well as, eventually, information as to his handwriting;
2) the purpose of collecting those answers is to evaluate the candidate’s professional abilities and his suitability to practice the profession concerned;
3) the use of that information, one consequence of that use being the candidate’s success or failure in the examination concerned, is liable to have an effect on his or her rights and interests, in that it may determine or influence, for example, the chance of entering the profession aspired to or of obtaining the post sought.

The comments of an examiner with respect to the candidate’s answers also constitute information relating to that candidate 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 his private life, in being able to object to the processing of the answers submitted by
him 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, Salvatore Manni, C-698/15).

_Perspectives in the light of the coming into force of the GDPR:_

**For a general analysis, see above under question 1**

Specifically concerning the concept of “personal data”, article 4(1) provides the following definition:

> ‘any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person’.

That provision is to be read in the light of Recital 26 of the GDPR:

> ‘The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.’

Here again, if the Regulation adds some precision to the definition in its Preamble, that definition is very much in line with the one available in Directive 95/46, with the result that CJEU case law should be transposable for the interpretation of the Regulation.

**Impact on national case law in MS different from the state of the court referring the preliminary question to the CJEU:** Not available yet.
Question 3: Definition of the concept of “controller”

3. In the light of the principle of effectiveness of data protection, how should the concept of “controller” of the processing of personal data be interpreted within the meaning of article 2 of Directive 95/46?

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

➢ Request for a preliminary ruling from 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), 10 July 2018, Tietosuojavaltuutettu / Jehovan todistajat — uskonnollinen yhdyskunta, Case C-25/17 (Jehovan)

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), 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: 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 2 (d) and article 3 (see quotation above)

Particularly article 2 (d), under which “'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law”.
National level

Spanish Organic Law n°15/1999, 13 December 1999, on the protection of personal data
(transposing directive 95/46)

The case(s):

A Spanish national resident in Spain lodged with the AEPD (Spanish data protection supervisory authority) a complaint against a Spanish publisher and against Google Spain and Google Inc., 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 1 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 stay 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:

The referring court seeks 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.
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. Analyzing the concrete role played by the operator of a search engine, the Court observes, firstly, 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 the activity of a search engine thus affects significantly, and additionally compared to that of web publishers, 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 irrelevant the fact that publishers of websites have the option of indicating to operators of search engines that they wish information published on their site to be excluded from the search engines’ indexes, 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 ‘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 6, under question 1.

Elements of judicial dialogue:

Several requests for preliminary rulings have been referred to the Court since Google Spain, concerning the concept of ‘controller’ within the meaning of the directive.

In Holstein (C-210/16), the question referred to the Court was the following: Is article 2(d) of Directive 95/46 to be interpreted as definitively and exhaustively defining the liability and responsibility for data protection violations, or does scope remain, under the ‘suitable measures’
pursuant to article 24 of Directive 95/46/EC and the ‘effective powers of intervention’ pursuant to the second indent of article 28(3) of Directive 95/46/EC, in multi-tiered information provider relationships, for responsibility of a body that does not control the data processing within the meaning of article 2(d) of Directive 95/46/EC when it chooses the operator of its information offering?

In *Fashion ID* (C-40/17), the question referred to the Court is (1) whether the person embedding a programming code in his website which causes the user’s browser to request content from a third party and, to this end, transmits personal data to the third party, is a ‘controller’ within the meaning of the directive, if that person is himself 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.

In *Jehovan* (C-25/17), the question referred to the Court was whether article 2(d) of Directive 95/46, read in the 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.

The decisions of the Court in *Holstein* and *Jehovan* provide some perspective on the concept of ‘joint control’ over data processing, and contribute to the broad interpretation of the concept of ‘controller’. In both cases, several actors were said to be contributing, in different proportions, to one and the same processing of data. One of these actors argued that its involvement in the process was too limited, and that it could not be considered as a processor or a controller. 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’. 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.
Perspectives in the light of the coming into force of the GDPR:

For a general analysis, see above under question 1

Concerning, specifically, the concept of “controller”, article 4 (7) provides the following definition:

“The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law”.

Once again, that definition is very much in line with the one in Directive 95/46, with the result that CJEU case law should be transposable for the interpretation of the Regulation.

However, as already observed in Chapter 1, the Regulation extends the scope of the protection, since it expressly regulates the activities of both controllers and processors. The concept of “processor” is defined by article 4 (8):

“A natural or legal person, public authority, agency or other body which processes personal data on behalf of the 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’ in Holstein and Jehovah.

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

Not available yet.
Question 4 - Definition of the concept of “data subject”

4. In the light of the principle of effectiveness of data protection, how should the concept of “data subject” be interpreted within the meaning of article 2 of Directive 95/46?

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 related rather to the question of who, precisely, 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. National case law emphasizes 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.

An illustration based on national case law:

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

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 2 (a)

“personal data’ shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

National level

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(s):

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, by his mother’s insurance company, proper access to data concerning her 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 as regard personal data related to the person exercising the right. Successors and assigns 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 concludes 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 recognize 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.
2.3. 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

The first subparagraph of Article 3 (2) states 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”. In 2006, a directive was adopted in order to specifically authorize the retention of data for security purposes (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).

But the right to data protection is not only provided by EU secondary legislation. It is also enshrined in the Charter of Fundamental Rights. Even if the former includes an exception to the protection of data for State security matters, the latter generalizes the scope of the protection. Thus State security issues are 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 “State security”.

Question 5 – The extension of the protection of data in the field of State security matters

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

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 v. Tom Watson, Peter Brice, Geoffrey Lewis, (C-698/15), Joined cases (Tele2).

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

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)

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), first subparagraph:

“2. This Directive shall not apply to the processing of personal data:

- 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 European Union 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”.

Article 13(1) - Exemptions and restrictions

1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others.


Article 1 – Scope and aim

‘1. This Directive provides for the harmonisation of the national provisions required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.’;

2. The provisions of this Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

3. This Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the activities relate to State security matters) and the activities of the State in areas of criminal law.

Article 4 (1) & (2) – Security of processing

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

1a. Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:

— ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,

— protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,

— ensure the implementation of a security policy with respect to the processing of personal data,
Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve; 1b. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

**Article 5 (1) & (3)**

‘1. Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary or the conveyance of a communication without prejudice to the principle of confidentiality.

3. Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.’

**Article 6 (1)**

‘Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).’

**Article 15 (1)**

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


Recital 16, 21, 22

Article 1 to 9, 11 and 13 (selection of the most relevant quotations)

‘Article 1 (1) - Subject matter and scope

‘1. This Directive aims to harmonise Member States’ provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.’

Article 3 (1) - Obligation to retain data

‘1. By way of derogation from Articles 5, 6 and 9 of Directive 2002/58/EC, Member States shall adopt measures to ensure that the data specified in Article 5 of this Directive are retained in accordance with the provisions thereof, to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned.’

Article 5 – Categories of data to be retained

1. Member States shall ensure that the following categories of data are retained under this Directive:

   (a) data necessary to trace and identify the source of a communication:

      (1) concerning fixed network telephony and mobile telephony:

         (i) the calling telephone number;

         (ii) the name and address of the subscriber or registered user;

      (2) concerning Internet access, Internet e-mail and Internet telephony:

         (i) the user ID(s) allocated;

         (ii) the user ID and telephone number allocated to any communication entering the public telephone network;

         (iii) the name and address of the subscriber or registered user to whom an Internet Protocol
(IP) address, user ID or telephone number was allocated at the time of the communication;

(b) data necessary to identify the destination of a communication:

(1) concerning fixed network telephony and mobile telephony:

(i) the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s);

(2) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;

(ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;

(c) data necessary to identify the date, time and duration of a communication:

(1) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(2) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(d) data necessary to identify the type of communication:

(1) concerning fixed network telephony and mobile telephony: the telephone service used;

(2) concerning Internet e-mail and Internet telephony: the Internet service used;

(e) data necessary to identify users’ communication equipment or what purports to be their equipment:

(1) concerning fixed network telephony, the calling and called telephone numbers;

(2) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity (IMSI) of the calling party;

(iii) the International Mobile Equipment Identity (IMEI) of the calling party;

(iv) the IMSI of the called party;
(v) the IMEI of the called party;
(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;

3) concerning Internet access, Internet e-mail and Internet telephony:
(i) the calling telephone number for dial-up access;
(ii) the digital subscriber line (DSL) or other end point of the originator of the communication;
(f) data necessary to identify the location of mobile communication equipment:
(1) the location label (Cell ID) at the start of the communication;
(2) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

2. No data revealing the content of the communication may be retained pursuant to this Directive.

**Article 6 – Periods of retention**

‘Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.’

**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.


**The case(s):**

_Digital Rights Ireland Ltd_, the owner of a mobile phone registered on 3 June 2006, brought on 11 August 2006 an action claiming that the Irish authorities had unlawfully processed, retained and exercised control over data related to its communications. 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 the 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 stay 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 of the Charter of Fundamental Rights of the European Union (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:

The Court states, firstly, 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 constitutes in itself an interference with the rights guaranteed by 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 & 8 of the directive) to the data. This interference, because it is wide-ranging, must be considered to be particularly serious.

The Court examines, secondly, whether such interference may be justified in the 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, 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 recognizes 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 the 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, including, in particular, 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 the 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.

The Court adds, finally, that the directive does not require the data in question to be retained within the European Union, 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 the 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; the decision, besides, twice uses the expression “effective protection of the data” (§54, §66).

**Conclusion of the Court:**

Impact on the follow-up case:

In Austria, on 27 June 2014, in the light of the CJEU 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 this statutory changes. After the judgment delivered by the Court of Justice in 2014 that invalidated Directive 2006/24, Digital Rights Ireland sought an order referring to the Court of Justice of the European Union the 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”.13

In the EU, the invalidated directive has not been replaced.14

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 preliminary ruling from the Court.

The Tele2 case is one illustration: 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 the 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 i 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 i s 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, EU law allows, in certain situations, the retention of electronic communications data.

13 These parts are extracted and/or based at least partially on the database template drafted by Isabella Oldani.
14 These parts are extracted and/or based at least partially on the database template drafted by Isabella Oldani
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 the light of articles 7, 8 and 11 and article 52(1) of the Charter of Fundamental Rights of the European Union, must be interpreted as precluding national legislation which, for the purpose of fighting crime, provides for general and indiscriminate retention 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 the 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 European Union.

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 Charter of Fundamental Rights of the European Union (‘the Charter’), the Court answers that the infringement, although effective, is justified in the 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.

**Perspectives in the light of the coming into force of the GDPR:**

The GDPR maintains the exception to the application of the protection of data that was laid down by Directive 95/46. Article 2 (2) reads:

“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”.

At the same time, the GDPR underlines the relevance of fundamental rights of data subjects in data protection matters. Recital (2), notably, reads:

“The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons”.

Still, it confirms the limitation of the scope of the Regulation, in Recital (16):

“This Regulation does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of Union law, such as activities concerning national security. This Regulation does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the Union.”

Finally, Recital (4) seems to confirm the methodology implemented by the Court in *Digital Rights Ireland* in order to reconcile conflicting interests, such as the data subject’s right to privacy on the one hand, and State security interests on the other hand:

“The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its
function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity”.

**Impact on national case law in MS 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, on the basis of the elements communicated to it in a non-adversarial manner, if data related to the claimant is included in the registers, and if so, whether such an inclusion is justified, relevant and proportionate having 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.
3. Impact of the Charter on the assessment of the legitimacy of data processing

3.1 Introduction

The right to the protection of data, laid down by EU secondary legislation, may come into conflict with other legitimate interests. Directive 95/46 does not ignore this fact, and article 7 of the directive, entitled “Criteria for making data processing legitimate”, lists a series of situations where data processing might be legitimate, including where “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)”.

The fundamental rights of the data subjects, related to data protection, are particularly the right to privacy, protected by article 7 of the Charter, and the right to the protection of personal data, covered by article 8 of the Charter.

The CJEU had to engage in the balancing, on the one hand of the said fundamental rights of the data subject, and on the other of other legitimate interests or even conflicting fundamental rights such as freedom of expression or access to information. It has done so by relying on article 52 (1) of the Charter, which reads:

“1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.”

This chapter aims at presenting, in a summary form, how the CJEU has defined the methodology and the guidelines that are to be implemented by Member States’ authorities in a case-by-case analysis, in order to balance conflicting interests and resolve the conflict.

Main question addressed:

1. In the light of the principle of effectiveness and proportionality, to what extent may data subjects’ rights to the protection of private life and personal data (articles 7 and 8 of the Charter) be limited by Member States because they are in conflict with other legitimate private interests of the controller or a third party, including fundamental rights?

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)
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), 29 January 2008, Productores de Música de España (Promusicae) v. Telefónica de España SAU, Case C–275/06 (Promusicae)

Relevant legal sources:

EU level

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, 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

“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 8 (1) and (2) The processing of special categories of data

1. Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

2. Paragraph 1 shall not apply where:

(a) the data subject has given his explicit consent to the processing of those data, except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject’s giving his consent; or
(b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
(c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
(d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
(e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.

Article 13(1) [see quotation above under question 1]

Recital 2:

‘This Directive seeks to respect the fundamental rights and observes the principles recognised in particular by the Charter of fundamental rights of the European Union. In particular, this Directive seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter.’

Article 5(1) [see quotation above under question 1]

Article 6(1) [see quotation above under question 1]

Article 15(1) [see quotation above under question ]

Relevant national legal sources

N/A
Question 1: The balance between data subjects’ rights to the protection of privacy and personal data, and others legitimate private interests

1. In the light of the principle of effectiveness and proportionality, to what extent may data subjects’ rights to the protection of private life and personal data (articles 7 and 8 of the Charter) be limited by Member States because they are in conflict with other legitimate private interests of the controller or a third party, including fundamental rights?

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.

In other cases referred to the Court, similar questions have been raised as to the balance between data subjects’ rights and the legitimate interests of the controller or third party, and/or other fundamental rights or freedoms of the controller or third parties, such as, in particular:

- in Lindqvist, the balance with the freedom of expression of the data controller,
- in ASNEF and FECEMD, the balance with the free movement of personal data,
- in Scarlet Extended, the balance with the right to intellectual property of a third party requesting disclosure of the data (as in Promusicae),
- in Google Spain, the balance with the right of the public to access information, and the economic interest of the controller,
- in Ryneš, the balance with the right to the protection of the property, health and life of the data controller and their family,
- in Breyer, the balance with the (economic) interest of the controller in ensuring the continued functioning of the services,
- in *Salvatore Manni*, the balance with the interest of third parties and of the market in accessing information published in the companies’ register, related to the natural person assuming management functions in the companies,

- in *Rīgas satiksme*, the balance with the legitimate interest of a third party in disclosure of personal data of a person responsible for a road accident in order to exercise a legal claim.

**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 defense, 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:**

The Court considers that it should first be ascertained whether Directive 2002/58 precludes the Member States from laying down, with a view to ensuring effective protection of copyright, an obligation to communicate personal data which will enable the copyright holder to bring civil proceedings based on the existence of that right, since the communication of information that is stored by Telefónica constitutes the processing of personal data within the meaning of the first paragraph of article 2 of Directive 2002/58, read in conjunction with article 2(b) of Directive 95/46. If that is not the case, it will then have to be ascertained whether it follows from EU law that the Member States are required to lay down such an obligation.

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 more substantially the impact of fundamental rights enshrined in articles 17(2) and 47 of the Charter. 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 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 the light, particularly, of the CJEU decisions in Lindqvist, ASNEF and FECEMD, Google Spain and Rīgas 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. In Rīgas 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 balancing 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 the light of ASNEF and FECEM 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 the 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, when transposing those directives, Member States must take care to rely on an interpretation of them which allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.

**Impact on the follow-up case:**

Not available yet.

**Elements of judicial dialogue:**

- Horizontal (within the CJEU):
  - 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 the 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 *ASNEF and FECEMD*, the Court observes that article 7(f) of Directive 95/46 precludes any national rules which, in the absence of the data subject’s consent, impose requirements that are additional to the two cumulative conditions set out in article 7(f), that is to say (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 are disclosed; and, (2) that such interests must not be overridden by the fundamental rights and freedoms of the data subject. The Court thus concludes that article 7(f) of Directive 95/46 must be interpreted as precluding national rules which, in the absence of the data subject’s consent, and in order to allow such processing of that data subject’s personal data as is necessary to pursue a legitimate interest of the data controller or of the third party or parties to whom those data are disclosed, require not only that the fundamental rights and freedoms of the data subject be respected, but also that the said data should appear in public sources, thereby excluding, in a categorical and generalised way, any processing of data not appearing in such sources.

- 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 *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 obtain through the list of results 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 his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty. In the 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 Ryneš, the Court, after concluding that video-surveillance covering even partially 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 the 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 telemedium by the user concerned, and under which the purpose of ensuring the general operability of the telemedium cannot justify use of the data beyond that of the particular use of the telemedium. The Court recalls that, based on its previous decisions in ASNEF and FECEMD, (C-468/10 and C-469/10), 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. If German legislation were to be interpreted as authorising the collection and use of personal data relating to a user of those services, without his consent, only to the extent necessary to facilitate and charge for the specific use of online media by the user concerned, even though the objective of ensuring the general functional capacity of the online media may justify the use of such data at the end of that period of use of such media, this would have a more restrictive scope than the principle laid down in article 7(f) of Directive 95/46. Article 7(f) of that directive 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.

- In Salvatore 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 him 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 the pending request for a preliminary ruling in *Fashion ID*, an additional interesting question is asked, concerning the person whose legitimate interests are to be balanced with those of the data subject: “Whose ‘legitimate interests’ are the decisive ones in the balancing of interests to be undertaken pursuant to Article 7(f) of Directive 95/46/EC? Is it the interests in embedding third-party content or the interests of the third party?”

*Further evolution in the light of the new GDPR:*

As already mentioned, the methodology implemented by the Court is addressed in Recital 4 of the Regulation:

“The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity”.

One important question for the future, since the methodology can only be implemented on a case-by-case analysis, is whether it creates uncertainty incompatible with the objectives set out in
Recitals (9) and (10) of the Regulation.

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

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 legal 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 from the website storing its articles information contained in one of those 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 balancing of interests in the 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 balancing 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

The influence of the Google Spain decision on the 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 Court of Justice of the European Union 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.

15 Drafted by Gianmatteo Sabatino
16 See Court of Cassation decision no. 13161/2016; Milan Tribunale, decision of 5th October 2016; Rome Tribunale, decision of 3rd December 2015; Milan Tribunale, decision of 28th February 2017. On that issue, see also Rizzuti, Il diritto
Indeed, according to the guidelines, the CJEU decision set out the concept of “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”. On the basis of such grounds, intended as a further development of the balancing 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, by a lawyer, and by a member of a National Authority.

The passing of time, therefore, becomes only one of the several criteria to be considered when carrying out the balancing 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. 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. 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.

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 the first place, 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. 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 de-list. 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.

---

17 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.”

18 See Milan Tribunale, decision of 28th February 2017.

19 See Rome Tribunale, decision of 3rd December 2015.

20 See Milan Tribunale, decision of 5th 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.

21 See Milan Tribunale, decision no. 12623 of 4th 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.

22 See Court of Cassation, decision no. 13161/2016; Mantova Tribunale, decision of 28th October 2016.

23 See Court of Cassation, decision no. 19761/2017.

24 See NPDA decision no. 277 of 15th 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.

25 See Court of Cassation, decision no. 13151/2017; NPDA decision no. 618 of 18th December 2014.
information when dealing with claims not only of infringement of privacy but also damage to reputation. Notwithstanding this, 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 recognize how information published online is able to reach an otherwise unreachable number of people. Judges cannot ignore this circumstance and, as a consequence, have to adjust the criteria used to carry out the balancing of interests in order to ensure a high level of protection for data subjects.

---

26 See Cassino Tribunale, decision of 25th March 2014.
27 See Court of Cassation, decision no. 13161/2016; Court of Cassation, decision no. 13151/2017.
4. Effective Data protection between administrative and judicial enforcement.28

4.1. Introduction

To ensure the efficient protection of personal data, the European Union relies mainly on national supervisory authorities as mentioned in article 28 of Directive 95/46. The role of judicial enforcement should not, however, be underestimated, and the directive lays down the “right to a judicial remedy” of any person who has suffered damage as a result of an unlawful processing operation (articles 22 & 23). Still, the role of judicial enforcement seems to be quite different in the Member States. The coexistence of administrative enforcement, carried out by national supervisory authorities, and judicial enforcement, raises important issues such as that of the coordination of both types of proceedings. This chapter aims to identify these issues, and where they have been addressed by the CJEU, to assess the role played by the Charter and/or the principles of effectiveness, proportionality and dissuasiveness, in the decisions of the CJEU and of Member States’ authorities.

Main questions addressed:

1. 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?

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. 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?

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?

5. What are the powers of courts in their judicial review of administrative decisions?

6. Where the national systems envisage two alternative procedures, with violations of data protection law determined by national supervisory authorities and damages determined by the courts, are the courts bound by the administrative decisions in

28 Drafted by Federica Casarosa with the collaboration of Paola Iamiceli, Chiara Tea Antoniazzi, Gianmatteo Sabatin.
terms of (a) the existence of the violation; (b) the use and acquisition of (new) evidence; and (c) the type and content of the penalty? If they are not bound, what legal effect do administrative decisions have on judicial remedies?

Cluster of relevant CJEU cases

➢ 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), 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")

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.
Question 1 – The right to effective judicial remedy and the coordination of administrative and judicial enforcement

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?

The possible relationships between administrative and judicial enforcement on the basis of current legislation are the following:

a) **Alternative** (e.g. Italy). 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** (e.g. Slovakia, Ireland). 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** (France?). 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**

*Without prejudice* to any **administrative remedy** for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall 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.

*[See, for comparison, articles 77-79, 83(7-8), GDPR]*
National level

Slovak Constitution

Article 46

(1) Everyone may claim his or her rights through procedures laid down by law before an independent and impartial court or, in cases provided by law, before another public authority of the Slovak Republic.

(2) Any person who claims his or her rights have been denied by a decision of a public administrative body may go to court to have the legality of the decision reviewed, save where otherwise provided by law. The review of decisions in matters concerning fundamental rights and freedoms shall however not be excluded from the jurisdiction of the courts.

(3) Everyone shall have the right to compensation for damage caused by an unlawful decision of a court, another public authority or a public administrative body or by an improper official procedure.

(4) A law shall lay down the details and terms of the judicial and other legal protection.

Code of Civil Procedure (Slovak)

Article 20, Paragraph 250v(1) and (3)

1. Individuals or legal persons who claim that their rights or legally protected interests have been harmed by the unlawful action of a public authority, which does not constitute a decision, and that they were the direct addressee of that action or that its effects directly prejudiced them, may apply for protection against the action before a court, provided such action or its effects persist or may recur. […]

3. Legal proceedings shall be inadmissible unless the claimant has exhausted the remedies available to him under specific legislation.

The case(s):

Puškár is an individual person who presented a claim before the Supreme Court of the Slovak Republic asking that the Finance Directorate, all tax offices under its control and the Financial Administration Criminal Office be ordered to remove his name from a list, previously drawn up by the Finance Directorate, of people in directorship positions within companies. 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.

Mr. Puškár 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. Puškár (as well as the other two applicants) had
not exhausted the remedies before the national administrative authorities. Mr. Puškár then lodged an appeal with the Constitutional Court of the Slovak Republic.

The Slovak Constitutional Court focused mainly on the jurisprudence on article 6(1) ECHR in connection with article 46 of the Slovak Constitution. The Constitutional Court addressed in particular 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*).

In this way, 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.

In another case referred to the Court, a question about the underlying relationship between administrative and judicial enforcement has been raised, namely in *Rīgas satiksme*, concerning 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, rather it focused on the balancing 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).

**Preliminary questions referred to the Court:**

The Slovak Supreme Court presented four questions; for the purpose of this analysis, only the first and the fourth questions 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 CFR.

“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 scrutinized in the 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.

As regards 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.

As regards 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 (para. 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 claims

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 declares that the Slovak legal provisions do not as such infringe EU law, and only refers 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.

**Impact on the follow-up case:**

The case is very recent and there is no direct follow-up in Slovak case law so far.

**Elements of judicial dialogue:**

The CJEU decision 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.
Possible further evolution in the light of the new GDPR:

Several provisions of the GDPR are related to the issue in the box, although none can be considered as giving a definitive answer.

Article 58 (5) of the GDPR states that:

“5. Each Member State shall provide by law that its supervisory authority shall have the power to bring infringements of this Regulation to the attention of the judicial authorities and where appropriate, to commence or engage otherwise in legal proceedings, in order to enforce the provisions of this Regulation.”

Article 79 (1) of the GDPR deals with the right to an effective judicial remedy, and the parallelism between judicial and administrative enforcement:

“1. Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation”.

This provision imposes on Member States an obligation to offer a judicial channel to data subjects whose rights have been violated.

Article 81 (3) states:

“3. Where those proceedings are pending at first instance, any court other than the court first seized may also, on the application of one of the parties, decline jurisdiction if the court first seized has jurisdiction over the actions in question and its law permits the consolidation thereof”.

This provision questions the relations between parallel proceedings in one Member State.

Impact on national case law in MS other than the state of the court referring the preliminary question to the CJEU:

ITALY

Although not directly applying the decision in Puskar, 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). In decision no. 6775/2016, 7 April 2016, the Supreme Court (Labour law section) concluded that article 145 of the Italian Data Protection Code providing

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. Defense is an inviolable right at every stage and instance of legal proceedings. The poor are entitled by law to proper means for action or defense in all courts. The law shall define the conditions and forms of reparation in case of judicial errors.” (official translation)
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).

One application in the Italian context of the principles developed by the CJEU in Puskar could be in relation to article 146 of the Italian Data Protection Code, which provides that a claim before the Supervisory Authority may be filed only if an equivalent request has first been presented to the controller or processor and the request has been rejected or not answered within 15 days, unless this time limit could result in imminent and irreparable harm. The application of this provision in practice could be guided by the proportionality test applied in Puskar.
Question 2 – Interaction between the CJEU and the ECtHR

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?

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 the ECtHR and CJEU jurisprudence was mentioned in the Puskar 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 as regards 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 as regards the exercise of the right to an effective legal remedy in case of mandatory administrative proceedings in order to comply with articles 47 CFR 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).

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, the whole 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 as regards 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 Puskar decisions and may complement the latter.
Question 3 – Coordination between EU institutions and national authorities

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?

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)

“The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.

Member States shall take the measures necessary to comply with the Commission’s decision.”

The case and Preliminary question referred to the Court:

As presented above in Chapter 1 on territorial scope (under question 6 & 7), the Schrems case was a case where personal data of EU residents was transferred from EU to servers belonging to the US, where they were processed.

The High Court of Ireland, hearing the appeal against the decision of the Irish Commissioner for DP, 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 as regards the competence to verify the level of protection offered by third countries, the Court distinguishes two scenarios:
1. The lack of a specific decision of the Commission as regards the existence of an adequate level of protection of personal data.

2. The existence of a specific decision of the Commission as regards the existence of an adequate level of protection of personal data.

In the first scenario, pursuant to article 25(1), the MS 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.

In the second scenario, by contrast, the MS, 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 MS 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.

Possible further evolution in the light of the new GDPR:

The GDPR confirms that, pursuant to article 45, the Commission may adopt an “adequacy decision”, by which it recognises that a third country ensures an adequate level of protection, with the consequence that data might be transferred from the European Union to that country.

While article 46 of the GDPR describes what the role of national authorities shall be in the absence of a prior “adequacy decision” of the Commission pursuant to article 45, there is no provision dealing with the expected attitude of national authorities when such a decision exists, but is questionable.

The question may be asked whether the approach laid down by the CJEU in Schrems should still apply under the GDPR. But there seems, prima facie, to be no strong argument against the continuing application of the Schrems solution.
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?

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 28(3)

“3. Each authority shall in particular be endowed with:
– investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,
– effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
– 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.
Decisions by the supervisory authority which give rise to complaints may be appealed against through the courts.”

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 (see description of the case in Chapter 1 on territorial scope (questions 6 & 7), and above). 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 supervisory authority and court.

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.

124
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 read in the 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 must, pursuant to article 28(3) of Directive 95/46 read in the light in particular 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.

**Elements of judicial dialogue:**

Although no preliminary references are known on this specific point, the CJEU has clarified the duty of cooperation between the supervisory authorities and the national courts in case of doubts regarding the validity of an EU act in terms of fundamental rights and freedoms. According to the CJEU, only the CJEU itself may declare an EU act invalid, and only a national court may ask the CJEU to verify the validity of an EU act. In this sense, article 47 CFREU requires claimants who are not satisfied with the decisions of the supervisory authorities for reasons relating to the validity of an EU act to have access to courts in order to challenge such administrative decisions.

It is important to note that the CJEU has referred to article 47 CFREU only when addressing the judicial review of administrative decisions, whereas it has referred to article 8 CFREU when affirming the right of access to a court (i.e. CJEU) through the cooperation between the supervisory authorities and national courts.

**Impact on national case law in MS other than the state of the court referring the preliminary question to the CJEU:**

No impact evidenced so far.

---

30 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.”

31 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.”
Questions 5 & 6 – Interaction between national administrative and judicial proceedings

5. What are the powers of courts in their judicial review of administrative decisions?
6. Where the national systems envisage two alternative procedures, with violations of data protection law determined by national supervisory authorities and damages determined by the courts, are the courts bound by the administrative decisions in terms of (a) the existence of the violation; (b) the use and acquisition of (new) evidence; and (c) the type and content of the penalty? If they are not bound, what legal effect do administrative decisions have on judicial remedies?

According to article 24 of Directive 95/46, Member States are compelled to “lay down the sanctions to be imposed in case of infringement” of the data protection legislation. Supervisory authorities may (in most countries) impose several measures: issuing a warning or reprimand to the data processor/controller, ordering the suspension of the processing of personal data, blocking and erasure of specific data, or ordering pecuniary sanctions. In almost all countries, the national supervisory authorities have powers to impose sanctions, except for Belgium, Denmark, Finland and Ireland.

According to article 28(3) of Directive 95/46, then, decisions by the supervisory authority that give rise to complaints may be appealed against through the courts. This applies to the data subject as well as to controllers, where they have been party to proceedings before a supervisory authority. The directive, 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).

No decision of the CJEU has addressed this issue in the DP area, 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 MS to determine that scope, subject to the principles of equivalence and effectiveness.32

As mentioned above under Question 1, the administrative and judicial enforcement may then be coordinated in a different manner as regards the subsequent allocation of damages. In Italy, civil courts are charged with judicial review and also with the award of damages in case of violation of data protections law; whereas in France, judicial review is carried out by administrative courts, and damages are awarded in the civil courts following general civil law provisions.

32 See para. 53. See also the Berlioz case in the tax law area, para. 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.”
Possible further evolution in the light of the new GDPR:

Although the GDPR calls for a dual (administrative/judicial) system, it does not provide information about how both channels should interact. This is not surprising, since such issues are governed by the principle of procedural autonomy of the Member States. However, comparison with the CJEU case law in other fields (notably consumer protection) shows that the Charter, and particularly the principle of effectiveness of judicial protection, can be used to shape guidelines regarding the interdependent functioning of administrative and judicial proceedings.

ITALY

In the Italian system, the authority responsible for overseeing Italian data protection law is the Italian Data Protection Authority. According to article 145 of the Data Protection Code (implementing Directive 95/46) in case of violation of the data protection legislation two alternative enforcement systems are available: one before the supervisory authority, the latter having the power to adopt injunctive measures and to issue fines for breaches; and one before the civil courts, where damages may be also awarded to the victim of an infringement.

In case of enforcement before the supervisory authority, data subjects and data processors may oppose the decision and initiate a proceeding before a civil court, which will provide for judicial review.

In several decisions of the first instance courts, conducting judicial review, it emerges that the supervisory authority’s decisions are not binding on the first instance court either in terms of the existence of the violation, or of the use and acquisition of (new) evidence, or of the type and content of the penalty.

For instance, in the decision of the Tribunale di Milano, no. 10374/2016, the court, carrying out a judicial review of the decision of the national supervisory authority, quashed the decision affirming that the balancing exercise between the public interest in the news (re-)published by an online blog, and the right to personal identity (enshrining the right to oblivion) was not correctly assessed by the national supervisory authority. In this case, then, the tribunal addressed in detail the proofs (i.e. the pieces of news published online) in order provide its own evaluation on whether the personal data of the claimant could be qualified as pertinent, complete and updated.

See also the decision by the Tribunale di Milano, no. 5022/2017, where the court confirmed the decision of the Data Protection Authority, and condemned a telephone operator (Telecom) for contacting about 2 million former customers who explicitly refused or did not consent to be contacted for commercial offers. It seems relevant because it refers to the binding force of CJEU decisions on data protection (e.g. Schrems) and to the role of CFREU. The decision also deals with judicial review: it states that the court before which the claimant appeals against the administrative decision cannot limit its powers to a mere evaluation of formal regularity, considering the nature of the fundamental rights of the parties involved.

A similar result emerges in cases of alternative proceedings regarding the same claim. In a decision of the Italian Supreme Court, the relationship between the role of the supervisory authority and that
of the courts in judicial proceedings was addressed in more detail.\footnote{See Cass. civ. Sez. III, Sent., 12/10/2012, no. 17408.} In particular, the case focused on a complex situation where the data subject presented a claim first before a court and secondly before the supervisory authority. The supervisory authority, erroneously, did not declare the claim inadmissible due to the commencement of the judicial action, and decided the case before the first instance court had concluded the proceedings. The first instance court decided the case, disregarding the decision of the supervisory authority. The claimant then appealed to the Supreme Court against the decision of the first instance court, on the ground of erroneous application of article 145 of the Data Protection Code.

The Supreme Court addressed the issue, clarifying that the availability of two alternative enforcement mechanisms did not, in that specific case, require that the court action be declared inadmissible, as it had been initiated prior to the claim to the data protection authority. In that specific case, it was the proceedings before the supervisory authority that should have been deemed inadmissible. However, given that the decision of the data protection authority was taken before the judicial proceedings ended, and was not appealed by the parties, it had conclusive effect only in relation to the parties’ arguments, meaning that the supervisory authority’s decision could not be reopened by the parties before the court.

In a different case, the Supreme Court again addressed the impact of the decision of the national supervisory authority vis-à-vis the judicial proceedings concerning damages.\footnote{Supreme Court (3) sect), n°13151/2017, 25 May 2017.} Given that the decision of the court might also be given in a different proceeding later in time than the claim before the national supervisory authority for breach of data protection rules, the Supreme Court affirmed that the decision of the supervisory authority cannot bind the civil court as such a decision will never acquire the status (or have the effects) of \textit{res judicata}, due to the fact that the Data Protection Authority is an administrative body and that it doesn’t offer the same guarantees as courts in terms of its impartiality.
5. Impact of the Charter on the conduct of proceedings

5.1. Introduction

The right to a fair hearing 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 the protection of data. 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 one specific issue relating to the conduct of proceedings: the admissibility of evidence in court. The right to the protection of data may be used as an argument to prevent the production of evidence in court, when it is claimed that the piece of evidence infringes the right to the protection of personal data. The CJEU relies, again, on a balance between both fundamental rights – the right to a fair hearing, and the right to the protection of data – to define the methodology national authorities should implement when facing such a situation.

Main questions addressed:

1. Should a document including personal data, access to which has been secured against unauthorized disclosure, be regarded as lawful evidence of the existence of the allegedly unlawful processing of such data when produced by an unauthorized person, with the result that the referring court may 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. In the 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), 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)
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 17 (right to property), 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

Article 7

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 12 - Right of access

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1);
(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.
Question 1: Admissible evidence of a violation of data protection

1. Should a document including personal data, access to which has been secured against unauthorized disclosure, be regarded as lawful evidence of the existence of the allegedly unlawful processing of such data when produced by an unauthorized person, with the result that the referring court may 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 4 (question 1). 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 Court of Justice 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 asks, 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 such as the contested list, 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 starts 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 urges 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 specifies 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 European Union or the need to protect the rights and freedoms of others, the Court leaves 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 stresses 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 goes beyond pure methodology to observe 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 guarantees 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 stresses 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 as regards 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 such as the contested list, 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 is interpreted as encompassing a
right to produce evidence based on documentation including personal data of the person having the right of access to justice, regardless of the lack of authorization by the person controlling the data and regardless of the circumstance that the same documentation includes third parties’ data. As we see below, this aspect is relevant for the issue addressed in the next section. In the balancing of conflicting interests (access to justice, data protection of the subject seeking judicial protection and third parties’ data protection), article 47 plays an important role in striking the balance in favour 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.

**Impact on the follow-up case:**

The case being very recent, the decision of the referring court is not yet available.

**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 Gemeindevbetriebe Frohnleiten, C-221/06, Donnici v Parliament, C-9/08, not published); and 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 the 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.
Apart from excluding any firm obligation to disclose personal data based on the right of access to justice (indeed, the balancing exercise is needed to ascertain whether there is any such obligation), the Court of Justice does not provide explicit guidelines on how to balance the conflicting interests. It does, however, rule that the mere reference to the minor age of the data subject cannot represent a sufficient ground for limiting the victim’s right to access data necessary to seek judicial protection against the harm suffered.

**Impact on national case law in MS 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. As regards 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 judgment 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 (*Tribunale* 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 (*Corte di cassazione*, no. 18279/2010). In a recent judgment concerning child custody, the *Tribunale* 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.
Question 2: Evidence obtained through unlawful processing of data

2. In the 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 the light of the subsequent decision of the Court in Puškár

Relevant legal sources:

National level


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 Court of Justice for a preliminary ruling.

**Preliminary question(s) referred to the Court:**

By 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 (question 1). 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 3 (question 2), the Court implicitly invites national authorities, in the implementation of national law, to follow the methodology described in Chapter 3, question 2 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. When the processing of data does not fall under one of the derogations from data protection admitted by law, 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 the 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:

Not available yet.

Elements of judicial dialogue:

As mentioned above, the question requires a joined analysis of Puškár and Rigas.

Impact on national case law in MS 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 in court evidence collected against employees through a data processing system, whereas the employer had not fulfilled its obligation to declare the existence of such processing to the French data supervisory authority (CNIL).

Before Ryneš, 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).
6. Effective, proportionate and dissuasive sanctions and remedies

6.1. Introduction

The effective protection of natural persons in relation to the processing of personal data calls for effective and dissuasive sanctions and remedies against infringers of the data subjects’ rights. In many 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, but up to now EU legislation has provided few incentives for Member States to implement measures in order to facilitate or encourage the bringing of collective actions. This will change with the coming into force of the GDPR. This chapter will explore these issues in terms of both the current position and future prospects.

Main questions addressed:

1. In order to ensure an effective remedy to data subjects, should EU law be interpreted as implicitly including a right to be de-listed, which data subjects may rely on against controllers to oblige them to remove, from the list of results displayed by search engines, links to web pages published by third parties, even where the data available - the publication of which was lawful – is not previously or simultaneously erased from those web pages?

2. In order to ensure the effective protection of personal data within the European Union 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?

3. Should a court or a supervisory authority with whom an aggregated complaint has been lodged by an individual also vested with a mandate by multiple claimants, extend to the whole group of claimants, under the principle of effectiveness, the type of protection assigned by law to the individual for his status as a consumer, e.g. with regard to the place of jurisdiction?

4. In order to ensure the effective protection of personal data within the European Union, can national data protection authorities be vested with the power to impose a fine on the data controller, even if article 28, Directive 95/46/EC does not expressly refer to such power?

5. What is or should be the impact of the principles of proportionality and/or dissuasiveness on the definition and/or implementation of sanctions and remedies for violations of data protection?

6. In order to ensure the effective protection of personal data within the European Union, to what extent may the sanctions and remedies that are applicable to consumer protection be transposed to the protection of data subjects?
**Relevant legal sources:**

**EU Level**

**Charter of Fundamental Rights of the European Union**

*Article 47 - Right to an effective remedy and to a fair trial*

Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.

Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.

Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

**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**

*Chapter II. General rules on the lawfulness of the processing of personal data*

*Section V. The data subject's right of access to data*

*Article 12 - Right of access*

Member States shall guarantee every data subject the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

— confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,

— communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,

— knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15(1);

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;

(c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b ), unless this proves impossible or involves a disproportionate effort.
Section VII. The data subject’s right to object

Article 14 - The data subject’s right to object.

Member States shall grant the data subject the right:

(a) at least in the cases referred to in Article 7 (e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

(...) Chapter III. Judicial remedies, liability and sanctions

Article 22 - Remedies

Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall 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 23 - Liability

1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

2. The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.

Article 24 - Sanctions

The Member States shall adopt suitable measures to ensure the full implementation of the provisions of this Directive and shall in particular lay down the sanctions to be imposed in case of infringement of the provisions adopted pursuant to this Directive.
Question 1: The use of “corrective remedies” and the right to be de-listed

1. In order to ensure an effective remedy to data subjects, should EU law be interpreted as implicitly including a right to be de-listed, which data subjects may rely on against controllers to oblige them to remove, from the list of results displayed by search engines, links to web pages published by third parties, even where the data available - the publication of which was lawful – is not previously or simultaneously erased from those web pages?

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), 9 March 2017, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v Salvatore Manni, Case C-398/15 (Salvatore Manni)

➢ Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany), lodged on 26 January 2017, Fashion ID Gmbh & Co.KG v. Verbraucherzentrale NRW EV, Case C-40/17 (Fashion ID)

➢ Request for a preliminary ruling from the Conseil d’État (France) lodged on 15 March 2017 — G.C., A.F., B.H., E.D. v Commission nationale de l’informatique et des libertés (CNIL), Case C-136/17

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

The case and relevant legal sources:

The facts of the case and the relevant legal sources have been presented several times in this Casebook, in particular in Chapter 2, under question 3. It should simply be recalled here that the case deals with a data subject requesting that the operator of a search engine be ordered to remove, from the list of results displayed by the search engine following a search made on the basis of his name, links to web pages published by third parties and containing information relating to him. Google, which the court recognized as a controller (see Chapter 2, question 3), claimed that, by virtue of the principle of proportionality, such a request seeking the removal of information was to be addressed not to the operator of the search engine, but to the publisher of the website where the information displayed by the search engine was available.
**Preliminary question(s) referred to the Court:**

Question 2 (c) and (d) and question 3 of the request for a preliminary ruling address the issue in the box.

(2) (c): May the [AEPD], protecting the rights embodied in [Article] 12(b) and [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, directly impose on [Google Search] a requirement that it withdraw from its indexes an item of information published by third parties, without addressing itself in advance or simultaneously to the owner of the web page on which that information is located?

(d): In the event that the answer to the foregoing question is affirmative, would the obligation of search engines to protect those rights be excluded when the information that contains the personal data has been lawfully published by third parties and is kept on the web page from which it originates?

(3) Regarding the scope of the right of erasure and/or the right to object, in relation to the “derecho al olvido” (the “right to be forgotten”), must it be considered that the rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for by [subparagraph (a) of the first paragraph of Article 14] of Directive 95/46, extend to enabling the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally, published on third parties’ web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties?’

**Reasoning of the Court:**

The Court gives separate answers to question 2 (c) and (d), and to question 3, although the issues at stake are quite similar.

Concerning the issue of the extent of the responsibility of the operator of a search engine, contained in question 2 (c) and (d), the Court firstly recalls the nature of the obligations of controllers and the rights of data subjects under EU legislation. It notes, in particular, that data subjects have the right to obtain from the controller the rectification, erasure or blocking of data processing which does not comply with EU legislation, “in particular” because it is incomplete or inaccurate. The use of the expression “in particular” implies, for the court, that the list is not exhaustive, so that non-compliant nature of the processing, which confers upon the data subjects the right to obtain erasure of data, may also arise from non-observance of other conditions. Notably, this should be the case where the processing of data is inadequate, irrelevant or excessive in relation to the purposes for which it is collected and/or processed, and when the balance of interests is weighted in favour of the data subjects’ right to privacy and protection of data (on the balance of interests and the principle of proportionality, see Chapter 3, question 2).

Assessing the role of search engines, the Court observes that the processing of data through search engines creates an impact on the data subjects’ rights to privacy and protection of data (in addition to that of the original publication of data):
“processing of data […] carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual’s name, since that processing enables any internet user to obtain through the list of results 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 his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous” (§80).

The Court thus concludes that supervisory or judicial authorities may order the operator of the search engine 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 containing information relating to that person, 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”.

Regarding question 3, the Court analyses in more depth the “scope of the data subject’s rights”, and observes that the right of the subject to object to the processing of data related to him applies not only to data that is inaccurate, but also to data that is inadequate, irrelevant or excessive in relation to the purposes of the processing. In particular, the Court considers that account should be taken of the passage of time: even initially lawful processing of accurate data may become incompatible with the protection under EU legislation, where such data is no longer necessary for the purposes for which it was collected. The Court therefore requests that national authorities engage in a balancing of interests taking into account the duration of the availability of data (see chapter 3, question 2, and the principle of proportionality). In the case at hand, the Court concludes that the sensitivity of the data and the fact that the publication took place 16 years earlier, implies that the data subject has a right to request that the information related to him no longer be linked to his name in the list of results displayed by the search engine.

Conclusion of the Court:

In certain circumstances, and particularly following a balancing of interests conducted so as to take into account the relevant elements stated in Chapter 3, the data subject has a right to be de-listed from the list of results displayed by a search engine. 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 without having to
establish that the inclusion of the information in the list of results has caused him damage, but only 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 his fundamental rights is justified by the preponderant interest of the general public in having access to the information in question.

**Impact on the follow-up case:**

The Google Spain case, insofar as it creates a right to be de-listed, has raised important debates and new questions.


The opinion of G29 highlights two major elements: an interpretation of the decision; and a framework for dealing with complaints brought to national authorities by data subjects confronted with a refusal to de-list. For the G29, there should be no limit on the right of de-listing from the European extensions of search engines. Besides, search engines do not need to inform source websites of the fact that one of their pages is inaccessible due to de-listing.

Regarding the framework for dealing with complaints, the G29 sets out 13 common requirements that must be applied by national supervisory authorities, based on the ‘general interest of the public to have access to information’.

In Google Spain, the CJEU concludes that the operator of a search engine is responsible for the deletion/removal of the data, after finding that such an operator is a controller within the meaning of the EU legislation. However, further case law will certainly bring clarification on the issue of who are the persons responsible for the effective enforcement of the data subjects’ rights. At least two requests for preliminary rulings are pending, which relate to this issue.

In Fashion ID (C-40/17), the Oberlandesgericht Düsseldorf (Germany) asks the CJEU whether the person embedding a programming code in his website, which causes the user’s browser to request content from a third party and, to this end, transmits personal data to the third party is a controller, even if that person is unable to influence the data processing. Then the referring court asks, if it should be found that such a person is not a controller, if EU legislation is to be interpreted as definitively regulating liability and responsibility in such a way that it precludes civil claims against a third party who, although not a ‘controller’, nonetheless creates the cause of the processing operation, without influencing it.

The issue is also addressed in the question recently referred for a preliminary ruling by the French Conseil d’Etat, which also questions the material scope of the right to be de-listed.

What information is covered by the right to be de-listed? The material scope of the right to be de-listed calls for further clarification. The issue has been raised by the French Conseil d’Etat,
concerning press articles containing sensitive information. The Conseil d’Etat decided to refer several questions for a preliminary ruling (24 February 2017, Req. no 391000 / 393769 / 399999 / 401258 / Request for a preliminary ruling Case C-136/17), which can be summarized as follows: When the request to be de-listed, submitted to the operator of a search engine, targets webpages displaying press articles containing sensitive information, the collection of which is unlawful or strongly regulated, such as information related to sexual orientation, political, religious or philosophical opinions, or information related to criminal offences, how should the right to be de-listed be implemented?

What is the territorial scope of the right to be de-listed? That issue of the territorial scope of the right to be de-listed may be seen as a major one in Europe. The Google Spain case has triggered important discussion between Google and Member States’ supervisory authorities (see, above, the Guidelines laid down by G29). Should Google delete the links not only on European extension (google.fr, google.de, …), but also on its worldwide extension (such as google.com)?

Since Google Spain, Google has implemented self-regulation in order to receive and address the claims of data subjects to be de-listed. However, Google initially limited the territorial scope of application of the right to be de-listed to its European extension. After February 2016, Google decided that the right to be de-listed would be applicable on a worldwide basis, but only for European internet users: using the IP address of the internet user, Google decides if the information subject to deletion may or may not be displayed. It is not displayed if the user is in Europe, but it is if the user is abroad.

The French Conseil d’Etat has referred a question for a preliminary ruling to the CJEU, on the issue of the territorial scope of the right to be de-listed (19 July 2017, Req. no 399922), which can be summarized as follows:

- in the light of the CJEU decision in Google Spain, when the request to be de-listed is admitted, should such a de-listing be effective on all national extensions of the search engine, so that the disputed links are totally unavailable, regardless of where the person doing the search is based, including when that person operates in a location outside of the territorial scope of EU legislation?

- if the answer to the first question is negative, should the de-listing be effective only on the national extension of the MS where the person doing the search is based, or shall it be effective on all national extensions of EU Member States?

- if the answer to the first question is negative, should the operator of the search engine delete, by using geo-blocking techniques, all disputed links displayed as results of a search made from an IP address deemed to be located in the Member State where the request is brought, or located in all EU Member States?

**Elements of judicial dialogue:**

Google Spain is interestingly complemented by the decision of the Court in Salvatore Manni (C-398/15). Mr Manni requested that the personal data related to him be erased, after the elapse of a certain period of time, from the public companies register, where 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” within the meaning of Directive 95/46, the Court observes 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 notes that under article 6(1)(e) of Directive 95/46, Member States are to ensure that personal data is 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 the light of the purpose of the processing or, here, the registration.

The Court observes that the purpose of the disclosure provided for by Directive 68/151 is to protect in particular 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 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.
Impact on national case law in MS different from the state of the court referring the preliminary question to the CJEU:

FRANCE: ON THE FOLLOW-UP OF GOOGLE SPAIN

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. 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 Cour de cassation goes against the decision of the courts of first instance, which considered that this service is automated, and thus that Google cannot be liable for unlawful content put forward via Google Suggest.

The French case law, after Google Spain, 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. For instance, when an issue concerns the functioning of public institutions, the de-listing would be an infringement of freedom of expression.

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.

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 must be interpreted accord to the case law of the CJEU.

---

35 Drafted by the students of Master PIDAN (UVSQ)
36 TGI Paris, 15th February 2012, Kriss Laure/Larry P, Google Inc
37 C. cass. civ. 1ère, 19 June 2013, no 12-17,591
39 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
41 L. n° 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés
42 See for example, TGI Paris, 10 February 2017, M. X c/ Google France et Google Inc.; CA Lyon, 8th chamber, 28 February 2016
One decision by the *Cour de cassation* 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.

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. 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. 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 emphasize 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 Court of Justice of the European Union, before deciding whether Google must ‘de-list’ information on all extensions of its search engine, or in some countries only. 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

2017, RG no 15/05788.
43 *C. cass., ch. civ. 1ère*, 12 May 2016, no 15-17.729
44 *TGI* Paris, 16 September 2014, *M. et Mme. X et M. Y c/ Google France*

150
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.

**FRANCE: ON OTHER TYPES OF REMEDIES**

*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.

This decision implicitly relies on the principles of effectiveness and dissuasiveness since it deprives of any commercial interest a file including unlawfully processed personal data. 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**

*Google Spain.* 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).48

By contrast, the Italian case law after *Google Spain* unanimously embraces the view, upheld by the CJEU, that search engine providers must be regarded as “data controllers” under article 2 (d) of Directive 95/46. 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 law49 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).

---

47 Drafted by Gianmatteo Sabatino
48 See Court of Cassation, decision no 5525/2012
49 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.
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\(^{50}\) 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 courts have devised a “double level of protection”\(^{51}\) 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: 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\(^{52}\); on the other hand, any complaint regarding the erasure, removal or adjustment of information must be addressed to the publisher of such information\(^{53}\) since that is the party solely responsible for the content of the information displayed.

*Manni*\(^{54}\). On the basis of what the CJEU established in *Manni* (decision of 9 March 2017, C-398/15), a recent Italian decision by the *Corte di Cassazione*, 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.

---

50 North Naples Tribunal, decision of 3 November 2016.


52 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 scrutinized 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.

53 See Rome *Tribunale*, decision of 3 December 2015.

54 Drafted by Lavinia Vizzoni
Question 2: Effective remedies and the principle of full compensation

2. In order to ensure the effective protection of personal data within the European Union 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?

Relevant EU case law

➢ Judgment of the European Union 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

Relevant national case law

➢ Italian Supreme Court (Corte di cassazione), Third Civil Chamber, 15 July 2014, n. 16133 (University of “Rome Three” v. Pieraccini et al.)

➢ Italian Supreme Court (Corte di cassazione), First Civil Chamber, 8 February 2017, n. 3311 (S.G. v. Società italiana degli avvocati amministrativisti)

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:

Italian Supreme Court (Corte di cassazione), Third Civil Chamber, 15 July 2014, n. 16133 (University of “Rome Three” v. Pieraccini et al.)

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 Tribunale of Rome since their names were included in an Excel file listing 3724 students enrolled at the University, showing their personal data, including tax code, University student status, employment position and wage status. The file could be accessed via Internet by a Google search based on the students’ names. The Tribunale 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 Supreme Court by the University of Rome, which challenged the Tribunale decision especially in regard to the award of damages for non-economic loss, as its seriousness or gravity were not ascertained.

**Reasoning of the Court:**

Referring to the settled caselaw of the Corte di cassazione (see partial decision no 26972/2008 by Joint Chambers), the decision states that non-economic losses may be recovered only if, assuming fundamental rights are violated or the law expressly allows for recovery of non-economic losses, the infringement is serious and the damages are not trivial ("futili"). Damages have to be proved and may not be ascertained ex se (automatically) since liability in tort may not have a punitive function. 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 leniency ("tolleranza") 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 principle of solidarity and the principle of effectiveness (of fundamental rights). Indeed, the effective protection of these rights 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 Supreme Court 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 the recent judgment of the Corte di cassazione, 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. It is worth noticing that the Court additionally condemns the claimant for abuse of the process of the court under article 96 of the Italian civil procedure code.

- 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.

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 him (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 illegalties established and of their consequences. These two elements resemble the assessment criteria used in the Italian decision examined above.

A short view on the new GDPR:

Not unlike article 23 of Directive 95/46/EC, 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, which the Directive had failed to do. The burden of proving the absence of liability is placed on the controller/processor, similarly to what was provided in the 95/46/EC
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.
Question 3: Collective redress

3. Should a court or a supervisory authority with whom an aggregated complaint has been lodged by an individual also vested with a mandate by multiple claimants, extend to the whole group of claimants, under the principle of effectiveness, the type of protection assigned by law to the individual for his status as a consumer, e.g. with regard to the place of jurisdiction?

Relevant CJEU case law

➢ Judgment of the Court (Third Chamber), 25 January 2018, Maximilian Schrems v Facebook Ireland Limited, Case C-498/16 (Schrems II).

➢ Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany), lodged on 26 January 2017, Fashion ID Gmbh & Co.KG v. Verbraucherzentrale NRW EV, Case C-40/17 (Fashion ID)

The issue of collective actions, in the implementation of EU legislation on data protection, has not been directly addressed by the CJEU, mainly because Member States have not yet, or have only very recently, adopted national legislation allowing for collective action against infringers of data protection.

However, two questions raising issues on collective redress have been referred for preliminary ruling by the CJEU.

In Fashion ID (Case C-40/17), the - still pending - question asked is whether it is possible for national law, in addition to the powers of intervention conferred on the data protection authorities and the remedies available to the data subject, to grant 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. This case cannot usefully be exploited at the present time.

Schrems II (C-498/16) will be considered as the main case in relation to the issue in the box.

Relevant EU legal sources

Regulation 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (Brussels I) / see also the equivalent provision in Brussels I revised (article 18, Regulation 1215/2012, Brussels I bis)

Article 16 of the Regulation:

1. A consumer may bring proceedings against the other party to a contract either in the courts of the Member State in which that party is domiciled or in the courts for the place where the consumer is domiciled.

2. Proceedings may be brought against a consumer by the other party to the contract only in the courts of the Member State in which the consumer is domiciled.

3. This Article shall not affect the right to bring a counter-claim in the court in which, in
accordance with this Section, the original claim is pending.’

To grant consumers effective access to justice, article 16 of the Regulation allows consumers to bring claims against professionals before the courts where the consumer (claimant) is domiciled, derogating from the general rule according to which the main court having jurisdiction is that of the Member State where the defendant has its domicile.

**Preliminary question referred to the Court**

In *Schrems III* (C-498/16), the question is whether a social network user, being a “consumer” within the meaning of Regulation Brussels I/IIbis, can, at the same time as his own claims arising from a consumer supply at the claimant’s place of jurisdiction, invoke the claims of others consumers on the same subject who are domiciled:

a. in the same Member State,
b. in another Member State: or
c. in a non-Member State.

**Reasoning of the Court**

The AG Opinion, delivered on 14 November 2017, proposed that such a question should be answered in the negative. His opinion relied mainly on the argument that to decide otherwise would not be consistent with the foreseeability of the forum, and would encourage forum shopping. Moreover, AG Bobek argued that it is not for the Court, interpreting article 16 of the Brussels I Regulation in the light of the principle of effectiveness of consumer protection, to make up for the EU and/or Member States’ failure to provide collective redress in consumer matters. The AG did not address the issue of whether effective means to coordinate multiple victims’ claims in collective redress procedures do (or should) exist in the field of data protection, an issue only touched upon addressed Directive 95/46, whereas it might attract more attention in the light of GDPR.

The Court followed the AG Opinion. It first recalled that the rule of jurisdiction laid down in article 16 of the Regulation is a derogation from the general rule, and should as such be given a strict interpretation. It also recalled that because the concern is to protect the consumer as a weaker party, the consumer is protected only if he is himself party to the proceedings.

The Court then stressed that the attribution of jurisdiction should be predictable. Consequently, it found that the assignment of claims, even when made by a consumer to another consumer, cannot have any impact on the determination of which court has jurisdiction.

As in previous decisions on the jurisdiction of courts, the CJEU implicitly relies on the principle of proportionality, balancing the interests of the claimant in access to justice, and of the defendant in being able to foresee which court will have jurisdiction.

**Conclusion of the Court**

Article 16(1) of Regulation No 44/2001 must be interpreted as meaning that it does not apply to 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.

A short view on the new GDPR:

Article 80, GDPR deals with representation of data subjects before supervisory authorities and courts. Pursuant to this provision, “[t]he data subject shall have the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf, to exercise the rights referred to in Articles 77, 78 and 79 on his or her behalf, and to exercise the right to receive compensation referred to in Article 82 on his or her behalf where provided for by Member State law”. It also adds that “Member States may provide that any body, organisation or association referred to in paragraph 1 of this Article, independently of a data subject's mandate, has the right to lodge, in that Member State, a complaint with the supervisory authority which is competent pursuant to Article 77 and to exercise the rights referred to in Articles 78 and 79 if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing”.

This provision does not necessarily deal with collective redress, since the mandate to the body, organization or association may remain individual and be dealt with as such. However, it seems reasonable to believe that the role of such representative institutions should develop (and probably will, through Schrems-like cases) in the area of collective redress, where multiple claims may be aggregated and coordinated. Taken together with the role of the institutions regulated by article 80, such aggregation could cover any type of complaint lodged with a supervisory authority (article 77) and any type of judicial remedy sought before a court under article 78, including damages (article 82).

If article 80 were interpreted also in regard to collective redress claims, one might ask whether this type of aggregation should be favoured from the standpoint of effective protection of data subjects due to the greater capacity of this type of institution to coordinate multiple claims, to identify potentially interested victims, to lower the costs of litigation, and therefore to increase the deterrent impact of enforcement mechanisms.

Once this provision is applicable (May 2018), a supervisory authority or a court, with which a collective complaint was lodged by a “group” of claimants represented by an individual like Mr Schrems, might ask whether, proceeding from the principle of effectiveness, article 80 GDPR, should not be interpreted in broad terms expanding the concept of “organisation” so as to include collective structures, though not formalized into a new legal entity: a possible question of interpretation for a future preliminary ruling?

If that were the case, other doubtful areas of interpretation could be: (i) the possibility that claimants from different MS could join a single procedure; (ii) how to determine the competent jurisdiction in such case and, more particularly, whether and how article 79 (2), second sentence, GDPR, could be applied, when it enables the claimant to file a lawsuit before a court of the MS where he/she has his/ her habitual residence as data subject, or whether only the first part of the paragraph should be applicable, thus putting the court having jurisdiction in the Member State
where the controller or processor has an establishment. On this latter reading, some similarities could be found with the consumer protection case law of the CJEU, where the Court distinguishes between individual redress mechanisms and collective redress mechanisms and acknowledges that the presence of representative associations may reduce the need for a higher degree of consumer protection, e.g. in the field of *ex officio* judicial powers (see *Salès Sinués* analysis in the Consumer Protection Casebook).
Question 4: The sanctioning powers of national data protection authorities

4. In order to ensure the effective protection of personal data within the European Union, can national data protection authorities be vested with the power to impose a fine on the data controller, even if article 28, Directive 95/46/EC does not expressly refer to such power?

Relevant CJEU case law

➢ 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 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

Chapter VI. Supervisory Authority and Working Party on the protection of individuals with regard to the processing of personal data

Article 28. Supervisory authority [see, comparatively, article 51 seq., part. article 58, GDPR]

1. Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.

These authorities shall act with complete independence in exercising the functions entrusted to them.

2. Each Member State shall provide that the supervisory authorities are consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data.

3. Each authority shall in particular be endowed with:

- investigative powers, such as powers of access to data forming the subject-matter of processing operations and powers to collect all the information necessary for the performance of its supervisory duties,

- effective powers of intervention, such as, for example, that of delivering opinions before processing operations are carried out, in accordance with Article 20, and ensuring appropriate publication of such opinions, of ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the controller, or that of referring the matter to national parliaments or other political institutions,
- 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.

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

4. Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data. The person concerned shall be informed of the outcome of the claim.

Each supervisory authority shall, in particular, hear claims for checks on the lawfulness of data processing lodged by any person when the national provisions adopted pursuant to Article 13 of this Directive apply. The person shall at any rate be informed that a check has taken place.

5. Each supervisory authority shall draw up a report on its activities at regular intervals. The report shall be made public.

6. Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3. Each authority may be requested to exercise its powers by an authority of another Member State.

The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

7. Member States shall provide that the members and staff of the supervisory authority, even after their employment has ended, are to be subject to a duty of professional secrecy with regard to confidential information to which they have access.

**The case and relevant legal sources:**

The facts of the case and the relevant legal sources have been presented in Chapter 1, question 2. It will simply be recalled here that the issue was whether the Hungarian data protection authority could exercise the power, conferred upon it by Hungarian law, to impose a fine on a company which, although registered in Slovakia, ran a property dealing website concerning Hungarian properties.

**Preliminary question referred to the Court:**

The Court was not directly asked whether the Hungarian law, inasmuch as it confers upon the Hungarian data protection authority the power to impose penalties on controllers violating the regulation on the protection of personal data, was compatible with EU legislation. The question was rather whether, given the territorial scope of the law, the Hungarian authority could exercise such a power against a company registered in Slovakia. This issue has been dealt with in Chapter 2.
However, the Court considered that, before dealing with the territorial scope of the national data protection authority’s powers, “it is necessary to examine what are the powers of that supervisory authority, in the light of Article 28(1), (3) and (6) of Directive 95/46”. Thus it deals with the issue in the box.

Reasoning of the Court:

For the Court, it follows from article 28(1) of Directive 95/46 that each supervisory authority established by a Member State has to ensure compliance, within the territory of that Member State, with the provisions adopted by the Member States pursuant to Directive 95/46. The Court then observes that pursuant to article 28(3) of Directive 95/46, those supervisory authorities are in particular to be endowed with investigative powers, such as powers to collect all the information necessary for the performance of their supervisory duties, and effective powers of intervention, such as powers to order the blocking, erasure or destruction of data, to impose a temporary or definitive ban on processing, or to warn or admonish the data controller. The Court stresses that this list of powers should not been seen as exhaustive, and that given the type of powers of intervention mentioned in the provision, as well as the discretion available to the Member States in transposing Directive 95/46, it should be considered that those powers of intervention may include the power to penalise the data controller by imposing a fine on him, where appropriate. The Court adds that such a power should be exercised in accordance with the procedural law of the Member State to which the supervisory authority belongs.

The decision of the Court can be read as implicitly referring to the principle of effectiveness, since the reasoning of the Court is based on the idea that, national supervisory authorities being established to ensure compliance with the regulation on data protection, they should be vested with the necessary powers to do so, even if such powers are not expressly listed in Directive 95/46.

Conclusion of the Court:

The Hungarian supervisory authority may exercise the power to impose a fine on a controller, even if such power is not expressly included in the Directive. However, this power should be exercised according to the procedural law of the Member State to which the supervisory authority belongs, and only on the territory of this Member State (see chapter 2 on territorial scope).

Impact on the follow-up case:

Information not available.

Elements of judicial dialogue:

Not available yet.
Impact on national case law in MS different from the state of the court referring the preliminary question to the CJEU:

Not available yet.

A short view of the new GDPR:

In the new 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, hereinafter GDPR), the powers of independent supervisory authorities are more extensively defined. Among these, the power “to impose an administrative fine pursuant to Article 83, in addition to, or instead of measures referred to in this paragraph, depending on the circumstances of each individual case” is explicitly referred to as a mandatory power for supervisory authorities.

The EU legislature has therefore taken into account the outcome of judicial dialogue that has occurred within the CJEU in decisions, like the ones here commented on, in which the Court has explicitly or implicitly interpreted Directive 95/46 in the light of the principle of effectiveness. Today this principle is explicitly referred to in article 83, GDPR, together with the principles of proportionality and dissuasiveness (see article 83(1)). A wider analysis on the application of these principles by the CJEU and on their subsequent incorporation into the GDPR is provided below under Question 4.
Question 5: Proportionate and dissuasive remedies or sanctions in data protection

Relevant CJEU case law

The issue in the box has been addressed only in passing by the CJEU, in its decision in the *Lidqvist* case.

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

The case and relevant legal sources:

The facts of the case, as well as the relevant legal sources, have been described in Chapter 2, question 1. It will simply be recalled, and added, that Mrs. Lindqvist, who was a maintenance worker, had infringed the 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 European Union 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 in perspective both principles of effectiveness and proportionality, 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 the follow-up case:
Not available yet.

Elements of judicial dialogue:
No information yet.

Impact on national case law in MS 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 publicizing 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 the 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 expressly so states, 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.

*A short view on the new GDPR:*

Compared with Directive 46/95, Regulation (EU) 2016/679 (GDPR) has paid much greater attention to the application of general principles (including effectiveness, dissuasiveness and proportionality) to penalties and other measures. In particular, Article 83(1) GDPR provides that “Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive”.

Moreover, “[w]hen deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: (a) 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; (b) the intentional or negligent character of the infringement; (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects; (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32; (e) any relevant previous infringements by the controller or processor; (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement; (g) the categories of personal data affected by the infringement; (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures; (j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and (k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.”.

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 penalties 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. Though now within a more regulated framework, the general principles developed by the CJEU under Directive 46/95 will continue to play an important role in the coming years.
Question 6: The application of consumer protection to data subjects

6. In order to ensure the effective protection of personal data within the European Union, to what extent may the sanctions and remedies that are applicable to consumer protection be transposed to the protection of data subjects?

Relevant CJEU case(s)

➢ Judgment of the Court (Third Chamber), 28 July 2016, Verein für Konsumenteninformation v. Amazon EU Sàrl, C-230/14 (Amazon)
➢ Judgment of the Court (Third Chamber), 25 January 2018, Maximilian Schrems v Facebook Ireland Limited, Case C-498/16 (Schrems II).

The case(s):

In certain circumstances, the data subject and the controller are party to a contract, and it is in the context of this contract that the data subject makes available its personal data to the controller. This is the case, particularly, for the functioning of social networks or of online sale platforms. In such circumstances, the question arises whether the users of the online service may rely, when they consider that there is a misuse of their personal data by the controller, on the rules enacted for the protection of consumers.

In Amazon, the main question was to determine whether Regulation Rome I (law applicable to contractual obligations) or Regulation Rome II (law applicable to non-contractual obligations) was applicable to identify the law applicable to an action for an injunction within the meaning of Directive 2009/22/EC, brought by an association and directed against the use of allegedly unfair contractual terms by an undertaking established in a Member State, entering into contracts in the course of electronic commerce with consumers resident in other Member States. The case also dealt with the issue of the unfairness of a choice-of-law clause included in a consumer contract, according to which the law applicable was the law of the Member State where the professional had its establishment. Indeed, the binding effect of such clause could be challenged under article 6 of Regulation Rome I, according to which the consumer shall not be deprived of the protection of the law of the Member State where he has his domicile. [On these issues, see the Casebook on consumer protection, Chapter 7].

One of the issues also concerned personal data, since several clauses in Amazon’s general terms and conditions gave Amazon the right to process, exchange and otherwise use the data collected from users of the sale platform. One of the questions referred to the Court related to such clauses.
Preliminary question referred to the Court:

The question was drafted as follows:

‘Is the processing of personal data by an undertaking which in the course of electronic commerce concludes contracts with consumers resident in other Member States, in accordance with Article 4(1)(a) of [Directive 95/46], regardless of the law that would otherwise apply, subject exclusively to the law of the Member State in which is situated the establishment of the undertaking in the context of which the processing takes place, or must the undertaking also comply with the data protection rules of those Member States to which its commercial activities are directed?’

In other words, the referring court was asking whether the contractual clauses concerning the processing of data were to be assessed only in the light of the rules laid down in article 4 of Directive 95/46, which defines the territorial scope of Member States’ laws protecting personal data, or if the law applicable to the consumer contract, i.e. the law of the Member States to which the seller/controller directed its commercial activities, could also apply.

Reasoning of the Court:

The Court engages in reasoning that is strictly in line with its reasoning developed for the interpretation of article 4 of Directive 95/46 (see chapter 1), on the basis that ‘the processing of personal data carried out by an undertaking engaged in electronic commerce is governed by the law of the Member State to which that undertaking directs its activities, if it is shown that the undertaking carries out the data processing in question in the context of the activities of an establishment situated in that Member State’.

So, it appears that the Court does not accept the expansion of the protection of data subjects through the application of the rules on consumer protection. When data processing is encompassed in a consumer contract, the question whether such data processing is lawful shall only be governed by the law of the Member State where the controller’s establishment in the context of the activities of which the data processing is carried out is located, pursuant to article 4 of Directive 95/46. The law of a Member State to which the seller/controller directs its commercial activities, applicable to the consumer contract pursuant to Regulation Rome I, may not apply to assess the lawfulness of the processing of data under such a contract, unless it is also the law of the Member State where the establishment is located in the context of the activities of which the data processing is carried out.

One might ask whether the Court might have relied on the principle of effectiveness and/or dissuasiveness to decide differently. Where a consumer contract includes a provision on the processing of data, sometimes the law applicable to the contract and the law applicable to the processing of data will be different. If a German sale platform sells goods to consumers domiciled in France, French law will usually apply to the consumer contract since the German platform “directs its activities” to France. But it is not certain that the circumstances will show that the data is processed in the context of the activities of an establishment located in France, and thus German law will apply to the processing of such data. In this regard, it could be said that it might be more effective and dissuasive to allow the consumer to rely either on the French law governing the contract, or on the German law governing the data processing. Letting the victim opt between two national regimes, to select the one that imposes heavier sanctions on the infringer, is a method that
EU private international law has already implemented for reasons of effectiveness and dissuasiveness (see for instance, Regulation Rome II in tort matters related to the environment).

**Conclusion of the Court:**

The lawfulness of a consumer contract clause concerning the protecting of data is to be assessed in the light of the law of the Member State to which that undertaking directs its activities, only insofar as it is shown that the undertaking carries out the data processing in question in the context of the activities of an establishment situated in that Member State, within the meaning of article 4 (1)(a) of Directive 95/46. It is for the national court to ascertain whether that is the case.

**Impact on the follow-up case:**

Not available.

**A short view on the new GDPR:**

The GDPR seems to introduce some changes to the approach described above.

If the controller’s establishment is located in a Member State, the solution should strictly speaking be the same. The law applicable to the processing of data, even if under a consumer contract, shall be the law of the Member State where the establishment is located in the context of whose activities the processing of data is carried out, without regard to the law governing the consumer contract. Certainly, the reason behind such an approach is that further harmonization of data protection within the European Union offers sufficient guarantee that the consumer’s personal data will, when a Member State’s law is applicable, be sufficiently protected.

If the controller’s establishment is located outside of the Union, the solution is different.

Art. 3 (2) (a) GDPR states that:

‘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 behavior as far as their behavior takes place within the Union.’

It follows from this provision that when a controller established outside of the European Union directs its activities to consumers established in the European Union, EU Regulation will apply to the processing of data undertaken by such a controller, irrespective of the place where the processing of data is effectively carried out.
Elements of judicial dialogue:

- Horizontal (within CJEU)

The conclusion of the Court in *Amazon* is to be read with the decision in *Schrems II*. The case deals with the issue whether the user of a social network is a consumer and can as such rely on EU rules protecting consumers (in particular Brussels I Regulation), depending on the type of use of the social network. The question is to determine whether a “consumer” loses that status, if, after the comparatively long use of a private Facebook account, he publishes books relating to the enforcement of his claims, on occasion also delivers lectures for remuneration, operates websites, collects donations for the enforcement of his claims and has the claims of numerous consumers assigned to him on the assurance that he will remit to them any proceeds awarded, after the deduction of legal costs. In his Opinion, Advocate General Bobek concluded that the status of consumer should, in the case at hand, be maintained. And he inferred from this conclusion that Mr Schrems may, for his own claims (on the different solution concerning the claims assigned to him by other consumers, see below, 6.2 Collective actions), rely on the Brussels I rules on jurisdiction protecting consumers. The Court adopted the same view.

A combined reading of *Amazon* and *Schrems II* implies that:

- when the processing of data is encompassed in a consumer contract, the data subject is also a consumer;

- the data subject may therefore rely, to identify the courts having jurisdiction over his claims against the other party/controller, on the rules enacted for the protection of consumers in Regulation Brussels I;

- however, the law applicable to assessing the lawfulness of the processing of data is necessarily the law of the Member State where the establishment is located in the context of the activities of which the processing is carried out, within the meaning of Directive 95/46; the law governing the consumer contract is not applicable to such assessment. Nor, as seen above, would that conclusion change under the GDPR, which further expands the scope of EU data protection in favour of data subjects who “are” in the Union and are affected by processing carried on by a controller or processor not established in the Union, when the processing activities are related to the offering of goods or services, regardless the (consumer/professional) status of the parties to the transaction.

Therefore, in the light of the case law examined, the application of rules of consumer protection concerning the identification of the court having jurisdiction to some extent reinforces the data subject’s protection, whereas consumer protection does not seem to influence the rules on the territorial scope of EU data protection, which apply irrespective of the status of the data subject as a consumer.

One might ask whether the consumer status of the data subject may play a role in other respects, requiring a stricter application of the principle of effectiveness in the field of data protection. For
instance, based on EU case law on effective consumer protection, should a judge *ex officio* ascertain whether a data subject’s consent to processing is based on an unfair term or a breach of a duty to inform?

With regard to this aspect, see GDPR, recital (42), which reads: “[…] 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.” (see also article 7(2) and (4), GDPR, on consent requirements).

For an extensive discussion of ex officio powers of judges in consumer protection, *see Rejus Consumer Casebook, chapter 1.*

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

**FRANCE**

In a 2016 decision, the Paris Appeal Court (*Cour d’appel de Paris, Pôle 2 – Chambre 2*, 12 February 2016, no 15/08624, Facebook) decided that the contract concluded between a user of the social network provided by Facebook, and the company Facebook Inc., is a consumer contract. Even if the service is provided to users free of charge, Facebook Inc., which is a professional, derives important benefits from its activity. The contract is not individually negotiated. Based on that decision that the contract is a consumer contract, the Appeal Court considers that pursuant to articles 15 and 16 of the Brussels I Regulation, the consumer could decide to bring his claim before the court of his place of domicile, in that case Paris, despite the choice-of-court provision included in the general terms and conditions of the contract, according to which the courts of California (USA) have exclusive jurisdiction over any litigation concerning the terms of the contract. Consequently, the Paris court had jurisdiction to rule on the validity of such choice-of-court provision.

Given that the choice-of-court provision included in the contract obliges the consumer to bring his claims against the professional before a court which is a long way from his domicile, and to incur costs out of proportion to the amounts of money at stake, the French Court concludes that the practical difficulties and the costs of accessing the foreign court are likely to deter the consumer from bringing any claim and cause him to forgo any legal remedy or defence.

On the other hand, Facebook has an agency in France, and has financial and human resources making it easy for it to ensure its legal representation and defence before the French courts. The choice-of-court provision being unfair, it must be deleted and the French courts have jurisdiction over the claims brought by the consumer. **The Appeal Court’s reasoning is implicitly based on**
the principle of effective access to justice and on the principle of proportionality. [see Consumer Casebook, chapter 1 and 7]