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 content of this publication only represents the views of the authors and is their sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

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:

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

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

Article 8(2) CFREU states that personal data
"must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law (…)".
The wording of this article makes it clear that the
fundamental right to data protection requires for personal data to be processed only if there is a specific lawful basis for doing so. The general framework of the lawful basis for processing is laid down by Regulation EU 2016/679, and before its entry into force by Directive 1995/46. Those two legal acts are quite different, but their basic approach is similar and reflects Article 8(2) CFR. For this reason, the CJEU's judgments related to interpreted Article 7 of Directive 95/46 are to be taken into account in interpreting and applying Article 6 Regulation EU 2016/679 (GDPR).
Article 7 of Directive 95/46 provided:
Member States shall provide that personal data may be processed only if:
(a) the data subject has unambiguously given his consent; or
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or
(d) processing is necessary in order to protect the vital interests of the data subject; or
(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).
Article 6 GDPR, entitled "Lawfulness of processing" provides:
"1. Processing shall be lawful only if and to the extent that at least one of the following applies:
(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(e) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks".

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

Main questions addressed in this chapter:

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

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

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

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

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

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

Relevant CJEU cases

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

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

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

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

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

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

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

[9] Drafted by C. Angiolini

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

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

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

Main question addressed

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

Relevant legal sources

EU Level

Directive 95/46

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

Article 7 of the Directive

See §1.1.

The case

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

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

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

Preliminary questions referred to the Court

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

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

Reasoning of the Court

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

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

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

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

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

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

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

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

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

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

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

Conclusion of the Court

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

Elements of judicial dialogue

- Horizontal judicial dialogue (within the CJEU):

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

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

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

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

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

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

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

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

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

The opinions of supervisory authorities

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

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

Italy

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

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

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

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

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

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

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

Relevant CJEU case

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

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

Cluster of cases

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

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

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

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

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

Main question addressed

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

Relevant legal sources

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

The case

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

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

Preliminary questions referred to the Court

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

Reasoning of the Court

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

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

Conclusion of the Court

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

Elements of judicial dialogue

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

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

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

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

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

The opinions of supervisory authorities

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

Furthermore, on 4 May 2020, the EDPB adopted new guidelines (No 5) on consent. According to that guidelines "**Free and freely given consent" means that data subjects can make "real" choice and control.**

In particular, the EDPB stated that:
"If consent is bundled up as a non-negotiable part of terms and conditions it is presumed not to have been freely given. Accordingly, consent will not be considered to be free if the data subject is unable to refuse or withdraw his or her consent without detriment (…). The GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract".
Moreover, the EDPB highlighted that, by reason of the wording of Article 7(4) GDPR and of recital 43 thereof, where the data are not necessary for the performance of the contract, (including the provision of a service), and the performance of that contract is made conditional on the obtaining of these data on the basis of consent, the conditionality would not render the consent invalid only in highly exceptional cases.
Furthermore, the EDPB recalled that the burden of proof concerning the existence of a free consent lies on the controller and that this rule is a concretisation of the general principle of accountability. According to the EDPB, in order to prove that the consent is free and freely given, the controller could argue that his organisation offers data subjects genuine choice if they were able to choose between a service that includes consenting to the use of personal data for additional purposes on the one hand, and an equivalent service offered by the same controller that does not involve consenting to data use for additional purposes on the other hand.
According to the EDPB, another important element for the assessment concerning the existence of a free consent are the granularity of consent (the possibility of consent or not separately to each purpose for processing and data processing operation).
Furthermore, the EDPB provided guidelines concerning the meaning of the "specific" and informed consent, based on "unambiguous indication of wishes". With regard to the latter requirement, the EDPB stated that:
"The use of pre-ticked opt-in boxes is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice. (…) A controller must also beware that consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service. Blanket acceptance of general terms and conditions cannot be seen as a clear affirmative action to consent to the use of personal data. The GDPR does not allow controllers to offer pre-ticked boxes or opt-out constructions that require an intervention from the data subject to prevent agreement (for example 'opt-out boxes')".

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

Italy
Italian courts have not yet referred to *Planet49* (C-673/17). Nevertheless, it is interesting to look to Italian case law and administrative decisions concerning data subject's consent. An important group of decisions concerns the freedom of the consent.
In that regard, the Italian Data Protection Authority have adopted a restrictive position, considering that consent cannot be qualified as freely given when the providing of a service is subordinate to data subject's consent (GPDP, 1° October 2015, n. 4611905; GPDP, 11 June 2015, n. 4243173; GPDP, 18 December 2014, n. 3750400; GPDP, *Linee guida in materia di attività promozionale e contrasto allo spam,* 4 July 2013, n. 2542348; GPDP, 10 January 2019, n. 9080914) or when there is a pre-checked checkbox which the user must deselect to refuse his or her consent (GPDP, 1° October 2015, n. 4611905; GPDP, 5 March 2015, n. 4203055; GPDP, 11 June 2015, n. 4243173; GPDP, 18 December 2014, n. 3750400; GPDP, *Linee guida*

in materia di attività promozionale e contrasto allo spam, 4 luglio 2013, n. 2542348; GPDP, 22 February 2007, n. 1388590; GPDP, 12 October 2015, n. 1179604; GPDP, 3 November 2005, n. 1195215; GPDP, 15 July 2010, n. 1741998; GPDP, 10 January 2019, n. 9080914).

Furthermore, in the judgment of 2 July 2018, n. 17278, the Court of Cassation affirmed that the consent could considered freely given also in some cases in which a service is provided only if the data subject expresses the consent to processing. In this regard, the Court stated that in order to decide if the consent is freely given it is important to consider if the service is non-fungible and essential.

Moreover, a recent judgement of the Italian Court of Cassation (of 21 October 2019, No. 26778), concerning a contractual relationship between a client and a bank, is of particular interest. In that case, the client signed a clause according to which, in the absence of consent to the processing of sensitive data, the bank would not be able to carry out the operations and services requested. The Court of Cassation, in the above mentioned case, affirmed the voidness of the clause because it is considered contrary to imperative provisions of data protection law.

As to the meaning of "informed consent" the Court of Cassation, in its decision no. 14381 of 25 May 2021, stated that consent to processing is valid only if it is freely and specifically expressed with reference to a clearly identified processing operation; it follows that in the case of a web platform (with annexed computer archives) designed to process the reputation profiles of individual physical or legal persons, based on a calculation system based on an algorithm aimed at establishing reliability scores, the requirement of "informed consent" cannot be considered satisfied if the executive scheme of the algorithm and the elements of which it is composed remain unknown or cannot be known by the data subjects.

France

Various decisions of the French Data Protection Authorities (*Commission nationale de l'informatique et des libertés*; hereinafter: CNIL) are of particular interest. For example, the decision of 30 October 2018 2018-042, concerning the lawfulness of the data processing implemented by a company which uses technologies that allows personal data to be collected via multifunction mobiles and to carry out advertising campaigns on mobiles. This company uses technical tools which allow the company to collect data from users of multifunction mobile phones even when these applications are not running. The advertising ID of the MFPs and the geolocation data of the people are collected. This data is then cross-referenced with points of interest determined by partners (store chains) to display targeted advertising on people's devices from the places they have visited. The company also processes, for the purposes of profiling and advertising targeting, geolocation data that it receives via real-time auction offers initially transmitted for the purpose of enabling the company to purchase advertising space. The company indicates that it processes this data with the consent of the persons concerned. **The CNIL stated that there was lack of consent to the processing of geolocation data for the purposes of advertising targeting**. *Inter alia*, the CNIL stated that the information given to the user does not explain that their data will be used for this real-time auction system, nor that it will then be stored for the purpose of defining a commercial profile (For more information on the decision, see the FRICORE Database, at this link).

Another important decision of the CNIL is the one of 21 January 2019 2019-001. In that case, the CNIL was seized for two collective complaints submitted in accordance with Article 80 of the GDPR, from associations who criticised Google for not having a valid legal basis for processing the personal data of the users of its services, in particular for the purposes of advertising personalisation.

On the basis of the investigations carried out, the CNIL found Google's failure to have a legal basis for the personalisation processing of advertising. Google relies on users' consent to process their data for the purpose of personalising advertising. **However, the CNIL stated that that consent is not validly collected for two reasons. First, user consent is not sufficiently informed.** The information on such processing, diluted in several documents, does not allow the user to be aware of the extent of the

processing. **Second, the consent collected is not "specific" and "unambiguous".** On the breach of the obligation to have a legal basis for the processing implemented, the CNIL considers that the consent on which the company bases personalised advertising processing is not validly obtained as provided for in Article 6 of the GDPR. The CNIL pronounced a financial penalty of 50 million euros against the company Google LLC in application of the GDPR for lack of transparency, unsatisfactory information and lack of valid consent for the personalisation of advertising. (For more information on the decision, see the FRICORE Database, at this link).

4.1.3. Question 3: Fundamental rights and legitimate basis for processing

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

➢ Judgment of the Court (Grand Chamber), 29 January 2008, *Productores de Música de España (Promusicae)* v. *Telefónica de España SAU*, Case C-275/06 (***Promusicae***)

Cluster of relevant CJEU cases

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

➢ Judgment of the Court (Grand Chamber), 29 January 2008, *Productores de Música de España (Promusicae)* v. *Telefónica de España SAU*, Case C-275/06 (***Promusicae***)

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

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

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

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

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

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

➢ Judgment of the Court (Second Chamber), 9 March 2017, *Camera di Commercio,Industria, Artigianato e Agricoltura di Lecce* v *Manni*, Case C-398/15 (***Manni***)

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

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

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

Main question addressed:

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

Relevant legal sources:

EU Level

Charter of Fundamental Fights of the EU

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

Directive 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Article 7 – Criteria for making data processing legitimate; Article 8 (1) and (2) The processing of special categories of data; Article 13(1) Exemptions and restrictions

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

Recital 2; Article 5 (1) Confidentiality of the communications; *Article 6 (1) Traffic data*; *Article 15(1), Application of certain provisions of Directive 95/46/EC*

The case(s):

Promusicae is a non-profit-making organisation of producers and publishers of musical and audiovisual recordings. In 2005, it made an application to the *Juzgado de lo Mercantil No 5 de Madrid* (Commercial Court No 5, Madrid) for preliminary measures against Telefónica, a commercial company whose activities include the provision of internet access services. Promusicae contended that some of Telefónica's clients used a peer-to-peer programme to share access to phonograms in which the members of Promusicae held the exploitation rights and was seeking an injunction against Telefónica to disclose the identities and physical addresses of certain clients. Disclosure of this information was meant to enable Promusicae to bring civil proceedings against the persons concerned. By order of 21 December 2005 the *Juzgado de lo Mercantil No 5 de Madrid* ordered the preliminary measures requested by Promusicae.

Telefónica appealed against that order, contending that under the LSSI the communication of the data sought by Promusicae was authorised only in a criminal investigation or for the purpose of safeguarding public security and national defence, not in civil proceedings or as a preliminary measure relating to civil proceedings. Promusicae relied, notably, on articles 17(2) and 47 of the Charter protecting the right to intellectual property and the right to effective justice. The *Juzgado de lo Mercantil No 5 de Madrid* decided to stay the proceedings and refer a question to the Court for a preliminary ruling.

Preliminary ruling referred to the Court:

"Does Community law, specifically [the directives listed above] and Articles 17(2) and 47 of the Charter (…) permit Member States to limit to the context of a criminal investigation or to safeguard public security and national defence, thus excluding civil proceedings, the duty of operators of electronic communications networks and services, providers of access to telecommunications networks and providers of data storage services to retain and make available connection and traffic data generated by the communications established during the supply of an information society service?"

Reasoning of the Court:

On the question whether Directive 2002/58 precludes the Member States from laying down an obligation for operators of electronic communications networks to communicate personal data for the purpose of the protection of intellectual property rights, the Court answers in the negative.

After recalling that under the directive's provisions, Member States may adopt legislative measures to restrict the scope of the obligation to ensure the confidentiality of data traffic, where *such a restriction constitutes a necessary, appropriate and proportionate measure within a democratic society* to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communications system, the Court observes that none of these exceptions appears to relate to situations that call for the bringing of civil proceedings. However, the Court considers that it is clear that Article 15(1) of Directive 2002/58 ends the list of the above exceptions with an express reference to Article 13(1) of Directive 95/46. That provision also authorises Member States to adopt legislative measures to restrict the obligation of confidentiality of personal data where that restriction is necessary *inter alia* for the protection of the rights and freedoms of others. As they do not specify the rights and freedoms concerned, those provisions of Article 15(1) of Directive 2002/58 must be interpreted as expressing the Community legislature's intention not to exclude from their scope the protection of the right to property or situations in which authors seek to obtain that protection in civil proceedings.

On the question whether EU law requires the Member States to lay down the disputed obligation, the Court briefly examines the impact of IP directives, on which it concludes that they do not impose such a requirement, before evaluating **the impact of fundamental rights enshrined in articles 17(2) and 47 of the Charter** more substantially.

Does an interpretation of the IP directives to the effect that Member States are not obliged, in order to ensure the effective protection of copyright, to lay down an obligation to communicate personal data in the context of civil proceedings, lead to an infringement of the fundamental right to property and the fundamental right to effective judicial protection?

To answer the question, the Court recalls that the fundamental right to property and the fundamental right to effective judicial protection constitute general principles of Community law. However, in the situation referred by the national court, another further fundamental right, namely the right that guarantees protection of personal data and hence of private life, is at stake, since Directive 2002/58 seeks to ensure full respect for the rights set out in Articles 7 and 8 of that Charter, also protected under Article 8 ECHR). It is thus necessary to reconcile the requirements of the protection of those different (and in this case conflicting) fundamental rights. To achieve this reconciliation, *the Member States must, when transposing the directives, take care to rely on an interpretation of the directives that allows a fair balance to be struck between the various fundamental rights protected by the Community legal order. Further, when implementing the measures transposing those directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them that would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality*.

In other terms, the Court urges the Member States to transpose and implement directives so as to avoid any conflict of fundamental rights. If such conflict cannot be avoided, in the view of the Court, Member States should rely on general principles of the EU, **in particular the principle of proportionality**, to reach a balanced solution that will not unduly sacrifice **the effective protection of one fundamental right for the protection of another** (**principle of effectiveness**).

To define the relevant elements to put in the balance, the decision is to be read in light of the CJEU decisions in *Lindqvist*, *ASNEF* and *FECEMD, Google Spain* and *Rigas Satiksme*.

In ***Lindqvist***, the Court concludes that *when conducting that balancing process, a national court should take account, in accordance with the principle of proportionality, of all the circumstances of the case before it, in particular the*

duration of the breach of data protection and the importance, for the persons concerned, of the protection of the data disclosed.
In ***ASNEF and FECEMD***, the Court judges that in relation to the balancing of interests, it is possible to take into consideration the fact that the data in question already appears in public sources.
In ***Google Spain***, the Court states that the assessment *may depend on the nature of the information in question and its sensitivity for the data subject's private life and the fact that its initial publication had taken place 16 years previously, balanced with the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life* (See Chapters 5 and 8).
In ***Rigas Satiksme***, the Court considers that, while the age of the data subject may be one of the factors which should be taken into account in the context of that balance of interests, it does not appear to be justified to refuse to disclose to an injured party the personal data necessary for bringing an action for damages against the person who caused the harm, on the sole ground that that person was a minor.
The decision is also to be read in light of ***ASNEF and FECEMD*** and ***Breyer*** (see below), in which the Court judges that the Member States cannot add new principles relating to the lawfulness of the processing of personal data or impose additional requirements that have the effect of amending the scope of one of the six principles provided for in Article 7 of Directive 95/46. Concerning in particular Article 7(f) of the Directive, only two cumulative conditions are set out for the lawfulness of the processing of data, which are: (1) that the processing of the personal data must be necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data is disclosed; and, (2) that such interests must not be overridden by the fundamental rights and freedoms of the data subject. Thus, Member States are precluded from excluding, categorically and in general, the possibility of processing certain categories of personal data without allowing the opposing rights and interests at issue to be balanced against each other in a particular case.

Conclusion of the Court:

Directives 2000/31, 2001/29, 2004/48 (IP) and 2002/58 (data protection) do not require Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings.
However, Community law requires that, the authorities and courts of Member States must make sure that they do not rely on an interpretation of data protection law which would be in conflict with fundamental rights or with the other general principles of Community law, such as the principle of proportionality.

Impact on the follow-up case:
The Commercial Court n° 5 of Madrid in its decision of 17 March 2008, mentioning the CJEU judgement, upheld Telefonica's opposition to Promusicae's request. Relying on national legislation applicable to the proceedings (*Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico*, Article 12; *Ley de Protección de Datos de Carácter Personal*, Article 11; *Ley de Competencia Desleal*, Article 29), the Court stated that connection and traffic data generated by the communications established during the supply of an information society service may be used only in the course of criminal investigations or for safeguarding public security and national defence or other cases permitted by law. Data processing is not permitted by national law for bringing civil proceedings for unfair competition or infringement of intellectual property rights.

Elements of judicial dialogue:

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

- In ***Scarlet Extended***, the Court builds on its analysis in *Promusicae* to decide whether it is possible for a national court to make an order, on the request of a management company representing authors of musical works, against an internet service provider for the installation of a filtering system

and for measures to be taken against its customers violating copyright. The Court reaches the conclusion that such an injunction would infringe the requirement that a fair balance be struck between the right to intellectual property, on the one hand, and the freedom to conduct business, the right to protection of personal data and the freedom to receive or impart information, on the other. But the decision is mainly motivated on the basis of freedom to conduct a business, not on the right to protection of data.

- In ***Ryneš***, the Court, after concluding that video surveillance covering even partial public space is not a 'purely personal or household activity' and thus falls under the regime of data protection (see Chapter 1, question 1), notes that EU law makes it possible to take account of legitimate interests pursued by the controller, such as the protection of the property, health and life of his family and himself, as in the referred case. The court draws no direct conclusion from this finding; it simply answers the question asked (is the activity in question covered by one of the admitted derogations to data protection?). However, in light of *Promusicae*, it is clear that the Court is inviting national authorities to follow the methodology described above, in order to balance the right to data protection and privacy with the legitimate interest of the controller to protect his home and family.
- In ***Breyer*****,** the Court complements the reasoning in *Promusicae*, by answering the question whether Article 7(f) of Directive 95/46 precludes a provision in national law whereby a service provider may collect and use a user's personal data without his consent only to the extent necessary in order to facilitate, and charge for, the specific use of the tele-medium by the user concerned, and under which the purpose of ensuring the general operability of the tele-medium cannot justify use of the data beyond that of the particular use of the tele-medium.
- In ***Manni***, the Court observes that the purpose of the disclosure of personal data in the companies' register (provided for by Directive 68/151) is in particular to protect the interests of third parties in relation to joint stock companies and limited liability companies, since the only safeguards they offer to third parties are their assets, and to guarantee legal certainty in relation to dealings between companies and third parties in view of the intensification of trade between Member States following the creation of the internal market. The Court observes moreover that, for several reasons, it is absolutely necessary to access data concerning a company long after its dissolution. For this reason, Member States cannot guarantee the natural persons referred to in Directive 68/151 the right, as a matter of principle, a given length of time after the dissolution of the company concerned, to the erasure of personal data concerning them that have been entered in the register pursuant to the latter provision, or the blocking of that data from public access. Such situation does not result in disproportionate interference with the fundamental rights of the persons concerned, and particularly their right to respect for private life and their right to protection of personal data as guaranteed by Articles 7 and 8 of the Charter, because the disclosure concerns only a limited amount of data, because other legitimate interests are at stake, and because persons engaging in such activity are aware of these requirements. National courts must engage in a case-by-case analysis to decide if, exceptionally, it is justified, on compelling legitimate grounds relating to their particular situation, to limit, after a sufficiently long period has expired since the dissolution of the company concerned, access to personal data in that register relating to the natural person referred to in Directive 68/151, by third parties who can demonstrate a specific interest in consulting that data.
- In ***Rigas Satiksme*****,** the Court follows the same reasoning as in *Promusicae*, to which it expressly refers. Firstly, Article 7(f) of Directive 95/46 does not impose the obligation to disclose personal data to a third party in order to enable them to bring an action for damages before a civil court for harm caused by the person concerned by the protection of that data. However, Article 7(f) of that directive does not preclude such disclosure on the basis of national law, and national courts should decide whether disclosure is to be ordered after balancing the conflicting interests, following the methodology described above.
- In ***M.I.C.M*** (C-597/19) the Court, in what regards the balance of interests, considered that in order for processing, such as the registration of IP addresses of persons whose Internet connections have been used to upload pieces of files containing protected works on peer-to-peer networks, for the

purposes of filing a request for disclosure of the names and postal addresses of the holders of those IP addresses, can be regarded as lawful by satisfying the conditions laid down by Regulation 2016/679, it is necessary, in particular, to ascertain whether that processing satisfies the above mentioned provisions of Directive 2002/58, which embodies, for users of electronic communications, the fundamental rights to respect for private life and the protection of personal data. Accordingly, in its conclusions the Court stated that Point (f) of subparagraph 1 of Article 6(1) of Regulation (EU) 2016/679, read in conjunction with Article 15(1) of Directive 2002/58/EC (Directive on privacy and electronic communications), as does not preclude in principle, neither the systematic recording, by the holder of intellectual property rights as well as by a third party on his or her behalf, of IP addresses of users of peer-to-peer networks whose Internet connections have allegedly been used in infringing activities, nor the communication of the names and of the postal addresses of those users to that right-holder or to a third party in order to enable it to bring a claim for damages before a civil court for prejudice allegedly caused by those users, provided, however, that the initiatives and requests to that effect of that right-holder or of such a third party are justified, proportionate and not abusive and have their legal basis in a national legislative measure, within the meaning of Article 15(1) of Directive 2002/58, which limits the scope of the rules laid down in Articles 5 and 6 of that directive.

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

Italy

Promusicae had an impact on Italian judgements concerning similar cases. The Court of Rome (decision of 19 March 2008, No 26121), relying on *Promusicae* and on the principle of proportionality, affirmed that is for national judges to balance the protection of intellectual property and the right to data protection. Interpreting national rules applicable to the case (mainly Articles 4, 24, 132, 123 of the code concerning privacy and data protection, d.lgs. 196/2003, which was largely amended by reason of the GDPR), the court stated that the Italian legislator limited the exception to the general prohibition to retention of traffic data to criminal cases, and that this choice was compatible with European law, as interpreted by the CJEU. Accordingly, the Court of Rome rejected access requests to user data grounded on the protection of intellectual property. The same conclusion and a similar reasoning was adopted by the Court of Rome in its decisions of 22 November 2017 No 39349, and No 39355, where the conclusions of AG Kokott in *Promusicae* were mentioned.

4.2. Guidelines emerging from the analysis

The CJEU addressed the cases related to lawful basis for processing — namely the ones concerning the legitimate interest of the data controller or of a third party and the data subject's consent — in light of Article 8 CFREU and other fundamental rights.

Fundamental rights and legal basis for processing

With regard to the balance between the right to data protection on the one hand and on the other hand intellectual property rights and the right to conduct a business, within the scope of application of Directive 2002/58, according to the CJEU,

- the right to (intellectual) property (Article 17 CFR) and its enforceability (Article 47 CFR) do not require Member States to lay down an obligation to communicate personal data in order to ensure effective protection of copyright in the context of civil proceedings (*Promusicae,* C-275/06).
- In light of the right to conduct a business and the right to data protection an injunction made against an internet service provider which requires it to install is precluded as a preventive measure for an unlimited period of time, a system for filtering all electronic communications passing via its services,

which applies indiscriminately to all its customers, exclusively at its expense, which is capable of identifying on that provider's network the movement of electronic files containing a musical, cinematographic or audio-visual work (*Scarlet Extended,* C-70/10)

- the systematic recording, by the holder of intellectual property rights as well as by a third party on their behalf, of IP addresses of users of peer-to-peer networks whose Internet connections have allegedly been used in infringing activities, and the communication of the names and of the postal addresses of those users to that right-holder or to a third party in order to enable it to bring a claim for damages before a civil court for prejudice allegedly caused by those users are not prohibited under Article 6(1)(f) GDPR, read in light of Directive 2002/58, where the initiatives and requests of that right-holder or of the third party are justified, proportionate and not abusive and have their legal basis in a national legislative measure, within the meaning of Article 15(1) of Directive 2002/58, which limits the scope of the rules laid down in Articles 5 and 6 of that directive (*M.I.C.M.,* C-597/19).

In that regard, the following question arises:

Within the framework of the GDPR, where the data controller can communicate personal data to a third party on the basis of its legitimate interest (e.g. the development of a specific medical device), a third party asks access to personal data and their access to personal data is essential for ensuring the protection of her fundamental right (e.g. right to health), could Article 47 CFREU play a role, granting the third party's access to data?

Legitimate interest as a legal basis for processing

In order to lawfully process personal data relying on the legal basis of the legitimate interest, three cumulative conditions should be met:

1) the pursuit of a present and effective legitimate interest by the data controller or by the third party or parties to whom the data are disclosed.

2) the need to process personal data for the purposes of the legitimate interests pursued. The necessity concept should be interpreted strictly (*Rīgas satiksme*, C-13/16, §30), and national courts should consider if the legitimate interest pursued through the processing cannot reasonably be as effectively achieved by other means less restrictive of the fundamental rights and freedoms of data subjects, in particular the rights to respect for private life and to the protection of personal data guaranteed by Articles 7 and 8 CFR.

3) the fundamental rights and freedoms of the person concerned by the data protection do not take precedence over the legitimate interest pursued. The seriousness of the infringement of the data subject's rights and freedoms is an essential component of the balancing exercise on a case-by-case basis (*Rīgas satiksme*, C-13/16, §28). In that assessment the following elements could be considered (*Asociația de Proprietari* C-708/18):

a) the availability of personal data at issue in public sources.

b) the nature of the personal data at issue, in particular of its potentially sensitive nature, of the nature and specific methods of processing and of the number of persons having access to those data and the methods of accessing them.

c) The data subject's reasonable expectations.

The principle of **proportionality** is recalled in the CJEU case law, at least in two different ways: a) as an element of the evaluation of the necessity of the processing for the purposes of the legitimate, b) as a principle which has to be applied in case of limitation of the fundamental rights set forth in the Charter (Article 52 CFR). The relationship between the principle of proportionality of processing and Article 52 CFREU with regard to the proportionality of limitations to the exercise of the right to data protection could be object of future CJEU's judgements.

Data subject consent as a legal basis for processing

Data subject's consent is not validly constituted as a lawful basis for processing if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent (*Planet49*, C-673/17).

Moreover, in light of the effectiveness of Article 8 CFREU the regulation of data subject's consent should be interpret with the objective of ensuring a genuine choice of the data subject. In this respect, according to *Orange Romania* (C-61/19), under Regulation EU 2016/679 it is for the data controller to demonstrate that the data subject has given a valid consent to the processing.