FRICoRe

Judicial Training Project

Fundamental Rights In Courts and Regulation

CASEBOOK

EFFECTIVE DATA PROTECTION AND FUNDAMENTAL RIGHTS

COUR DE JUSTIC

DE L'UNION

SSM

Scuola Superiore della Magistratura

UNIVERSITY OF TRENTO

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

Effective Data Protection and Fundamental Rights

Edited by Paola Iamiceli, Fabrizio Cafaggi, Chiara Angiolini

Publisher: Scuola Superiore della Magistratura, Rome – 2022

ISBN 9791280600271

Published in the framework of the project:

Fundamental Rights In Courts and Regulation (FRICoRe)

Coordinating Partner:

University of Trento (*Italy*)

Partners:

Scuola Superiore della Magistratura (*Italy*)

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

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

University of Groningen (*The Netherlands*)

Pompeu Fabra University (*Spain*)

University of Coimbra (*Portugal*)

Fondazione Bruno Kessler (*Italy*)

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

Edition: May 2022

Scientific Coordinator of the FRICoRe Project:

Paola Iamiceli

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

Paola Iamiceli

Project Manager:

Chiara Patera

Co-editors and Co-authors of this Casebook:

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

Introduction: Fabrizio Cafaggi and Paola Iamiceli

Ch. 1: Sandrine Clavel, Fabienne Jault-Seseke

Ch. 2: Sandrine Clavel, Chiara Angiolini

Ch. 3: Sandrine Clavel, Mateusz Grochowski

Ch. 4: Chiara Angiolini

Ch. 5: Sandrine Clavel, Mateusz Grochowski

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

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

Ch. 8: Sandrine Clavel, Mateusz Osiecki

Ch. 9: Chiara Angiolini, Sébastien Fassiaux

Note on national experts and contributors:

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

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

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

Table of Contents:

INTRODUCTION: A BRIEF GUIDE TO THE CASEBOOK 8

Cross-project methodology ... 8

The main issues addressed in this Casebook ... 10

The structure of the Casebook: some keys for reading ... 12

1. IMPACT OF THE CHARTER ON THE TERRITORIAL SCOPE OF DATA PROTECTION 15

1.1. Introduction ... 15

1.2. Intra-EU relations ... 15

1.2.1. Question 1: Interpretation of the connecting factor defining the territorial scope of a Member State's law on data protection and of the GDPR ... 16

1.2.2. Question 1a: Geographical scope of controllers' obligations ... 22

1.2.3. Question 2: Coordination between national data protection authorities regarding intra- EU cross border processing ... 24

1.2.4. Question 3: Impact of the territorial limitation of national data protection authorities: the duty of cooperation ... 30

1.2.5. Questions 4: Coordination between national courts regarding intra-EU cross-border processing ... 42

1.3. Relations with third countries ... 48

1.3.1. Question 5 & 6: The scrutiny of third countries' legislation in terms of EU law and its consequences ... 49

1.4. Further developments in CJEU case-law: Facebook Ireland Ltd, Maximillian Schrems (C-311/18), 16 July 2020 ... 54

1.5. Guidelines emerging from the analysis ... 56

2. IMPACT OF THE CHARTER ON THE MATERIAL SCOPE OF DATA PROTECTION 58

2.1. Introduction ... 58

2.1.1. Question 1: Definition of the concept of "personal data" ... 59

2.1.2. Question 2: Definition of the concept of "processing" of personal data ... 66

2.1.3. Question 3: Definition of the concept of "controller" ... 72

2.1.4. Question 3a: the concept of controllership ... 72

2.1.5. Question 3b: joint controllership ... 76

2.1.6. Question 4: Definition of the concept of "data subject" ... 81

2.2. Guidelines emerging from the analysis ... 82

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

3.1. The general scope of exceptions under GDPR ... 84

3.1.1. Question 1: The extension of the protection of data in the field of State security matters ... 85

3.1.2. Question 2: The role of effective judicial protection and proportionality in establishing the state security exception. ... 93

3.1.3. Question 3: The role of effective judicial protection and proportionality in establishing the state security exception ... 96

3.2. Guidelines emerging from the analysis ... 99

4. IMPACT OF THE CHARTER ON THE ASSESSMENT OF THE LEGITIMACY OF DATA PROCESSING ... 100

4.1. Introduction. The lawful basis for processing and Article 8 CFREU between Directive 95/46 and Regulation UE 2016/679 ... 100

4.1.1. Question 1: The legitimate interest as a lawful basis for processing ... 101

4.1.2. Question 2: Consent of the data subject as a legitimate basis for processing ... *108*
4.1.3. Question 3: Fundamental rights and legitimate basis for processing ... *114*
4.2. Guidelines emerging from the analysis ... 119
5. PRIVACY VS. FREEDOM OF EXPRESSION — THE FUNDAMENTAL RIGHTS PERSPECTIVE 122
5.1. Introduction ... 122
5.1.1. *Question 1: Social media platforms and freedom of expression* ... *124*
5.1.2. *Question 1b: the intersections of freedom of expression and privacy in domestic case law* ... *130*
5.1.3. *Question 2: The role of public interest in revealing information vis-à-vis data and privacy protection* ... *133*
5.2. Guidelines emerging from the analysis ... 136
6. EFFECTIVE DATA PROTECTION BETWEEN ADMINISTRATIVE AND JUDICIAL ENFORCEMENT ... 138
6.1. Introduction ... 138
6.1.1. *Question 1: The right to effective judicial remedy and the coordination of administrative and judicial enforcement* ... *142*
6.1.2. *Question 2: Interaction between the CJEU and the ECtHR* ... *147*
6.2. Administrative authorities and effective protection of data subjects ... 149
6.2.1. *Question 3: Coordination between EU institutions and national authorities* ... *149*
6.2.2. Question 3c: The cooperation between national authorities and the right to seek action of national not-leading DPA ... *151*
6.2.3. Question 4: Duty of cooperation of national authorities regarding the possible invalidity of an EU act ... *155*
7. EFFECTIVE, PROPORTIONATE AND DISSUASIVE SANCTIONS AND REMEDIES 158
7.1. Introduction. Remedies and sanctions within the GDPR ... 158
7.2. The impact of the principle of effectiveness on the system of sanctions and remedies drawn by the GDP ... 161
7.2.1. *Question 1: The impact of the principle of effectiveness on remedies: the example of the right to "de-listing"* ... *161*
7.2.2. Question 2: Effective remedies and the principle of full compensation ... *175*
7.2.3. Question 3: Impact of the principle of effectiveness on the array of full compensation ... *179*
7.3. The impact of the principle of proportionality on remedies and sanctions ... 183
7.3.1. *Question 4: Sanctions and the principle of proportionality* ... *183*
7.3.2. Question 5: the principle of proportionality and the right to be de-listed ... *185*
7.3.3. Question 6: Proportionality, effectiveness, data/privacy protection and the information obligations ... *189*
7.4. BOX: Impact of fundamental rights on automated decision-making and profiling ... 197
7.5. BOX: AI, the black box and data subjects' rights: the role of Article 47 CFR ... 199
7.6. BOX: Balancing multiple individuals' rights under article 47 of the Charter. The example of the right to access ... 199
8. DATA PROTECTION AND PROCEDURAL RULES: THE IMPACT OF THE CHARTER 201
8.1. Introduction ... 201
8.1.1. *Question 1: Right to have access to personal data which enables instituting civil proceedings in light of Articles 8 and 47 of the Charter and of the principles of proportionality and effectiveness.* ... *202*
8.1.2. *Question 2: Admissible evidence of a violation of data protection* ... *206*
8.1.3. *Question 3: Evidence obtained through unlawful processing of data* ... *210*
8.2. Guidelines emerging from the analysis ... 213
9. EFFECTIVE DATA PROTECTION AND CONSUMER LAW: THE INTERSECTIONS 215

9.1. Introduction 215
9.2. Collective redress in data protection. The (possible) role of consumer protection associations 216
9.2.1. Collective redress in data protection and its comparison with consumer law 216
9.2.2. Question 1: The role of consumer protection associations in ensuring an effective data protection 217
9.2.3. The role of consumer associations in the field of data protection in light of new Directive EU, 2020/1828, on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, adopted on 25 November 2020222
9.3. Unfair commercial practices and information provided to the data subject 223
9.3.1. Question 2a: Unfair commercial practices and information provided to the data subject 224
9.3.2. Question 2b: Competent administrative authorities and their coordination 228
9.4. Information to be provided to the data subject, consumer rights directive, and unfair terms directive 231
9.4.1. Question 3: Unfair contractual terms and information provided to the data subject 231
9.4.2. Question 4: Relationship between information duties under the Consumer Rights Directive and the GDPR 235
9.4.3. Question 5: Relationship between the administrative and judicial authorities 236
9.4.4. Question 6: Lack of conformity of digital content or services and the GDPR compliance 237
9.5. Guidelines emerging from the analysis 240

9. Effective data protection and consumer law: the intersections

9.1. Introduction

Both the case law and EU legislation show the existence of areas of intersections between data and consumer protection. In this chapter the relationship between them is addressed assuming the data protection perspective. **The general question addressed is whether the application of consumer law can ensure the application of the right to an effective remedy (Article 47 CFR) and the right to data protection (Article 8. CFR),** where a natural person is to be qualified both as a consumer and as a data subject.

In this analysis, the fact that the number of data subjects who are not consumers in the online context is increasing should be taken into account. The relationship between users and online platforms is a good example: generally speaking, all users are data subjects *vis à vis* the online platform, but not all of them are consumers. Some of the data subjects cannot be qualified as consumers, but as professionals (e.g., a natural person sells for profit and in an organised manner tablecloths on an online platform, and personal data concerning her are processed by the online platform). The following table shows this relationship (without considering the relationship between users, not relevant for our purposes).

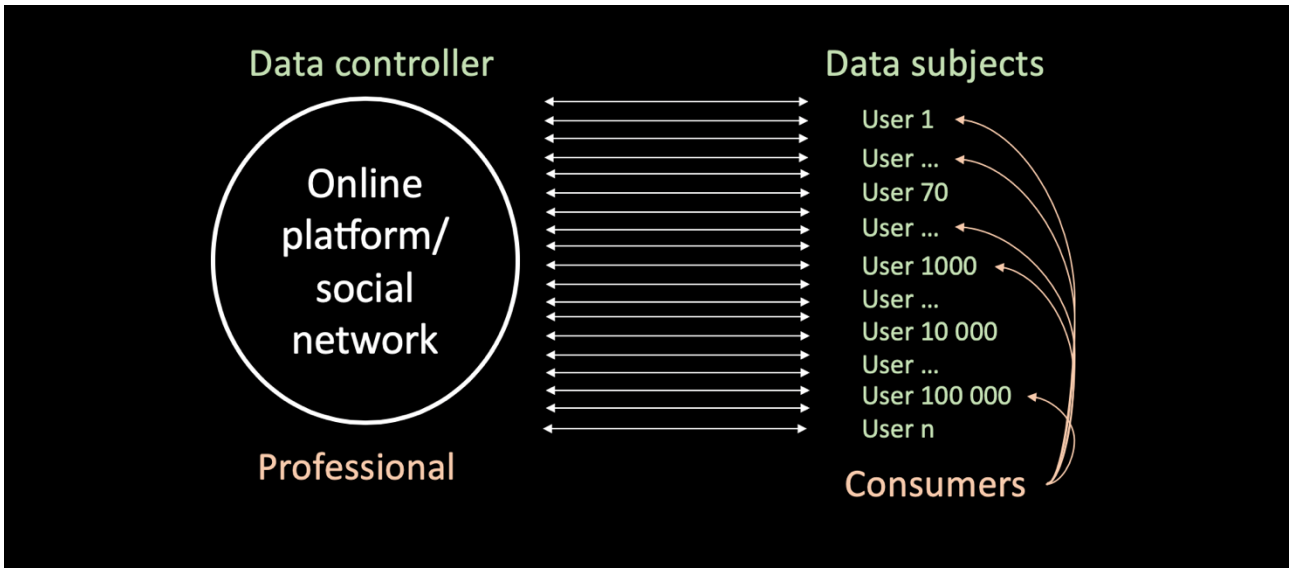

Figure 1. The interplay between the qualification of data subject and consumers in the relationship between natural persons and online platforms.

Main question addressed:

1. In light of the principle of effectiveness and of Article 47 CFREU and Article 8 CFR, can a consumer protection association seek an action in case of violations of data protection law?

1. A) Shall, in light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, the Unfair Commercial Practices Directive (2005/29) be applied in case of a **violation of the duty of information on data processing** provided by Articles 13 and 14 of the General Data Protection Regulation (2016/679)?

In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the Charter of Fundamental Rights, could the Unfair Commercial Practices Directive (2005/29) be **used to**

extensively interpret the duty of information provided in the General Data Protection Regulation (2016/679)?
b) Which authority **is competent**? How should authorities coordinate in light of principles of effectiveness, good administration and duty of cooperation?
2. In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, could the **UCTD** (93/13) (hereinafter UCTD), and the **Consumer Rights Directive** (2011/83) be applied in case of missing or wrongful information to be provided to the data subject?

3. In light of the principle of effectiveness, proportionality, equivalence, dissuasiveness and Article 47 of the CFR, what is the **relationship between the information duties provided in Articles 5 and 6 of the Consumer Rights Directive** (2011/83) and in **Articles 13 and 14 of the GDPR** (2016/679)? Could the information duties provided in the Consumer Rights Directive be interpreted, in certain cases, as covering also the ones of the GDPR? What are the consequences on remedies available under the Consumer Rights Directive?

4. In light of Articles 41 and 47 of the CFR, what is the relationship between the administrative authorities and judicial ones? Is there an impact of the principles of effectiveness, proportionality and dissuasiveness in organising the coordination between data protection authorities ascertaining a data protection violation and judicial authorities in proceedings concerning the ascertainment of a consumer law violation?

5. In light of the principle of effectiveness, dissuasiveness and of Article 47 and Article 8 CFR, could the consumer remedies against a lack of conformity of a digital content/service provided by Directive 2019/770 be used against a violation of data protection law?

9.2. Collective redress in data protection. The (possible) role of consumer protection associations

9.2.1. Collective redress in data protection and its comparison with consumer law

In the field of data protection, the GDPR repealed Directive 95/46/EC (the Data Protection Directive) and introduced a new collective redress mechanism. Article 80 GDPR introduced three new innovations for collective redress in the field of data protection: the data subject has the right to mandate a not-for-profit body (*opt-in*), organisation or association with regard to the protection of their personal data:
- to lodge the complaint on her behalf,
- to exercise on rights on their behalf
- to i) lodge a complaint with a supervisory authority (Article 77 GDPR), ii) an effective judicial remedy against a supervisory authority (Article 78 GDPR) iii) an effective judicial remedy against a controller or processor (Article 79 GDPR).

That not-for-profit body must
- have been properly constituted in accordance with the law of a Member State
- have statutory objectives which are in the public interest,
- be active in the field of the protection of data subjects' rights and freedoms

Furthermore, Article 80 GDPR states that Member States **may** provide that:
- the data subject has the right to mandate a not-for-profit body, organisation or association with the above mentioned characteristics to exercise the right to receive compensation referred to in Article 82 on her behalf (*opt-in*)

- any body, with the above mentioned characteristics independently of a data subject's mandate, has the right to lodge a complaint with the competent supervisory authority in that Member State,(Article 77 GDPR) and to exercise the rights to an effective judicial remedy against a supervisory authority (Article 78 GDPR) and against a controller or processor (Article 79 GDPR) if it considers that the rights of a data subject under this Regulation have been infringed as a result of the processing (*opt-out*).
However, the major weakness of this article is that it does not oblige Member States to act for providing an *opt-out* action. Member States are free to choose whether to implement such collective redress mechanisms in their national legislation. The initial Commission proposal included an obligation for Member States to provide for such a mechanism, but the Council amended the text to remove that obligation, despite the fact that the Parliament had approved it. The fact that Member States seem reluctant to implement collective redress mechanisms in general is reflected in their national legislations since, as explained below, only six of them adopted a functioning and efficient collective redress system (Belgium, France, Italy, Portugal, Spain and Sweden).[69]
Data subjects who are also consumers, are already taking advantage of this new possibility at national level. In **France,** consumer group UPF-Que Choisir brought a collective claim on 26 June 2019 before the *Tribunal de grande instance de Paris* (Tribunal of First Instance of Paris) to obtain an injunction against and claim compensation from Google for violation of the GDPR. The association wants to obtain an injunction against Google for stopping the illegal use by its Android system of the users' personal data and for obtaining their express consent before collecting and treating their data. The association claims a compensation of €1000 for any user of Google's Android system and who has a Google account. Consumers who believe their rights have been violated will be able to join the case once the first instance judge has decided on Google's liability.

9.2.2. Question 1: The role of consumer protection associations in ensuring an effective data protection

Relevant CJEU cases:

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

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

❖ Judgment of the Court (Third Chamber) of 22 of April 2022 and Opinion of Advocate General delivered on 2 December 2021, *Meta Platform Ireland Limited v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, Case C-319/20, ("**Meta Platforms Ireland Ltd**")

In light of the principle of effectiveness and of Article 47 CFREU and Article 8 CFR, can a consumer protection association seek an action in case of violations of data protection law?

The analysis is mainly based on the *Fashion ID* case (C-40/17).

The case

Fashion ID, an online clothing retailer, embedded the 'Like' social plugin from the social network Facebook ('the Facebook "Like" button') on its website. When a visitor consults the website of Fashion ID, that visitor's personal data are transmitted to Facebook Ireland as a result of that website including

[69] BEUC, *Why we need collective redress at EU level: a compelling collection of cases*, October 2019, accessible at: https://www.beuc.eu/publications/beuc-x-2019-062_why_we_need_collective_redress_at_eu_level.pdf.

that button. It seems that that transmission occurs without that visitor being aware of it regardless of whether or not they are a member of the social network Facebook or has clicked on the Facebook 'Like' button.
Verbraucherzentrale NRW, a public-service association tasked with safeguarding the interests of consumers, criticises Fashion ID for transmitting to Facebook Ireland personal data belonging to visitors to its website, first, without their consent and, second, in breach of the duties to inform set out in the provisions relating to the protection of personal data. Verbraucherzentrale NRW brought legal proceedings for an injunction before the Landgericht Düsseldorf (Regional Court, Düsseldorf, Germany) against Fashion ID to force it to stop that practice.
By decision of 9 March 2016, the Landgericht Düsseldorf (Regional Court, Düsseldorf) upheld in part the requests made by Verbraucherzentrale NRW, after having found that it has standing to bring proceedings under Paragraph 8(3)(3) of the UWG.
Fashion ID brought an appeal against that decision before the referring court, the Oberlandesgericht Düsseldorf (Higher Regional Court, Düsseldorf, Germany). The referring court asked the following question to the CJEU because it had doubts whether Directive 95/46 gave public-service associations the right to bring or defend legal proceedings in order to defend the interests of persons who have suffered harm.

Preliminary questions referred to the Court

(1) Do the rules in Articles 22, 23 and 24 of Directive [95/46] preclude national legislation which, in addition to the powers of intervention conferred on the data-protection authorities and the remedies available to the data subject, grants public-service associations the power to take action against the infringer in the event of an infringement in order to safeguard the interests of consumers?
By its first question the referring court asks, in essence, whether Articles 22 to 24 of Directive 95/46 must be interpreted as precluding national legislation which allows consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the laws protecting personal data.

Reasoning of the Court

As a preliminary point, the Court noted that, under Article 22 of Directive 95/46, Member States are required to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.
Article 28(3) of Directive 95/46 provides that the supervisory authority responsible for monitoring the application of the transposing measures within each Member State has the power to engage in legal proceedings where the national provisions adopted pursuant to that directive have been violated or to bring those violations to the attention of the judicial authorities.
However, no provision of that directive obliges Member States to provide, or expressly empowers them to provide, in their national law that an association can represent a data subject in legal proceedings or commence legal proceedings on its own initiative against the person allegedly responsible for an infringement of the laws protecting personal data.
Nevertheless, nothing in Directive 95/46 precludes national legislation allowing consumer-protection associations to bring or defend legal proceedings against the person allegedly responsible for such an infringement.
The Court then recalled that Member States are required, when transposing a directive, to ensure that it is fully effective in accordance with the objective which it seeks to attain, but they retain a broad discretion as to the choice of ways and means of ensuring that it is implemented. In this regard, one of the underlying objectives of Directive 95/46 is to ensure effective and complete protection of the fundamental rights

and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data.
The fact that a Member State provides in its national legislation that it is possible for a consumer protection association to commence legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data in no way undermines the objectives of that protection and, in fact, contributes to the realisation of those objectives.
Since Directive 95/46 lays down rules that are relatively general and have a degree of flexibility, Member States have a margin of discretion in implementing that directive. Although Article 22 of that directive requires Member States to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the personal data processing in question, that directive does not, however, contain any provisions specifically governing the conditions under which that remedy may be exercised. In addition, Article 24 of the directive provides that Member States are to adopt 'suitable measures' to ensure the full implementation of its provisions, without defining such measures.
The Court then explained that a provision making it possible for a consumer protection association to commence legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data may constitute a suitable measure, within the meaning of that provision, that contributes to the realisation of the objectives of that directive.
Finally, the fact that Regulation 2016/679 (the GDPR), which repealed and replaced Directive 95/46 and has been applicable since 25 May 2018, in Article 80(2) thereof, expressly authorises Member States to allow consumer-protection associations to bring or defend legal proceedings against a person who is allegedly responsible for an infringement of the laws protecting personal data does not mean that Member States could not grant them that right under Directive 95/46, but confirms, rather, that the interpretation of that directive in the present judgment reflects the will of the EU legislature.

Conclusion of the Court

Articles 22 to 24 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data must be interpreted as not precluding national legislation which allows consumer-protection associations to bring or defend legal proceedings against a person allegedly responsible for an infringement of the protection of personal data.

Impact on the follow-up case

The referring court (*Oberlandesgericht Düsseldorf*) still has to deliver its decision.

Elements of judicial dialogue

The ***Schrems II*** **case** (C-498/16) is also relevant to answer the question of whether a consumer protection association can seek an action in case of violations of data protection law.
In that case, the plaintiff (Mr Schrems) had founded an association which sought to uphold the fundamental right to data protection. Firstly, the qualification of the applicant as a consumer should be considered: in the *Schrems* case (C-498/16) the referring court asked the question whether, in order to apply Regulation No 44/2001, the activities of publishing books, lecturing, operating websites, fundraising and being assigned the claims of numerous consumers for the purpose of their enforcement do not entail the loss of a private Facebook account user's status as a 'consumer'. The CJEU, recalling its previous case law, stated that the concept of consumer is distinct from the knowledge and information that the person concerned actually possesses. Therefore, neither the expertise which that person may acquire in the field covered by those services nor his assurances given for the purposes of representing the rights and interests of the users of those services can deprive him of the status of a 'consumer' with regard to the application of Regulation No 44/2001.

However, the applicant brought the action against Facebook on the basis of his own rights and similar rights of seven other contractual partners of the defendant, who are also consumers in Austria, Germany and India. Austrian law indeed allows that one applicant brings different claims against the same defendant and that these claims be heard jointly in the same proceedings. The plaintiff claimed that the defendant had committed numerous infringements of data protection provisions. After his actions were dismissed by the lower courts, Mr Schrems brought an appeal before the *Oberster Gerichtshof* (Supreme Court, Austria), which referred a question to the CJEU.

In its question, the referring court asked, in essence, whether Article 16(1) of Regulation No 44/2001 (related to jurisdiction over consumer contracts) must be interpreted as meaning that it does not apply to the proceedings brought by a consumer for the purpose of asserting, in the courts of the place where he is domiciled, not only his own claims, but also claims assigned by other consumers domiciled in the same Member State, in other Member States or in non-member countries. In other words, as AG Bobek puts it in his opinion of the case, can Article 16(1) of Regulation No 44/2001 establish an additional special jurisdiction in the domicile of the assignee, thus effectively opening up the possibility of collecting consumer claims from around the world?

The Court did not depart from its settled case law and held that the assignment of claims cannot, in itself, have an impact on the determination of the court having jurisdiction. It follows that the jurisdiction of courts other than those expressly referred to by Regulation No 44/2001 cannot be established through the concentration of several claims in the person of a single applicant.[70]

By holding that the special rules of jurisdiction over consumer contracts do not allow consumers to seek redress jointly for their own claims and for claims assigned to them by consumers domiciled in the same Member State, in other Member States or in non-member countries, the Court interpreted Article 16(1) of Regulation 44/2001 strictly. Although the claim in these proceedings related to violations of data protection laws, the Court's conclusion applies to any claims related to consumer contracts.

While the Court in *Schrems* denied collective redress through the assignment of rights by consumers, it held in *Fashion ID* that Member States could allow consumer protection associations to seek redress for violation of data protection laws. Consequently, if Austria had allowed such claims by consumer protection associations and if Mr Schrems had filed suit with his association, it is likely that he would have had standing to bring those third-party claims as well. In any event, it is worth noting that the Court does not generally exclude the possibility of collective redress for violations of data protection provisions. However, the issue in *Schrems* was rather specific, as it concerned the assignment of rights by consumers to a single plaintiff (a possibility under Austrian law). Therefore, the Court did not hold that consumers victims of violations of data protection law cannot obtain collective redress, but rather that multiple plaintiffs cannot circumvent the European rules on international jurisdiction by concentrating their claims in the person of a single applicant.

Meanwhile, the GDPR entered into force and now provides in its Article 80 that data subjects have the right to mandate a not-for-profit body, organisation or association to lodge complaints and to exercise the right to receive compensation, where provided for by Member State law (see below). As explained below, the major drawback of Article 80 is that Member States are free to implement it or not, which leaves consumer protection associations upholding the fundamental right to data protection with unharmonised collective redress mechanisms in the EU.

Moreover, with regard to the application of Article 80 GDPR for protecting (also) economic interests, the case **C-319/20, *Meta Platforms Ireland Limited v Bundesverband der Verbraucherzentralen***

[70] On 28 February 2018, the Austrian Supreme Court upheld the Higher Regional Court's decision dismissing the appeal. Given the CJEU's preliminary ruling, the Austrian Supreme Court explained that the plaintiff could only rely on his personal claim and not on the other claims assigned to him. The Austrian Court did not depart from the CJEU's ruling and dealt with the issue rapidly.

und Verbraucherverbände is of particular interest. In this preliminary reference, the German Federal Court of Justice asked to the CJEU as to whether the rules in Chapter VIII of the GDPR, in particular in its Article 80 concerning collective redress, and Article 84 concerning sanctions preclude national rules which — alongside the powers of intervention of the supervisory authorities responsible for monitoring and enforcing the Regulation and the options for legal redress for data subjects — empower, on the one hand, competitors and, on the other, associations, entities and chambers entitled under national law, to bring proceedings for breaches of Regulation (EU) 2016/679, independently of the infringement of specific rights of individual data subjects and without being mandated to do so by a data subject, against the infringer before the civil courts on the basis of the prohibition of unfair commercial practices or breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions. In its **opinion** delivered **on 3 December 2021, the Advocate General**, relying, *inter alia,* on the principle of dissuasiveness (§65) affirmed that Article 80(2) GDPR must be interpreted as meaning that it does not preclude national legislation which allows consumer protection associations to bring legal proceedings against the person alleged to be responsible for the infringements of the protection of personal data, on the basis of the prohibition of unfair commercial practices, the infringement of a law relating to consumer protection or the prohibition of the use of invalid general terms and conditions, provided that the objective of the representative action in question is to ensure observance of the rights which the persons affected by the contested processing derive directly from that regulation.

The **CJEU, in its decision of 22 of April 2022**, stated that Article 80(2 GDPRP does not preclude national legislation which allows a consumer protection association to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects, against the person allegedly responsible for an infringement of the laws protecting personal data, on the basis of the infringement of the prohibition of unfair commercial practices, a breach of a consumer protection law or the prohibition of the use of invalid general terms and conditions, where the data processing concerned is liable to affect the rights that identified or identifiable natural persons derive from that regulation.

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

France

The decision of the Paris First Degree Court, of 9 April 2019 No 14/07298 is of particular interest. In that case, the association UNION FÉDÉRALE DES CONSOMMATEURS – QUE CHOISIR (hereinafter UFC – QUE CHOISIR) has brought an action before the Paris First Degree Court against Facebook for the purpose of establishing the unfair or unlawful nature of clauses in the platform's "General Terms and Conditions of Use" in the 2013, 2015 and 2016 versions, to have them deleted or deemed to be unwritten and to repair the damage caused to the collective interest of consumers. UFC QUE CHOISIR has requested that all the contractual conditions proposed by Facebook be declared abusive and illegal on its internal website with regard to the Consumer Code in particular Articles L 111-1, L. 211-1 and L. 212-1. The applicant argued that Facebook terms of use were not accessible, clear and understandable and did not comply with the provisions of the Law No. 78-17 of 6 January 1978 on information technology, data files and civil liberties.

In line with previous decisions (TGI Paris, 7 August 2018, No. 14/07300, UFC Que Choisir v. Twitter ; TGI Paris, 12 February 2019, No. 14/07224, UFC Que Choisir v. Google) and the recommendation on social networking contracts of the Commission on Unfair Terms, the qualification of a consumer contract was retained even though Facebook noted that social network access was free. Thus, the contract concluded between the company Facebook and the member of its social network is a consumer contract, subject to all the provisions of consumer law, subject only that the member does not use the network for professional purposes (CJEU 25 January 2018, C-498/16, Schrems). The Court applied consumer law

(see par. XX of this Chapter and condemned Facebook to pay 30 000 euros to the association UFC-QUE CHOISIR in compensation for the moral prejudice caused to the collective interest of consumers. (for further information on that case, see the FRiCoRe database at this link).

9.2.3. The role of consumer associations in the field of data protection in light of new Directive EU, 2020/1828, on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC, adopted on 25 November 2020

In the field of data protection, as explained above, Article 80 of the GDPR notably allows non-profit organisations to bring actions on behalf of data subjects whenever Member States provide for this possibility. However, as a study requested by the European Parliament's Committee on Legal Affairs duly noted, the article's "wording is rather unclear and by including a reference to national law, the EU legislator made it clear it was not ready to recognise a European collective action mechanism yet".[71]
Against this backdrop, on 11 April 2018, the European Commission published a legislative proposal for the adoption of a new directive on representative actions for the protection of the collective interests of consumers.[72] The new directive EU 2020/1828, on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC was adopted on 25 November 2020.
With regard to the role of consumer protection associations in the field of data protection, Article 2 of the directive states that:
"This Directive applies to representative actions brought against infringements by traders of the provisions of Union law referred to in Annex I, including such provisions as transposed into national law, that harm or may harm the collective interests of consumers".
Regulation UE 2016/679 and Directive 2002/58 are included in Annex I.
According to its recital 14, the directive should cover infringements of the provisions of EU law referred to in Annex I *to the extent that those provisions protect the interests of consumers*, regardless of whether those consumers are referred to as consumers, travellers, users, customers, retail investors, retail clients, **data subjects** or something else. **However, this Directive should only protect the interests of natural persons who have been harmed or may be harmed by those infringements if those persons are consumers under this Directive. Infringements that harm natural persons qualifying as traders under this Directive should not be covered by it** (see also recital 16).
Furthermore, according to Recital 15 the directive should be without prejudice to the legal acts listed in Annex I and therefore it should not change or extend the definitions laid down in those legal acts or replace any enforcement mechanism that those legal acts might contain. In addition, recital 15 of the directive expressly provides that *the enforcement mechanisms provided for in or based on Regulation (EU) 2016/679 (…) could, where applicable, still be used for the protection of the collective interests of consumers.*
The directive at certain extent encourages the role of consumer protection associations in data protection cases. The coordination between collective redress in consumer and data protection cases will be an important issue for Member States in the implementation of the new directive, also in light of Article 47, Article 8 CFREU and of the principle of effectiveness.

---

[71] Study requested by the JURI committee of the European Parliament, *Collective redress in the Member States of the European Union*, October 2018, p. 44, accessible at: http://www.europarl.europa.eu/RegData/etudes/STUD/2018/608829/IPOL_STU(2018)608829_EN.pdf.
[72] Proposal for a Directive of the European Parliament and of the Council on representative actions for the protection of the collective interests of consumers, and repealing Directive 2009/22/EC, COM/2018/0184 final - 2018/089 (COD). The Commission proposal was published on 11 April 2018.

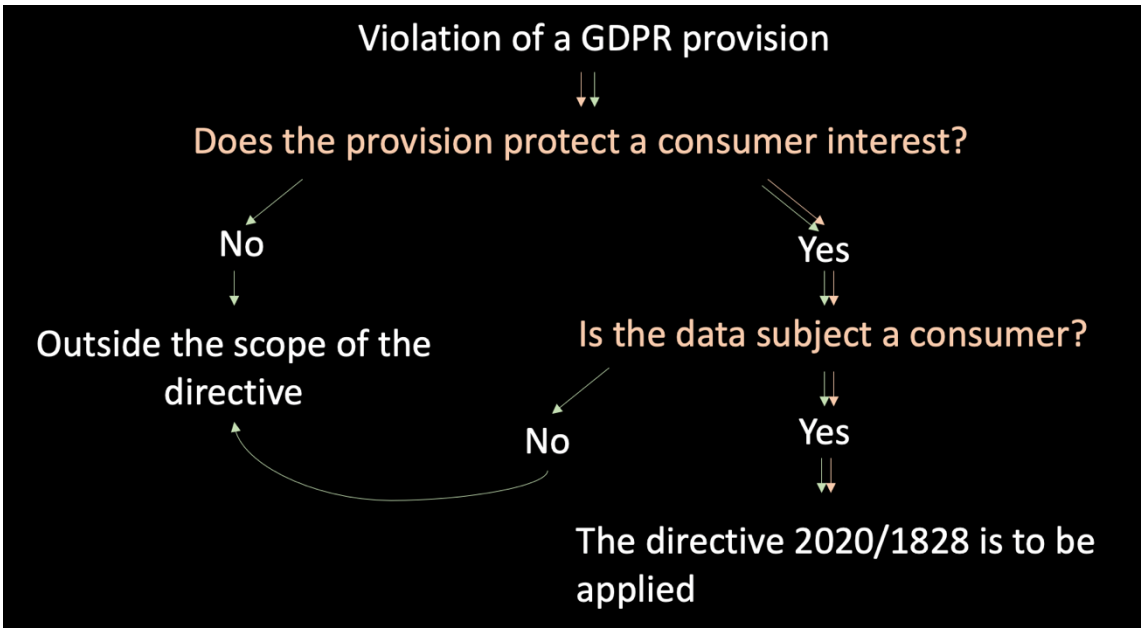

Fig. 2 The application of the directive in case of violations of data protection law

The directive creates a different protection against violations of data protection law if the infringed provisions are protecting also the interests of consumers, and the victims can be qualified as consumers. In this respect, the following question arises:

If the data subject is also a consumer, can Article 47 CFREU lead to a concurrence of remedies that combines data protection and consumer law remedies?

Furthermore, the comparison between the legislation on collective actions in consumer law and in data protection law shows that within the latter the collective redress system is less developed. In this respect, it should be noted that both the relationships between, on the one hand, the data subject and the data controller and on the other hand, the consumer and the professional, are characterized by an imbalance of power, although — at least partially — different in nature. The weaker position of the consumer *vis-à-vis* the seller or supplier, concerns the consumer's level of knowledge and her bargaining power (e.g., *Costea,* 3 September 2015, C-110/14; *Siba,* C-537/13, 15 January 2015; *Pouvin*, C-590/17, 21 March 2019; *Vapenik,* C-508/12, 5 December 2013). The data subject's weaker position is due at least to the knowledge concerning the data subject that the data controller acquires in processing data, and to the fact that the ways and timing of processing are put in place by the controller, with the consequence of an information asymmetry concerning the operations of processing.

9.3. Unfair commercial practices and information provided to the data subject

a. Shall, in light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, the Unfair Commercial Practices Directive (2005/29) be applied in case of a **violation of the duty of information on data processing** provided by Articles 13 and 14 of the General Data Protection Regulation (2016/679)? In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, could the Unfair Commercial Practices Directive (2005/29) be **used to interpret extensively the duty of information provided in the General Data Protection Regulation** (2016/679)?

b. Which authority **is competent**? How should authorities coordinate in light of principles of effectiveness, good administration and duty of cooperation?

Relevant national cases in cluster:

➢ Italian consumer protection Authority (Autorità Garante per la Concorrenza e il Mercato – AGCM), decision n° 26597, 11 May 2017, *Whatsapp-Trasferimento dati a Facebook*

➢ Italian consumer protection Authority (Autorità Garante per la Concorrenza e il Mercato – AGCM), decision n° 27432, 29 November 2018, *Facebook- condivisione dati con terzi*

➢ Administrative court (T.A.R.) of Rome, 10 January 2020, n. 260 (judicial review of Italian consumer protection Authority, decision n° 27432, 29 November 2018)

➢ Administrative court (T.A.R.) of Rome, 10 January 2020, n. 261 (judicial review of Italian consumer protection Authority, decision n° 27432, 29 November 2018)

➢ Council of State, decisions No. 2631 and 2630, 29 March 2021

Introduction: coordination and existence of parallel systems and authorities regulating the digital economy

Although unfair commercial practices linked to infringements of data protection laws are not limited to the digital economy, such practices frequently occur online. The most relevant cases do involve online platforms, online traders and connected objects. Digital markets are characterized by a lack of informed consent by data subjects, leading to a lack of transparency in the way their data are collected and processed. These characteristics lead to situations where a single conduct can potentially constitute infringements of data protection, consumer and/or competition law.

Another issue is to determine which regulator is competent to investigate and sanction infringements of data protection law that also constitute infringements of consumer law and potentially restrict competition on the market. In February 2019, the German Competition Authority (*Bundeskartellamt*) issued a decision against Facebook for abusing its dominant position on the German market for social networks, based on the extent of collecting, using and merging data in user accounts. Similarly, the Italian Competition Authority (*Autorità Garante della Concorrenza e del Mercato*), also in charge of consumer protection, fined WhatsApp in May 2017 for violating consumer law because it shared its users' personal data with Facebook and forced its users in accepting its new terms and conditions.

Both cases are discussed below as they involve conducts prohibited under a mix of consumer, data protection and/or competition law. These cases illustrate the existence of parallel systems and authorities regulating the digital economy. Each system has its own legal bases, goals, procedures and remedies. But can those systems overlap, and to what extent? This section will focus on the interplay between the General Data Protection Regulation (the ***GDPR***) and Directive 2005/49 (the ***Unfair Commercial Practices Directive***). In particular, it aims to answer the question whether violations of information duties provided by the GDPR can also constitute unfair commercial practices under the Unfair Commercial Practices Directive, and whether this directive could be used to interpret extensively the duty of information provided in the GDPR. This section also tries to determine which authority is competent, and how they should coordinate.

9.3.1. Question 2a: Unfair commercial practices and information provided to the data subject

In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, shall the Unfair Commercial Practices Directive (2005/29) be applied in case of a **violation of the duty of information on data processing** provided by Articles 13 and 14 of the General Data Protection Regulation (2016/679)?

In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, could the Unfair Commercial Practices Directive (2005/29) be **used to interpret extensively the duty of information provided in the General Data Protection Regulation** (2016/679)?

With regard to the question, there are no CJEU judgements. This sub-section will thus focus on EU legal instruments and on national cases in Italy and Germany.

EU law perspective

The European Commission **Guidance on the implementation/application of the Unfair Commercial Practices Directive**[73] provides that:

- A trader's violation of Data Protection rules will not, in itself, always mean that the practice is also in breach of Directive 2005/29, but such **data protection violations should be considered when assessing the overall unfairness of commercial practices**, particularly in the situation where the trader processes consumer data in violation of data protection requirements, (*i.e.,* for direct marketing purposes or any other commercial purposes like profiling, personal pricing or big data applications).
- Personal data, consumer preferences and other user generated content, have a "de facto" economic value. Depending on the circumstances, this could also be considered a violation of the EU data protection requirements to provide the required information to the individual concerned as to the purposes of the processing of the personal data.

Furthermore, the European Commission in the Guidance affirmed that:

"According to its Article 51(1), the EU Charter of fundamental rights applies to the Member States when they implement Union law, thus also when they implement the provisions of the UCPD. The Charter contains provisions, among others, on the **protection of personal data (Article 8)**, the rights of the child (Article 24), consumer protection (Article 38) and the **right to an effective remedy and a fair trial (Article 47)**. The Court has stressed the significance of Article 47 of the Charter on access to justice in relation to remedies available to consumers in connection with consumer rights granted under EU directives. **The principle of effectiveness**, as referred to by the Court, means that national rules of procedure may not make it excessively difficult or impossible in practice for consumers to exercise rights conferred by EU law."

The statement on the economic value of certain uses of personal data, such as the ones for commercial purposes should be coordinated with the impossibility of their qualification as "mere commodities". In this respect, **recital (24) of Directive 2019/770** states:

"Digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. (…) While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies".

According to the **EDPB' s Opinion 4/2017 on the Proposal for a Directive** on certain aspects concerning contracts for the supply of digital content, personal data cannot be regarded as a commodity. In this Opinion, the EDPB states:

"The EDPS warns against any new provision introducing the idea that people can pay with their data the same way as they do with money. Fundamental rights such as the right to the protection of personal data cannot be reduced to simple consumer interests, and personal data cannot be considered as a mere commodity".

[73] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016SC0163&from=IT

National case law

Italy

In two decisions the Italian consumer protection Authority (*Autorità Garante per la Concorrenza ed il Mercato,* hereinafter: ***AGCM***) has considered the conduct of professionals concerning the information of the data subject in light of Directive 2005/29 on unfair commercial practices.

In both **decisions** (dec. n° 27432, 29 November 2018 and n° 26597, 11 May 2017), the AGCM affirmed that **the unfair commercial practices discipline is to be applied** where **personal data** concerning Facebook's users acquire economic value because are **used for commercial purposes**, also in absence of a price payed for the commercial use of these data.

Furthermore, in the decision n° 27432, 29 November 2018 the AGCM considered:

a) as **a misleading commercial practice,** the professional's conduct consisting in not providing a clear, complete and immediate **information concerning his activity of collecting and using, for commercial purposes, the data of its users** during the first registration phase of the user on Facebook Platform. The AGCM considered that the information provided by Facebook is generic and incomplete and that it does not adequately distinguish between, on the one hand, the use of data for the customisation of the service with the aim of facilitating socialisation with other users ("consumers"), and on the other hand, the use of data to carry out targeted advertising campaigns. **The misleading character of the practice is aggravated by the circumstance that, in the use of Facebook, the commercial purposes are mixed and presented as confused with the social and cultural purposes typical of the social network.**

b) as an **aggressive commercial practice** the professional's conduct according to which the professional applies, in relation to its registered users, a mechanism that, through various steps, involves the **transmission of user data from the platform of the social network to third party websites/apps and *vice versa*,** without the prior express consent of the person concerned, for the use of the same for profiling and commercial purposes. In the case, the option available to the user to authorise or not this method is pre-set on the consent to the technical integration between Facebook and third party websites/apps (so-called "Platform activation"), which implies, by default, a generic predisposition to the reciprocal transmission (Facebook/third parties) of Facebook users' data, and users' right to opt-out. Moreover, Facebook affirms that the deactivation of the above mentioned integration produces for the users penalising consequences, both in the use of Facebook, and in the accessibility and use of third-party websites and apps**. <u>The AGCM considered that this practice, by means of undue influence, is to be considered suitable to considerably restrict the freedom of choice or conduct of the average consumer, thus inducing them to take a decision of a commercial nature that they would not otherwise have taken, in particular, the decision to integrate the functionalities of Facebook with those of third party websites/apps, including games, and to transfer, consequently, his data from Facebook to third parties and vice versa</u>**. According to the AGCM decision, the professional exercises undue influence over registered consumers, who, without express and prior consent, therefore unconsciously and automatically, suffer the transmission and use by Facebook/third parties, for commercial purposes, of the data concerning them (information deriving from the use of Facebook and from their own experience on third party websites and apps). Undue conditioning derives from the application of the pre-selection system of the widest consent to the transmission of one's own data from/to third parties, described above, together with the description of significant limitations in the usability of the social network and of the websites/apps of third parties due to the deselection of the transmission option.

With regard to **decision n° 26597, 11 May 2017**, the proceeding concerns WhatsApp's conduct towards its customers (consumer users), which has led users to accept in full the changes made to the Terms of Use of the WhatsApp Messenger application, which provided the option, pre-selected, of sharing certain personal data from their WhatsApp with Facebook for the company's use of such data for commercial

profiling and advertising purposes. In the event of non-acceptance of that changes, the information provided to the user/consumer suggested that the service would be discontinued. It should be noted also that for those who were already users of the application at the time of the update, WhatsApp allowed them to accept its contents even "partially". The existence of such an option was not represented in the main screen dedicated to the acceptance of the new Terms of Use. Only on the next screen, which was accessed by clicking on the link that referred to the reading of the Terms and Privacy Policy, the user would have realised that he had an alternative choice that was, however, pre-set, by checking in the box provided, to consent to the sharing of data. If the user had wanted to continue to use the application, without sharing their data with Facebook, he would have to uncheck the checkbox.

The commercial practice is qualified by the AGCM **as aggressive in that, through undue influence, it is likely to significantly restrict the average consumer's freedom of choice or conduct, thereby causing him to take a transactional decision that he would not have taken otherwise**. This undue influence stems from the fact that WhatsApp Messenger users were in fact forced to accept the new contractual terms in full, in particular with regard to the sharing of data with Facebook, making them believe that it would otherwise have been impossible to continue using the application where those who were already users at the date of the amendment of the Terms, instead, had the opportunity to "partially" accept its contents.

In July 2019 the **Italian consumer protection Authority (AGCM), the Italian Data protection Authority (GPDP) and the Media Authority (AGCOM) issued a joint statement "Big Data. Joint Investigation, Guidelines and Policy Recommendations"**, in which they elaborated some shared guidelines and policies, which states that it is necessary (point n. 10):

"To strengthen the powers of AGCM and AGCom to acquire information outside the investigation procedures and to increase the maximum level of sanctions in order to ensure an effective deterrent effect of the consumer protection rules".

In this respect the Authorities affirm that **consumer protection** can affect a variety of profiles related to the relationship between operators and users in the acquisition, processing and processing of data. According to that statement, the fact that the **legislation on the protection of personal data** is applicable to the conduct of companies does not exempt them from complying with the rules **on unfair commercial practices**; **the two disciplines are seen as complementary and not alternative**. The authorities considered that consumer protection and privacy protection are undoubtedly important components of a fair competition.

The **Italian administrative court of Rome in the judgement n. 260, 10 January 2020**, which constitute the judicial review of the AGCM decision n° 27432/2018, stated that the economic value of person data of the users requires the professional to inform the consumer that the information obtained from such data will be used for commercial purposes that go beyond its use in the "social network". The practice may be qualified as misleading in case of lack of adequate information, or in the case of misleading statements. In the present case, the court confirmed the AGCM's decision, stating that the claim used by Facebook in the registration page in order to encourage users to subscribe ("Subscribe. It's free and it will be forever") suggested the absence of a counter-performance required from the consumer in exchange for the use of the service. Therefore, according to the court's judgement, the practice is to be sanctioned because of the incompleteness of the information provided, where the claim of gratuitousness of the service did not allow the consumer to understand that the professional would use the users data for remunerative and commercial purposes.

The Council of State, in its decisions no. 2631 and 2630 of 29 March 2021 confirmed the decision of the Tribunal. In its reasoning, the Council of State considered that the special EU discipline of personal data protection has a very broad scope also due to the broad concept of "processing" (Article 4 GDPR), but that the application of data protection rules does not exclude the application of other disciplines, such as consumer law. Therefore, according to the Council of State, there is not a principle of the

speciality of data protection law that excludes the application of other provisions. In this vein, the Council of State considered that when the processing involves behaviours and situations regulated by other legal sources for the protection of other values and interests, the legal system — first at EU level and then at a national level — cannot exclude the application of other sectoral disciplines, such as that of consumer protection, to reduce the protection guaranteed to natural persons. Accordingly, the Council of State affirmed the need to ensure "multi-level protections" that can enhance the protection of individuals' rights. As to the merit of the case, the Council of State affirmed that in the present case is not at stake the commercialisation of personal data by the data subject, but the exploitation of personal data made available by the data subject in favor of a third party who will use it for commercial purposes, without the data subject is fully aware of the data uses.
Considering the above mentioned litigation, in light of the principle of effectiveness and dissuasiveness, the following questions can be raised:

In light of Article 47 of the CFR, when there is a violation of data protection law and the conduct is qualified also as a commercial practice, taking into account Article 8 of the CFR, what are the cases in which the practice is not to be considered unfair? Could a decision of the Data Protection Authority declaring a violation of data protection rules be relevant in the Consumer Authority's assessment concerning the existence of an unfair practice? If so, is it decisive in that assessment?

The application of unfair commercial practices directive could lead to focus on the importance of the information related to the use of personal data for profit also in the interpretation of the information duties of the data controller (Article 13 GDPR). In this respect,

In light of Article 8 and 47 CFR, could an extensive interpretation of Article 13 GDPR, including the duty to inform about the commercial and remunerative use of personal data be applied where the data subject is not a consumer?

9.3.2. Question 2b: Competent administrative authorities and their coordination

National cases

Italy
The consumer protection authority examined the question of its **competence** in the decisions 27432, 29 November 2018 n° 26597, 11 May 2017. The AGCM affirmed that the data protection and the commercial practices disciplines have different material scopes and pursue different interests. As a result, the Authority affirmed that there is no conflict between the two disciplines, but rather they are complementary. On this ground the authority stated that the conducts analysed in the proceeding are considered in light of the unfair commercial practices' rules. Therefore, the Italian consumer protection Authority affirmed its competence.
It should be noted that in both proceedings (related to decisions 27432, 29 November 2018 and decision n° 26597, 11 May 2017) the Italian consumer protection Authority required an **opinion to the Italian media Agency** (*Autorità per le Garanzie nelle Comunicazioni*, AGCOM), in accordance with **Article 27(6) consumer code**, which states that when a commercial practice has been or is intended to be disseminated in the periodical or daily press, or by radio or television or any other telecommunications medium, before issuing a decision, the consumer protection Authority shall request the opinion of the Communications Regulatory Authority.
In July 2019 the **Italian consumer protection Authority (AGCM), the Italian Data protection Authority (GPDP) and the Media Authority (AGCOM) issued a joint statement titled "Big Data. Joint Investigation, Guidelines and Policy Recommendations"**, in which they elaborated some

shared guidelines and policies, and according to which (point n° 11) **it is necessary to create a permanent coordination between the three authorities.** In particular, the authorities considered that:
"The challenges posed by the development of the digital economy and Big Data require full use to be made of the synergies between ex ante and ex post instruments for protecting privacy, competition, consumers and pluralism.
AGCM, AGCom and the GPDP, each within their own sphere of competence, can best guarantee their own institutional objectives, insofar as they will be able to take full advantage of the opportunities offered by fruitful cooperation.
To this end, the three Authorities, in the exercise of the complementary competences assigned to them and which contribute to tackling the critical issues of the digital economy, are committed to close forms of collaboration in interventions that affect the digital markets, including through the signing of a memorandum of understanding."

The Authorities considered also that in order to allow a full understanding of the new phenomena in the digital economy, it seems appropriate to strengthen the powers of acquisition of information by AGCM and AGCOM outside the investigative procedures (investigations, pre-instructive activities), including the possibility to impose administrative sanctions in case of refusal or delay in providing the information.
In the judgment of the **Italian administrative court of Rome n. 260, 10 January 2020**, which constitutes the judicial review of the AGCM decision 27432/2018, the court addressed the question of the consumer protection authority's competence, which was denied by the claimant. In this respect, the court stated that the plaintiff's arguments presuppose that the protection of personal data only concerns fundamental rights. The national court considered that this approach does not take into account the economic value of personal data. The court stated that personal data are to be protected as an expression of an individual's right to privacy, and as such subject to specific and not renounceable forms of protection, such as the right to revoke consent, access, rectification, erasure.
In the court's view, a different kind of protection of personal data is to be developed, because of the economic value of personal data. The court affirmed that the existence of an economic value of the personal data, typical of the new economies of the digital markets, requires the operators to respect, in the relative commercial transactions, those obligations of clarity, completeness and not deceptiveness of the information provided for by the legislation for the protection of the consumer, which must be made aware of the exchange which is related to the adhesion to a contract for the fruition of a service, such as the use of a "social network". The court recalled the *Guidance on the implementation/application of directive 2005/29/ec on unfair commercial practices* released by the EU Commission on 25 Mary 2016, where the economic value of personal data and the possible relevance of Directive 2005/29 is affirmed.
Moreover, the Italian administrative court stated that the omission of information about the exploitation for commercial purposes of user data is not a matter entirely regulated and sanctioned within data protection law. The court recalled also *Wind Tre* (C-54 and C-55/17), concerning the coordination among multiple administrative bodies competent in relation to the same conduct.
Then, according to the court, in the present case there is no incompatibility or antinomy between the provisions of data protection and consumer law, since they are complementary, imposing, in relation to the respective purposes of protection, specific information obligations, in one case functional to the protection of personal data, understood as a fundamental right, and in the other to the correct information to be provided to the consumer in order to allow her to make an informed economic choice.
Furthermore, the court highlights that there is no risk of over-deterrence consisting in a double sanction for the same conduct, considering that the object of investigation by the competent authorities concerns different conduct of the operator, the correct processing of personal data and the clarity and completeness of the information about the exploitation of the data for commercial purposes

Similar arguments and the same conclusion were adopted by the **administrative court of Rome in the judgment 10 January 2020, n. 261**.

Germany

On 6 February 2019, the German Competition Authority (*Bundeskartellamt*), which was also granted competences in the area of consumer protection, issued a decision against Facebook for abusing its dominant position on the German market for social networks, based on violations of data protection law. In its summary of the decision,[74] the Authority explains that the GDPR does not rule out the possibility for authorities other than the national data protection authorities (including competition and/or consumer protection authorities) to apply substantive data protection law.

The Authority also explains that the GDPR explicitly states that data protection law can also be enforced under civil law, i.e., that full consistency is not aspired to. More importantly, the Authority explains that:

"This applies in particular to consumer protection organisations and competitors and their associations. These entities can enforce data protection based on stipulations of the Act Against Unfair Competition (UWG) or regulations on business terms linked to data protection and also based on Section 19 GWB. A large part of the ECJ's case law which data protection authorities and the data protection board have to consider has been obtained from civil law proceedings. Civil law proceedings promote rather than threaten the consistent implementation of data protection law, especially as the ECJ can be involved at an early stage as part of the preliminary ruling procedure".

The *Bundeskartellamt* explained that, in the course of its proceedings against Facebook, it maintained regular contact with data protection authorities, none of which considered they had exclusive competence. This is consistent with the approach taken by the Italian competition, data protection and telecom authorities in their joint statement.

EU law perspective

The AGCM decision fining WhatsApp for data transfer to Facebook of May 2017 came three years after the European Commission approved the merger between the two companies.[75] In its merger decision, the Commission had concluded that the merged entity would be unable to establish reliable automated matching between Facebook users' accounts and WhatsApp users' accounts. However, in August 2016, WhatsApp announced updates to its terms of service and privacy policy, including the possibility of linking WhatsApp users' phone numbers with Facebook users' identities. This led the Commission to fine Facebook €110 million for providing misleading information during the merger process.[76]

Therefore, the Italian authority issued a decision against WhatsApp based on consumer law, but the problem originates in the Commission's decision not to oppose to the merger. The Commission has been criticised for not taking enough into account data protection concerns in its review of the merger. In its decision, the Commission indeed stated that:

"For the purposes of this decision, the Commission has analysed potential data concentration only to the extent that it is likely to strengthen Facebook's position in the online advertising market or in any sub-segments thereof. Any privacy-related concerns flowing from the increased concentration of data within the control of Facebook as a result of the Transaction do not fall within the scope of the EU competition law rules but within the scope of the EU data protection rules".

---

[74] https://www.bundeskartellamt.de/SharedDocs/Entscheidung/EN/Fallberichte/Missbrauchsaufsicht/2019/B6-22-16.pdf?__blob=publicationFile&v=3

[75] European Commission, Case COMP/M.7217 Facebook/Whatsapp 3 October 2014.

[76] https://ec.europa.eu/commission/presscorner/detail/en/IP_17_1369

The Commission's decision suggests that it has not coordinated its investigation with national data or consumer protection authorities. This suggests that there is the need of more coordination between the different national and European authorities in the field of consumer, data protection and competition enforcement. In this respect, the following question arises:

In light of the principles of effectiveness and good administration, is it necessary to provide a system of coordination between data protection and consumer authorities at national and European level? Could the documents and the investigations made by an authority be used in proceedings of another authority?

9.4. Information to be provided to the data subject, consumer rights directive, and unfair terms directive

Main questions addressed

3. In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, could the **UCTD** (93/13) and the **Consumer Rights Directive** (2011/83) be applied in case of missing or wrongful information to be provided to the data subject? 4. In light of the principle of effectiveness, proportionality, equivalence, dissuasiveness and Article 47 of the CFR, what is the **relationship between the information duties provided in Articles 5 and 6 of the Consumer Rights Directive** (2011/83) and in **Articles 13 and 14 of the General Data Protection Regulation** (2016/679)? Could the information duties provided in the Consumer Rights Directive be interpreted, in certain cases, as covering also the ones of the GDPR? What are the consequences on remedies available under the Consumer Rights Directive? 5. In light of Articles 41 and 47 of the CFR, what is the relationship between the administrative authorities and judicial ones?

Relevant national cases in cluster:

- LG Berlin, 30/04/2013, (2013) Neue Juristische Wochenschrift 2605, 2606 – Apple
- LG Berlin, 19/11/2013, (2014) MultiMedia und Recht 563, 565 – Google
- LG Frankfurt a.M., 10/06/2016, (2016) Beck Rechtsprechung (BeckRS) 10907 – Samsung

9.4.1. Question 3: Unfair contractual terms and information provided to the data subject

In light of the principles of effectiveness, proportionality, dissuasiveness, and of Article 47 of the CFR, could the **UCTD** (93/13) and the **Consumer Rights Directive** (2011/83) be applied in case of missing or wrongful information to be provided to the data subject?

With regards to this question, there are no European cases. This sub-section with thus focus on German cases.

National case law

Germany

On **30 April 2013**, the **Landgericht Berlin** (District Court of Berlin) issued a decision against **Apple**.[77] The plaintiff is a consumer protection association and requests an injunction against non-transparent clauses of the defendant's terms and conditions. The defendant sells computer hardware and communication devices. They also operate a telemedia service which is available in German at 'www.apple.com/de'. On this website, the defendant publishes their terms and conditions as well as their 'Apple privacy policy'. The plaintiff regards clauses of the privacy policy and the terms and conditions as problematic under §307 BGB and requests an injunction against their use.

[77] Registration No. 15 O 92/12.

The district court held that the clauses of a privacy policy also constitute terms and conditions. Under §305 German Civil Code, terms and conditions are pre-formulated conditions for numerous contracts which one party stipulates to the other. On the basis of the presentation of the privacy policy as part of the order process (as one click-wrapping option with the terms and conditions), the court adopted the least consumer-friendly interpretation of that clause. It held that consumers would assume the privacy policy to be part of the terms and conditions of the order. Consequently, the privacy policy forms part of the terms and conditions and is subject to the same control.

On **19 November 2013**, the **Landgericht Berlin** (District Court of Berlin) issued a decision against **Google**.[78] The defendant offers numerous services on their website, i.e., a well-known internet search engine, specialised search engines for images, maps, books, movies, e-mail and calendar services. Many of these services can be used without registration and free of charge, whereas some services (i.e., the email service) require registration and some are chargeable.

The plaintiff, a registered consumer protection association, first successfully requested an injunction regarding the terms of use and its privacy policy against the defendant in 2008.[79] In the current case, the plaintiff requests an injunction against the defendant's updated Terms of Use and privacy policy (used on the website in July 2012).

One of the issues dealt with by the District Court of Berlin is the extent of the possibility to control privacy policies and terms of services, and whether certain clauses of the terms and conditions are void.

First, the court decides that the defendant's terms of use and privacy policy constitute terms and conditions and are, thus, subject to the same level of control. It is decisive that the defendant's conditions of contract are pre-formulated for a multitude of contracts and stipulated in a one-sided manner. Adopting the least consumer friendly interpretation of the website, the privacy policy is included in the analysis as it is impossible to sign up for the defendant's services without consenting to it and the terms of use through a single click-wrapping link. Consequently, the terms of use and the privacy policy constitute terms and conditions. In addition, the defendant's services do not constitute 'gifts' but a reciprocal relationship as the defendant makes use of collected information in exchange for the offered services.

Second, the court determines several clauses of the defendant's terms and conditions void. Regarding the terms and conditions, the court determines that the clauses are worded too broadly and that some clauses are too one-sided. For example, it is unclear to the consumer how the defendant examines the uploaded content and what constitutes infringements, because the clauses are worded too broadly and do not contain restrictions regarding conduct entailing criminal responsibility. The defendant also assumes continuing obligations although it needs to be possible to terminate the relationship in case of misconduct of either party. The privacy policy is similarly void as the consumer cannot understand from it in which ways his data is processed. Lastly, the clauses regarding 'android market' are illegal as far as the defendant is authorised to access the devices owned by the consumer, to unilaterally change the conditions of the contract and to terminate the use of services. Therefore, the court stresses that it does not matter whether the clauses are currently in use. Due to the abstract danger of re-offending, an official court injunction is necessary.

On **10 June 2016**, the **Landgericht Frankfurt** (District Court of Frankfurt) issued a decision against **Samsung Electronics**.[80] The plaintiff is the consumer protection association of North Rhine-Westphalia. It acquired a 'smart TV' produced by the defendant Samsung Electronics. These smart TVs feature the user surface 'Smart Hub' where the consumer can access third party applications, but also upload their own movies and receive recommendations regarding the TV programme. In the assembly

[78] Registration No. 15 O 402/12.

[79] LG Hamburg, judgment of 19.05.2011 - 10 U 32/09.

[80] Registration No. 2-03 O 364/15.

instructions, there was neither reference to the terms and conditions, nor to the privacy policy. The terms and conditions related to the privacy policy could be accessed after the assembly of the TV. During the first use of the TV, the TV uses the consumer's IP address to download and present the terms and conditions, as well as the appropriate privacy policy according to the region of the plaintiff. The plaintiff can then read the terms and conditions and the privacy policy displayed without sub-sections or headings, and then issue a blanket approval regarding them. The plaintiff complains that the HbbTV function was activated without the consent of the consumer, and that this function transfers data to the producer without previously informing or obtaining the consumer's consent.
Addressing the points raised by the plaintiff, the district court Frankfurt concludes that there is no duty for the defendant to inform the consumer about the activated HbbTV function, and the possible transfer of information. While this function transmits IP-addresses, §13(1) TMG is aimed at service providers who use data collected during the provision of the service. The defendant is not in a position where they have active knowledge of the data or the authority to dispose about the collected data, hence, §13(1) TMG is not applicable to the defendant.
While the district court Frankfurt addresses the points raised by the plaintiff, its focus is on controlling the terms and conditions, including therein also the privacy policy without explicit discussion. The district court raises this issue on its own motion and decides that the privacy policy lacks transparency. Due to its length and unclear presentation (56 TV pages in running text without sections or headings), the district court finds that the privacy policy is not a suitable basis for agreeing to the collection and use of data. Furthermore, the court does not deem the phrasing of the privacy policy suitable. The provider has to inform the consumer at the beginning of the use of the product, regarding the form, extent and purpose of collecting and using the data in an understandable manner.
Therefore, it is necessary to inform the consumer of which kind of data is collected. By using phrases including 'for example' and 'possibly' regarding the used data, the provider does not present an exhaustive list of what kind of data is collected and the consumer cannot validly agree.

France
The decision of the Paris First Degree Court, of 9 April 2019 No 14/07298 is of particular interest. In that decision, the Paris Hight Court noted that "by collecting data submitted free of charge by the user when accessing the platform and by marketing them for a fee, the company Facebook, which, acting for commercial purposes, makes a profit from its activity, is a professional within the meaning of the introductory article of the Consumer Code" (TGI Paris, 7 August 2018, No. 14/07300, UFC Que Choisir v. Twitter; TGI Paris, 12 February 2019, n°14/07224, UFC Que Choisir c/ Google). Thus, the Court affirmed that the contract concluded between the company Facebook and the member of its social network is a consumer contract, subject to all the provisions of consumer law, subject only that the member does not use the network for professional purposes (CJEU 25 January 2018, C-498/16, Schrems). French consumer law and the regulations relating to distance contracts, consumer information, unfair terms, form and interpretation of the contract are applicable. The relevant clauses relating to the definition of the purpose of the service provided by the company Facebook can be assessed on the basis of the regulations on unfair terms.
Two articles of the Consumer Code were used to support the judges' reasoning. Article L. 211-1 imposing an obligation of clarity in the drafting of clauses, which implies in particular the use of French, and Article L. 111-1 imposing a general obligation of pre-contractual information. The underlying idea was that the social network can neither collect nor share the personal data of its users without having clearly informed them about the economic value of their data, just as it can neither suggest that its social network is disinterested, nor suspend/delete an account without justification or recourse, nor modify the general conditions without the users' information or agreement, nor exclude any liability on its part. The judges also relied on the Law No. 78-17 of 6 January 1978 on information technology, data files and civil liberties

and justified its application with regard to Article 4§1(a) of the Directive 95/46/CE and to Article 5 1° of the referred Law No. 78-17. Indeed, the simultaneous display on the home page of the Facebook social network site of the user's personal data (surname, first name, date of birth) and advertisements related to the user's activities on the internet confirm that the sale of advertising space, conducted by the company Facebook, the data controller's establishment on French territory, constitutes processing of personal data within the meaning of Article 2(b) of Directive 95/46/EC and Article 2 of the Law No. 78-17 of 6 January 1978. The judges have used the Law No. 78-17 of 6 January 1978 in order to assess the illegality of the clauses and thus forbid the social network to use for free or to resell without time limit the contents created by its users, to indefinitely keep the data of its users even after the deletion of their account, or to remove a published content without warning its author.
Facebook has been convicted by the Paris First Degree Court for having inserted 430 abusive or illegal clauses in the Terms and Conditions of its social network with regard to Articles 6, 32-I, 32-II, 32-II of the Law No. 78-17 of 6 January 1978 on information technology, data files and civil liberties, the law of 4 August 1994, and article L. 211-1 of the French Consumer Code. They will therefore be deemed to be unwritten. Moreover, the judges order Facebook to allow all of its French members to read the entirety of this judgment by means of a hypertext link in an exclusively dedicated banner that must appear on the home page of its Internet site as well as on those of its tablet and telephone applications for a period of three months (for further information on that case, see the FRiCoRe database at this link).

EU law perspective

Article 3(1) of the ***UCTD*** provides that terms that have not been negotiated individually should be considered as unfair "if it causes a significant imbalance in the parties' rights and obligations arising under the contract". This provision leaves courts the possibility to consider if violations of information requirements under the GDPR cause a significant imbalance in the parties' rights and obligations.
Nevertheless, **in case of conflict between the UCTD and the GDPR**, the latter should be considered the *lex specialis* because it regulates the specific sector of data protection. Indeed, one could argue that Recital 42 of the GDPR provides indications on how to apply the UCTD in the area of data protection, (and therefore has *lex specialis* value) by providing that, "in accordance with Council Directive 93/13/EEC a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment".
In July 2019, the Commission adopted a **Guidance Notice on the interpretation and application of the UCTD**.[81] The Guidance is remarkably silent about the interplay of transparency requirements under the directive and similar information duties under data protection provisions. However, concerning the interplay of transparency requirements under the directive and those in other EU instruments in general, the Guidance provides the following:

- "Where other EU provisions apply in addition to the UCTD, one will, in general, favour an interpretation that preserves as much as possible the *effet utile* of the UCTD and of a potentially conflicting provision. For instance, rules of procedure should not jeopardise the effectiveness of the protection against unfair contract terms under the UCTD" (p. 16).
- "Various EU acts regulate in a detailed fashion the pre-contractual information that traders have to provide to consumers in general or with regard to specific kinds of contracts. […] The UCTD is

[81] Commission notice — Guidance on the interpretation and application of Council Directive 93/13/EEC on unfair terms in consumer contracts, OJ C 323, 27.9.2019, pp. 4–92.

without prejudice to such provisions and the consequences of the failure to comply with them as set out in such specific instruments" (p.28).

- "Insofar as specific pre-contractual and contractual information requirements apply, they will also have to be taken into account for the transparency requirements under the UCTD, on a case-by-case basis, and in light of the purpose and scope of those instruments" (p. 28).
- "The fact of whether a seller or supplier has complied with sector-specific requirements is an important element when assessing compliance with the transparency requirements under the UCTD. However, given the parallel applicability of the UCTD with sectorial legislation, compliance with such instruments does not automatically indicate compliance with all transparency requirements under the UCTD" (p. 29).

Since this guidance was published after the entry into force of the GDPR, it is reasonable to assume that the Commission foresaw the interaction of then transparency requirements provided for in the UCTD and the GDPR when drafting these guidelines.

Regarding the relationship between information duties under the Consumer Rights Directive and the GDPR, see Section 9.4.2 below.

9.4.2. Question 4: Relationship between information duties under the Consumer Rights Directive and the GDPR

In light of the principle of effectiveness, proportionality, equivalence, dissuasiveness and Article 47 of the CFR, what is the **relationship between the information duties provided in Articles 5 and 6 of the Consumer Rights Directive** (2011/83) and in **Articles 13 and 14 of the GDPR**? Could the information duties provided in the Consumer Rights Directive be interpreted, in certain cases, as covering also the ones of the GDPR? What are the consequences on remedies available under the Consumer Rights Directive?

EU law perspective

In this area, the principle *lex specialis derogat legi generali* is confirmed by Article 3(2) of the **Consumer Rights Directive**, which provides that in case of conflict with another Union act governing specific sectors, the provision of that other Union act shall prevail and shall apply to those specific sectors.

In June 2014, the Commission adopted a **Guidance document concerning the Consumer Rights Directive.** This guidance states that, in case of conflicts about information requirements provided for in Directive 95/46/EC (the Data Protection Directive) or Directive 2002/58/EC (the ePrivacy Directive), these sector-specific requirements prevail. This is especially relevant in online sales for issues such as information about data processing and data subjects' consent to the tracking and use of personal data supplied. By extension, this could also hold true for the GDPR. Therefore, information duties from both the Consumer Rights Directive and the GDPR apply in parallel, but the ones from the latter prevail in case of conflict. This is consistent with the fact that the GDPR contains more detailed transparency requirements than the Consumer Rights Directive.

It is true that both consumer protection and data protection share **common purposes**, such as the free moments of goods and services in the internal market, transparency and fair treatment.

In that regard, it should be recalled that the under Article 13 of Directive 2011/83, as modified by Directive 2019/2161, that directive applies where the trader supplies or undertakes to supply digital content which is not supplied on a tangible medium or a digital service to the consumer and the consumer provides or undertakes to provide personal data to the trader, except where the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content which is not supplied on a tangible medium or digital service or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose.

Furthermore, according to Article 6 of Directive 2011/83, as modified by Directive 2019/2161, before the consumer is bound by a distance or off-premises contract, or any corresponding offer, the trader shall provide the consumer with the information in a clear and comprehensible concerning, where applicable, that the price was personalised on the basis of automated decision-making. This provision may contribute to ensuring the effectiveness of data protection, by reinforcing information duties provided within data protection legislation.
Hence, the **remedies** available under the Consumer Rights Directive cannot be used against violations of information duties provided in the GDPR alone. Violations of information duties under the GDPR can only be remedied with the Consumer Rights Directive if they also constitute violations of information requirements under that directive.

9.4.3. Question 5: Relationship between the administrative and judicial authorities

In light of Articles 41 and 47 of the CFR, what is the **relationship between the administrative authorities and judicial ones**?

This question aims at analysing the possible impact of an administrative decision issued by a data protection authority which ascertains a data protection violation on a judicial proceeding concerning the ascertainment of a consumer law violation. In this respect, the new directive 2020/1828, on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC was adopted on 25 November 2020, and the new **Directive on the better enforcement and modernisation of Union consumer protection rules** should be considered.

EU law perspective

As explained in Section 9.1.2, Directive EU 2020/1828, on representative actions for the protection of the collective interests of consumers and repealing Directive 2009/22/EC was adopted on 25 November 2020. With this new directive, the EU legislator set out rules to ensure that representative actions aimed at the protection of the collective interests of consumers are available in all Member States.
It should first be noted that the directive allows Member States to decide whether the representative action can be brought in judicial or administrative proceedings. Recital 19 of Directive 2020/1828 provides:
"Since both judicial proceedings and administrative proceedings could effectively and efficiently serve to protect the collective interests of consumers, it is left to the discretion of the Member States whether a representative action can be brought in judicial proceedings, administrative proceedings, or both, depending on the relevant area of law or the relevant economic sector**. This should be without prejudice to the right to an effective remedy under Article 47 of the Charter, whereby Member States are to ensure that consumers and traders have the right to an effective remedy before a court or tribunal, against any administrative decision taken pursuant to national measures transposing this Directive. This should include the possibility for a party in an action to obtain a decision ordering the suspension of the enforcement of the disputed decision, in accordance with national law.**"
The directive further deals with the coordination between administrative and judicial authorities. In particular, Article 15 of Directive 2020/1828 states:
"Member States shall ensure that the final decision of a court or administrative authority of any Member State concerning the existence of an infringement harming collective interests of consumers can be used by all parties as evidence in the context of any other action before their national courts or administrative authorities to seek redress measures against the same trader for the same practice, in accordance with national law on evaluation of evidence.".

On 27 November 2019, the European Parliament and the Council also adopted the new **Directive on the better enforcement and modernisation of Union consumer protection rules**, 2161/2019. The amending directive modernises Directive 2005/29/EC (unfair commercial practices), Directive 93/13/EEC (unfair contract terms), Directive 2011/83/EU (consumer rights) and Directives 98/6/EC (indication of prices).

The new directive provides that consumers will have the right to bring individual actions if they are harmed by unfair commercial practices, such as aggressive marketing. Member States shall provide for contractual and non-contractual remedies. At a minimum, contractual remedies shall include the right to obtain a price reduction or to terminate the contract. Non-contractual remedies shall, as a minimum, include the right to compensation for damages. To that effect, the new directive inserts a new Article 11a titled 'Redress' to Directive 2005/29/EC, which provides:

1. "Consumers harmed by unfair commercial practices, shall have access to proportionate and effective remedies, including compensation for damage suffered by the consumer and, where relevant, a price reduction or the termination of the contract. Member States may determine the conditions for the application and effects of those remedies. Member States may take into account, where appropriate, the gravity and nature of the unfair commercial practice, the damage suffered by the consumer and other relevant circumstances.
2. Those remedies shall be without prejudice to the application of other remedies available to consumers under Union or national law".

This right to individual remedies is being introduced in Directive 2005/29/EC because the Commission considered that consumers harmed by unfair commercial practices did not have access to effective remedies.

Taken together, both directives would allow consumers, which in some cases may be also data subjects, harmed by unfair commercial practices to initiate representative actions and seek the new remedies available for infringements of unfair commercial practices. While individual consumers should not be able to interfere with the procedural decisions undertaking by the qualified entities allowed to initiate the action, the consumers concerned by a representative action should be entitled to benefit from that representative action. In representative actions for redress measures, the benefits should come in the form of remedies, such as compensation, repair, replacement, price reduction, contract termination or reimbursement of the price paid. In representative actions for injunctive measures, the benefit for the consumers concerned would be the cessation or prohibition of a practice that constitutes an infringement (recitals 36 and 37).

9.4.4. Question 6: Lack of conformity of digital content or services and the GDPR compliance

In light of the principle of effectiveness, dissuasiveness and of Article 47 and Article 8 CFR, could the consumer remedies against a lack of conformity of a digital content/service provided by Directive 2019/770 be used against a violation of data protection law?

New Directive 2019/770 on certain aspects concerning contracts for the supply of digital content and digital services

Directive 2019/770 (the ***Digital Content Directive***) was published in May 2019.[82] As part of the EU's Digital Single Market strategy, this directive fully harmonises certain key contractual rules for the supply of digital content or services. Member States have until 1 July 2021 to adopt and publish the measures necessary to comply with this directive. They shall apply those measures from 1 January 2022.

Among the measures that Member States must transpose there are remedies for lack of conformity of the digital content or service offered by a trader. In this respect, Article 14 of the directive provides for

[82] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *O.J.E.U.*, 22.5.2019, L 136/1.

three options for the consumer: (i) have the digital content or service brought into conformity; (ii) receive a proportionate reduction in price; or (iii) terminate the contract, in accordance with the conditions established by the directive.[83] When it comes to compensation, Article 3(10) of the directive provides that Member States are free to regulate the right to damages in case of violations of their national legislation transposing the directive. However, it is beyond the scope of this Casebook to detail these remedies extensively. Instead, the question at hand is whether these remedies for lack of conformity of a digital content or service can be used for violations of data protection law.

The scope of the directive is rather broad, as it applies to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price.[84] **Furthermore, Article 3(1) of the directive, which provides that it applies *"where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader".***

In this regard, Recital 24 of the directive provides the following:

"*Such business models are used in different forms in a considerable part of the market. While fully recognising that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies. This Directive should, therefore, apply to contracts where the trader supplies, or undertakes to supply, digital content or a digital service to the consumer, and the consumer provides, or undertakes to provide, personal data. The personal data could be provided to the trader either at the time when the contract is concluded or at a later time, such as when the consumer gives consent for the trader to use any personal data that the consumer might upload or create with the use of the digital content or digital service. Union law on the protection of personal data provides for an exhaustive list of legal grounds for the lawful processing of personal data. This Directive should apply to any contract where the consumer provides or undertakes to provide personal data to the trader. For example, this Directive should apply where the consumer opens a social media account and provides a name and email address that are used for purposes other than solely supplying the digital content or digital service, or other than complying with legal requirements. It should equally apply where the consumer gives consent for any material that constitutes personal data, such as photographs or posts that the consumer uploads, to be processed by the trader for marketing purposes. Member States should however remain free to determine whether the requirements for the formation, existence and validity of a contract under national law are fulfilled".*

Taking into account the possibility of processing personal data for commercial purposes, Directive 2019/770 extends some contractual remedies where the professional provides a digital content, or a service and the consumer/data subject "provides" personal data. With regard to the wording « the consumer provides or undertakes to provide personal data », the interpretation of similar wording in the GDPR is relevant. Article 20 GDPR on the right to data portability refers to personal data that, "have been provided" by the data subject, and the WP29 (the *Guidelines on the right to data portability*, 2017) interpreted it in an extensive way, including both data actively provided by the consumer or «observed data». Directive 2019/770 could be interpreted in the same way, also considering that the interpretation allows to better apply the directive in the online context, where most of personal data are collected through the observation of data subject's activity.

The directive also provides that Union law on the protection of personal data, especially the ***GDPR***, shall apply to any personal data processed in connection with such contracts.[85] In case of conflict between Directive 2019/770 and data protection law, the latter prevails.[86]

In the same vein, Recital 48 of the directive explicitly mentions that the lack of compliance with the GDPR may constitute a lack of conformity in the sense of the Digital Content Directive:

---

[83] Article 14 of Directive (EU) 2019/770.

[84] Article 3(1) of Directive (EU) 2019/770.

[85] Article 3(8) of Directive (EU) 2019/770.

[86] Article 3(8) of Directive (EU) 2019/770.

"Facts leading to a lack of compliance with requirements provided for by Regulation (EU) 2016/679, including core principles such as the requirements for data minimisation, data protection by design and data protection by default, may, depending on the circumstances of the case, also be considered to constitute a lack of conformity of the digital content or digital service with subjective or objective requirements for conformity provided for in this Directive. One example could be where a trader explicitly assumes an obligation in the contract, or the contract can be interpreted in that way, which is also linked to the trader's obligations under Regulation (EU) 2016/679. In that case, such a contractual commitment can become part of the subjective requirements for conformity. A second example could be where non-compliance with the obligations under Regulation (EU) 2016/679 could, at the same time render the digital content or digital service unfit for its intended purpose and, therefore, constitute a lack of conformity with the objective requirement for conformity which requires the digital content or digital service to be fit for the purposes for which digital content or digital services of the same type would be normally used".

Therefore, if there is an infringement of data protection law in processing the personal data collected by a trader and the directive applies, the consumer would be able to seek remedies available under the Digital Content Directive if that mishandling of personal data also constitutes a lack of conformity and all conditions laid down in the directive are fulfilled. Recital 48 of the directive confirms this finding:

"Where the facts leading to non-compliance with requirements under Regulation (EU) 2016/679 also constitute a lack of conformity of the digital content or digital service with subjective or objective requirements for conformity as provided for in this Directive, the consumer should be entitled to the remedies for the lack of conformity provided for by this Directive, unless the contract is already void or voidable under national law".

In this respect, the **principle of effectiveness, Article 47 and Article 8 CFREU** should be taken into account by Member States in the implementation of Directive 2019/770 and by courts in its interpretation. In particular, it raises the question whether the compliance with data protection law of the service and of the digital content is to be qualified as an objective requirement for conformity, regulated by Article 8 of that directive. Another issue is the relationship between the information provided to the data subject in accordance with Regulation 2016/679 and Article 7 of Directive 2019/770, which regulates the subjective requirements for conformity of digital content or service. It should also be considered that in several cases traders which enter in a contract with the economic operator, such as an online platform, or a social network are data subjects (See figure 1) which are active on digital environments. In this respect, the following question raises:

In light of Article 47 and 8 CFR, does the remedy consisting in the brought into conformity of a service with regard to data protection compliance could be applied by analogy, in order to grant the right to data protection also in cases in which the data subject is not a consumer, and operates in a digital environment which is not compliant with data protection requirement?

Furthermore, consumers are not the only ones who can seek remedies for lack of conformity. In order to guarantee effective enforcement of the directive's provisions, Member States shall include in their legislation the possibility for either public bodies, consumer organisations, professional organisations or not-for-profit bodies active in the field of data protection to take action under national law before courts or administrative bodies.[87] Member States are free to choose which of these types of organisations (one or more) will be able to take action.

When implementing the Digital Content Directive, Member States must therefore take into account the articulation between the two sets of laws: not only the remedies provided for in the directive, but also the

[87] Article 21(2) of Directive (EU) 2019/770.

collective redress mechanism foreseen in the GDPR. Indeed, the combination of both schemes is currently the best way to ensure effective consumer protection in the data protection space.

9.5. Guidelines emerging from the analysis

The general issue addressed in this chapter concerns the role of the application of consumer law in ensuring effective data protection (Article 8 and Article 47 CFR).

Collective redress between collective and data protection

With regard to collective redress, national legislation could allow consumer protection associations

a) to bring or defend legal proceedings against a person allegedly responsible for an infringement of the protection of personal data (*Fashion ID,* C-40/17);
b) to bring legal proceedings, in the absence of a mandate conferred on it for that purpose and independently of the infringement of specific rights of the data subjects, against the person allegedly responsible for an infringement of the data protection laws, on the basis of consumer protection law infringment, where the data processing concerned is liable to affect data subjects rights provided for by the GDPR (*Facebook Ireland Limited,* C-319/20).

Furthermore, when a violation of the GDPR violates the interests of consumers, and the person harmed is a consumer, Directive 2020/1828 on representative actions for the protection of the collective interests of consumers, which repeals Directive 2009/22 is to be applied. In any case, the relationship between collective redress in consumer and data protection should be carefully assessed; the existence of collective redress in consumer law, applicable to consumers who seek action for a data protection claim may not be sufficient for ensuring effective data protection, especially within the digital context (e.g., where the parties are a small professional and an online platform).

Unfair commercial practices and information provided to the data subject

In light of the EU Commission's *Guidance on the implementation/application of the Unfair Commercial Practices Directive,* although a trader's violation of Data Protection rules will not, in itself, always mean that there is an unfair commercial practice, data protection violations should be considered when assessing the overall unfairness of commercial practices, particularly in the situation where the trader processes consumer data in violation of data protection requirements. The Italian decisions of the Consumer protection authority, of the Administrative Tribunal of Rome and of the Council of State are examples of the interplay between data protection rules and Directive 2005/29.

Information to be provided to the data subject and consumers rights (Directive 2011/83)

The amendments of Directive 2011/83 provided in Directive 2019/2161 show the importance of the relationship between data and consumer law. In fact, the directive applies where the trader supplies or undertakes to supply digital content which is not supplied on a tangible medium or a digital service to the consumer and the consumer provides or undertakes to provide personal data to the trader, except in some specific cases (Article 3 Directive 2011/83). Moreover, before the consumer is bound by a distance or off-premises contract the trader shall provide the consumer with the information concerning the fact that the price was personalised on the basis of automated decision-making. This provision may contribute to ensuring the effectiveness of data protection, by reinforcing information duties provided within data protection legislation.

However, the **remedies** available under the Consumer Rights Directive cannot be used against violations of information duties provided in the GDPR alone. Violations of information duties under the GDPR can only be remedied with the Consumer Rights Directive if they also constitute violations of information requirements under that directive.

Information to be provided to the data subject and unfair contractual terms

National case law (especially French and German one) shows the importance of the interplay, with regard to information duties, of the GDPR and the UCTD directive. There are no EU case law or documents in that regard. Nevertheless, the principle of effectiveness and Article 47 and 8 CFREU may be of important guidance in order to interpret the relationship between the concept of unfairness under Directive 1993/13 and breaches of data protection law.

Competent administrative authorities and their coordination

As explained in a joint statement by the Italian consumer, telecom, and data protection authorities of July 2019, **data protection and consumer protection are seen to be complementary and not exclusive from one another**.
The same conduct can constitute an infringement of consumer, data protection, and competition law; the **coordination between the national and European authorities** in charge of consumer, data protection, and competition enforcement is a key issue, as the lack of such coordination may have negative consequences on the principles of effectiveness, good administration and the duty of cooperation.

Lack of conformity of digital content or services and the GDPR compliance

In light of Article 47 8 CFR, and of recital 48 of Directive 2019/770 on digital contents and services, the remedy consisting in the brought into conformity of a service with regard to data protection compliance could be a mean for granting to consumers the right to data protection.