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:

7. Effective, proportionate and dissuasive sanctions and remedies

7.1. Introduction. Remedies and sanctions within the GDPR

What is the relationship between sanctions and remedies? Which authority can apply sanctions and which one can administer remedies? What are the procedural instruments of coordination when the administrative authority administers sanctions and the judicial body remedies?

The effective protection of natural persons concerning the processing of personal data calls for effective, proportionate and dissuasive sanctions and remedies against infringers of the data subjects' rights. In most Member States, the major focus has been on administrative sanctions, implemented by national supervisory authorities. However, the relevance of civil remedies should not be underestimated. The role of collective redress is also essential, even if not fully developed at the European level (see the box at the end of Chapter 8 and for a comparison of collective redress in consumer and data protection at the EU level, see Chapter 9). Within the GDPR the system of remedies and sanctions is highly articulated; the principle of effectiveness, proportionality, and dissuasiveness are of particular importance in its interpretation, as several provisions of the GDPR demonstrate.

With regard to **remedies,** the data subjects' rights are significant, considering that they shape an important set of remedies for granting the data subject the means for reacting against unlawful processing and exercising control over data concerning her. The **data subjects' rights** are the following: the right of access (Article 15 GDPR), the right to rectification (Article 16 GDPR), the right to erasure (Article 17 GDPR), the right to restriction of processing (Article 18 GDPR), the right to data portability (Article 20 GDPR), the right to object (Article 21 GDPR), and the right to not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, except for the exception provided for by Article 22 (2) GDPR.

Furthermore, Article 82 regulates the right to **compensation** of persons who suffered material or non-material damage as a result of an infringement of the GDPR. Such compensation, as expressly stated by Article 82 should be **effective** (see also recital 146, according to which compensation should be **full and effective**).

Furthermore, according to Article 58 GDPR, **Data Protection Authorities** have **investigative powers** (*e.g.*, to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with Union or a Member State procedural law), **corrective ones** (*e.g.*, to impose a temporary or definitive limitation including a ban on processing; to order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 GDPR; corrective powers include the power to impose an administrative fine) and **authorisation and advisory powers** (*e.g.*, to issue, on its own initiative or on request, opinions to the national parliament, the Member State's government). According to recital 129 of the GDPR those powers should be **effective**.

Moreover, the GDPR expressly states that **sanctions** must be **effective, proportionate, and dissuasive** (see Article 83, Article 84, recitals 151-152 GDPR). Article 83 GDPR identifies some criteria to be considered in determining the amount of administrative fines, such as the nature, gravity, and duration of the infringement taking into account the nature, scope, or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them.

The GDPR partially regulates the **coordination between DPAs' corrective powers and the imposition of fines**. In particular, Article 83 GDPR provides that, depending on the circumstances of each individual case, administrative fines may be imposed in addition to, or instead of, the following corrective measures, provided for by Article 58 GDPR: i) issuing warnings to a controller or processor

that intended processing operations are likely to infringe provisions of this Regulation; ii) withdrawing a certification or to order the certification body to withdraw a certification issued pursuant to Articles 42 and 43, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met; iii) ordering the suspension of data flows to a recipient in a third country or an international organization. Furthermore, according to Article 83 GDPR a criterion for determining the amount of administrative fines is the existence of corrective measures referred to in Article 58(2) against the controller or processor concerned with regard to the same subject-matter and the compliance with those measures. This means that effectiveness, proportionality and dissuasiveness should be assessed taking into account the possible combination between fines and other corrective measures.
For sake of clarity in this Casebook we will use the term 'corrective measures' for measures different from fines, whereas the latter will be referred to as fine, sanctions or penalties.
As to the **role of judicial authorities,** in addition to what has already been said with respect to the powers of the administrative authorities pursuant to Article 58 GDPR, the data subject has the right to lodge a complaint with a supervisory authority (Article 77), and the right to an **effective judicial remedy** where they consider that his or her rights under the GDPR have been infringed as a result of the processing of their personal data in non-compliance with the GDPR (Article 79, recital 139 GDPR). Furthermore, according to Article 80 GDPR, collective redress should be available with an opt-in formula for the exercise of the data subjects' rights before DPAs and Courts. Moreover, Member States may choose to establish an opt-out class action for the exercise of data subject rights and an opt-in class action for exercising the right to compensation provided for by Article 82 (On collective redress see also the box at the end of Chapter 8 and paragraph XX of chapter 9).

Moreover, according to Article 83 GDPR, DPAs should have the competence of establishing administrative fines (in this respect, see also the introduction of chapter 6). Nevertheless, according to that provision, if the Member States' legal system does not provide for administrative fines, the fine may be initiated by the competent DPA and imposed by competent national courts, while ensuring that those legal remedies are **effective** and have an **equivalent effect** to the administrative fines imposed by DPAs. Considering the complexity of the system of remedies and sanctions drawn by EU data protection legislation, and that their application may have a significant impact on fundamental rights, the following question arises as a general question including more specific sub-questions along the chapter.

What is or should be the impact of Article 47 CFR, Article 19 TEU and of the principles of effectiveness, proportionality and/or dissuasiveness on the definition and the implementation of sanctions and remedies for violations of data protection carried out by administrative authorities and Courts? Does the application of the principles of effectiveness, proportionality and dissuasiveness differ when they are applied to sanctions or remedies?

Main questions addressed

1. What is the relationship between sanctions and remedies? Which authority can apply sanctions and which one can administer remedies? What are the procedural instruments of coordination when the administrative authority administers sanctions and the judicial body remedies?

What is or should be the impact of Article 47 CFR, Article 19 TEU and of the principles of effectiveness, proportionality and/or dissuasiveness on the definition and/or implementation of sanctions and remedies for violations of data protection carried out by administrative authorities and Courts? Does the application of the principles of effectiveness, proportionality and dissuasiveness differ when they are applied in interpreting sanctions or remedies?

2. In order to ensure an effective remedy, should data subjects be entitled to obtain the removal from the list of results displayed by a search engine of a particular operator, and from links to web pages published by third parties?
3. In order to ensure the effective protection of personal data within the EU and full compensation of victims, should courts award compensation for material and non-material damages for any infringement of EU data protection law regardless of whether specific harm is found to have been caused by the infringement?

4. How do the principle of effectiveness and Article 47 CFREU influence the array of full compensation in the case of unlawful collection and processing of data?

5. Which is the role of the principle of proportionality in the application of sanctions?

6. Which is the role of the principle of proportionality in applying the right to be de-listed, which stems from the right to erasure provided for by Article 17 GDPR?

7. What is the relationship between data protection/privacy and information to be provided to the data subject, considered the importance of the latter for the exercise of data subjects' rights? Do Article 47 CFREU and the principles of effectiveness and proportionality play a role in this regard?

Furthermore, the issues related to balancing multiple individuals' rights and Article 47 CFREU are addressed in a box at the end of the chapter.

Relevant legal sources:

EU Level
Charter of Fundamental Rights of the EU
Article 47 - Right to an effective remedy and to a fair trial

Directive 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data *(Act no longer in force, date of end of validity: 24/05/2018, repealed by Regulation (EU) 2016/679)*
Chapter II. General rules on the lawfulness of the processing of personal data; Article 12 - Right of access; Article 14 - The data subject's right to object; Article 22 - Remedies; Article 23 - Liability; Article 24 - Sanctions

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
(In force since: 25/05/2018)

Article 13 - Information to be provided where personal data are collected from the data subject; Article 14 - Information to be provided where personal data have not been obtained from the data subject; Article 15 - Right of access by the data subject; Section III. Rectification and erasure; Article 16 - Right to rectification; Article 17 - Right to erasure ('right to be forgotten'); Article 18 - Right to restriction of processing; Article 19 - Notification obligation regarding rectification or erasure of personal data or restriction of processing

CHAPTER VIII. Remedies, liability and penalties
Article 77 - Right to lodge a complaint with a supervisory authority; Article 78 - Right to an effective judicial remedy against a supervisory authority; Article 79 - Right to an effective judicial remedy against a controller or processor; Article

80 - Representation of data subjects; Article 81 - Suspension of proceedings; Article 82 - Right to compensation and liability.

7.2. The impact of the principle of effectiveness on the system of sanctions and remedies drawn by the GDP

7.2.1. Question 1: The impact of the principle of effectiveness on remedies: the example of the right to "de-listing"

In order to ensure an effective remedy, should data subjects be entitled to obtain the removal from the list of results displayed by a particular operator search engine and, links to web pages published by third parties?

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

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *G.C., A.F., B.H., E.D.* v *Commission nationale de l'informatique et des libertés* (CNIL), Case C-136/17 (***GC and Others)***

Cluster of relevant CJEU cases

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

➢ Judgment of the Court (Second Chamber), 26 July 2019, *Fashion ID Gmbh & Co.KG* v. *Verbraucherzentrale NRW EV*, Case C-40/17 (***Fashion ID***)

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *G.C., A.F., B.H., E.D.* v *Commission nationale de l'informatique et des libertés* (CNIL), Case C-136/17 (***GC and Others)***

➢ Judgement of the Court (Grand Chamber), 24 September 2019, *Google LLC v. Commission nationale de l'informatique et des libertés* (CNIL), C-507/17 (***Google v. CNIL***)

➢ Judgment of the Court (Third Chamber) of 3 October 2019, *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, C-18/18

➢ Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 24 September 2020 — *TU, RE v Google LLC*, Case C-460/20 (**TU, RE v Google LLC**) [pending]; AG Opinion, 7 April 2022

➢ Request for a preliminary ruling from the Hof van beroep te Brussel (Belgium) lodged on 2 March 2021 — *Proximus NV v Gegevensbeschermingsautoriteit*, Case C-129/21, (**Proximus**) [pending]

Relevant legal sources

EU Charter of Fundamental Rights

Article 8 Right to data protection; Article 7 right to a private life; Article 11; Freedom of expression; Article 52 Scope of guaranteed rights

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

Article 17 Right to erasure ('right to be forgotten')

The case and relevant legal sources:

GC, AF, BH and ED requested Google to de-reference in the list of results displayed by the search engine operated by Google in response to searches against their names various links leading to web pages published by third parties.

Google refused to comply with the users' request. Then, the data subjects brought complaints before the CNIL, seeking for Google to be ordered to de-reference the links in question. By letters dated 24 April 2015, 28 August 2015, 21 March 2016 and 9 May 2016 respectively, the president of the CNIL informed them that the procedures on their complaints had been closed. The applicants sought an action before the French Council of State against those refusals of the CNIL to serve formal notice on Google to carry out the de-referencing requested.

Preliminary question(s) referred to the Court:

Several questions were referred by the CJEU.

In its first question, the referring court essentially asks whether the prohibition or restrictions relating to the processing of sensitive data apply also, subject to the exceptions provided for by the directive, to the operator of a search engine in the context of his responsibilities, powers and capabilities as the controller of the processing carried out for the needs of the functioning of the search engine.

The other questions concerned the scope of the obligations of the search engine, in relation to the type of data (sensitive and judicial data), and the purposes of the processing.

Reasoning of the Court:

The CJEU, relied on its previous case law and specifically on *Google Spain* (C-131/12), a leading case with regard to the "de-listing" and the role of the principle of effectiveness in shaping remedies. In the present case, the Court stated that in so far as the activity of a search engine is liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data, the operator of the search engine as a controller (*i.e.*, the person determining the purposes and means of processing) must ensure that the processing meets the requirements of data protection laws in order that the guarantees laid down by that legislation may have full effect and that "**effective and complete protection of data subjects**, in particular of their right to privacy, may actually be achieved".

Then, the CJEU, relying on its previous case law affirmed that, in order to respect data subjects' rights the operator of a search engine is obliged to remove from the list of results appearing as a result of a search carried out on the basis of a person's name, links to web pages, published by third parties and containing information relating to that person, even where that name or that information is not previously or simultaneously deleted from the web pages in question, and that may be the case even where their publication on those web pages is in itself lawful.

Furthermore, the Court affirmed, in light of her fundamental rights under Articles 7 and 8 CFR, that when the data subject, request that personal data concerning her no longer be made available to the general public on account of its inclusion in such a list of results, the right to the protection of personal data and the right to a private life override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. Nevertheless, the CJEU stated that that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his or her fundamental rights is justified by the preponderant interest of the general public in having, on account of its inclusion in the list of results, access to the information in question.

The Court expressly referred to Article 17 GDPR concerning the right to erasure and the right to be forgotten, interpreting it in light of fundamental rights and the principle of proportionality (see, in this chapter, Question 7), and specifically the right to information (see also in this respect, Chapter 5).

Conclusion of the Court:

The CJEU stated that the prohibition or restrictions relating to the processing of special categories of personal data, apply also, subject to the exceptions provided for by data protection laws, to the operator of **a search engine**, in the context of his responsibilities, powers and capabilities, **as the controller of the processing carried out in connection with the activity of the search engine**, on the occasion of a verification performed by that operator, under the supervision of the competent national authorities, following a request by the data subject.

Furthermore, according to the CJEU, the operator of a search engine is in principle required to answer to requests for de-referencing in relation to links to web pages containing sensitive data. Nevertheless, the refusal to answer to the request for de-listing of the search engine could be justified by the fact that the processing is lawful, considering the exceptions to the prohibition of processing provided for by EU law, and interpreting these exceptions in light of fundamental rights (with regard to the role of freedom of expression and the balance of that freedom with the right to data protection and to a private life see Chapter 5, §XX).

Impact on the follow-up case:

Council of State, 6 December 2019, No. 401258.

Regarding the "right to de-referencing" of personal data relating to criminal proceedings, the Council of State stated that the provisions of Article 46 of the Law No. 78-17 of 6 January 1978 ensure the implementation in national law of those of Article 10 of the GDPR, which repealed and replaced those of Article 8(5) of Directive 95/46/EC of 24 October 1995. Expressly relying on *GC and Others* (C-136/17), the Council of State affirmed that the two links still in dispute led to web pages containing the words spoken by the applicant in an interview he gave to a magazine with a large circulation about her conviction. Then, the French judge considered that these pages therefore contain information which constitutes personal data relating to the criminal proceedings and that **the interference with the fundamental rights to privacy and protection of personal data of the data subject is likely to be particularly serious because of the sensitivity of such data.** Accordingly, the Council of State affirmed that that it is in principle the responsibility of the CNIL, upon receiving a request for it to give formal notice to the operator of a search engine to de-list links to web pages published by third parties and containing such data, to comply with this request. For an analysis of the impact of the principle of proportionality within the interpretation of criteria to be adopted, according to the Council of State, for balancing fundamental rights at stake, see Question 7 in this chapter.

Elements of judicial dialogue:

GC and Others (C-136/17) followed a leading case on the right to be de-listed: *Google Spain* (C-131/12; for an explanation of the judgement see the Guidelines on the implementation of the CJEU judgment in *Google Spain*" adopted by Article 29 Data Protection Working Party (WP29) in 2014: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf; see also the RE-JUS data protection Casebook, Chapter 6, Question 1 available at: https://www.rejus.eu/sites/default/files/content/materials/rejus_casebook_effective_justice_in_data_protection_.pdf).

In this judgement, the CJEU stated the that the operator of a search engine is a controller within the meaning of EU legislation. Accordingly, the data subject may exercise her rights against that operator, and in certain circumstances, and particularly following a balance of interests, the data subject has a right to be de-listed from the list of results displayed by a search engine. According to the CJEU, such a right can notably also be asserted against the operator of the search engine in a case where the name or

information is not erased beforehand or simultaneously from the web pages to which the list is linked, and even when the publication on those pages was lawful. The data subject may ask to be de-listed on the grounds that the information relating to him should, given the time elapsed since the publication, no longer be linked to his name, unless it should appear that, given the role played by the data subject in public life, such interference with their fundamental rights is justified by the preponderant interest of the general public in having access to the information in question. The Court thus concludes that supervisory or judicial authorities may order the operator of the search engine to remove links to web pages published by third parties containing information relating to a person from the list of results displayed following a search made on the basis of that person's name, without an order to that effect presupposing the previous or simultaneous removal of that name and information — of the publisher's own accord or following an order of one of those authorities — from the web page on which they were published. For the Court, such right to be de-listed is driven by ***the principle of effectiveness***, since, given

"the ease with which information published on a website can be replicated on other sites and the fact that the persons responsible for its publication are not always subject to European Union legislation, **effective and complete protection of data users** could not be achieved if the latter had to obtain first or in parallel the erasure of the information relating to them from the publishers of websites".

With regard to the extension of the controllers' obligations, according to *Google v. CNIL* (C-507/17), the fact that the search engine is operated by an undertaking with seat in a third State does not exempt the controller form the obligations and guarantees laid down by Directive 95/46 and Regulation 2016/679 when processing of personal data for the purposes of that search engine's operation is carried out in the context of the advertising and commercial activity of an establishment of the controller in the territory of a Member State (see, in this respect, Question 1a of Chapter 1).

Furthermore, in relation to the pending case *TU, RE v Google LLC* (C-460/20) the AG in its opinion affirmed that according to Article 17(3) GDPR:

- within the context of the weighing-up of conflicting fundamental rights arising from Articles 7, 8, 11 and 16 CFREU, which is to be undertaken within the scope of the examination of a request for de-referencing made to the operator of a search engine on the basis of the alleged false nature of the information which appears in the referenced content, it is not possible to concentrate conclusively on the issue of whether the data subject could reasonably seek legal protection against the content provider, for instance by means of interim relief. In the context of such a request, it is incumbent on the data subject to *prima facie* provide evidence of the false nature of the content the de-referencing of which is sought, where that is not manifestly impossible or excessively difficult, in particular with regard to the nature of the information concerned. It is for the operator of the search engine to carry out the checks which fall within its specific capacities, contacting the publisher of the referenced web page, where possible. Where the circumstances of the case so indicate in order to avoid irreparable harm to the data subject, the operator of the search engine will be temporarily able to suspend referencing, or in search results to indicate that the truth of some of the information in the content to which the link in question relates is contested,.
- within the context of the weighing-up of conflicting rights and interests arising from Articles 7, 8, 11 and 16 CFR, in connection with a request for de-referencing made to the operator of a search engine seeking to obtain the removal, from the results of an image search carried out on the basis of a natural person's name, of photographs displayed in the form of thumbnails depicting that person, account should not be taken of the context of the publication on the internet in which those thumbnails originally appear.

Moreover, the judgement *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (C-18/18) is of particular interest. In that case, the CJEU addressed the question if the extension of the duties of host providers to remove unlawful information, under Article 15 of Directive 2000/31. In that regard, the CJEU stated that that provision does not preclude a court of a Member State from:
i) ordering a host provider to remove information which it stores, the content of which is identical to the content of information which was previously declared to be unlawful, or to block access to that information, irrespective of who requested the storage of that information;
ii) ordering a host provider to remove information which it stores, the content of which is equivalent to the content of information which was previously declared to be unlawful, or to block access to that information, provided that the monitoring of and search for the information concerned by such an injunction are limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction, and provided that the differences in the wording of that equivalent content, compared with the wording characterising the information which was previously declared to be illegal, are not such as to require the host provider to carry out an independent assessment of that content, and
iii) ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law.
In that case, the Court stated that in order for an injunction which is intended to bring an end to an illegal act and to prevent it being repeated, in addition to any further impairment of the interests involved, to be capable of achieving those objectives **effectively**, that injunction must be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal. The Court affirmed that otherwise, the effects of such an injunction could easily be circumvented by the storing of messages which are scarcely different from those which were previously declared to be illegal, which could result in the person concerned having to initiate multiple proceedings in order to bring an end to the conduct of which he is a victim.
Lastly, in the pending case *Proximus* (C-129/21) the referring Court asked to the CJEU whether Article 17[(2)] GDPR must be interpreted as precluding a national supervisory authority from ordering a provider of public directories and directory enquiry services which has been requested to cease disclosing data relating to an individual to take reasonable steps to inform search engines of that request for erasure. In this respect, the data subject's right to an effective remedy in relation to the right to erasure could play a role in the future CJEU's reasoning, jointly with the principle of proportionality (see Section XX of this Chapter).

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

France[34]
The French case-law before *Google Spain* recognised that the *Google Suggest* service can constitute an offence under press law, when it offers suggestions about a person or a company that can cause prejudice to them[35]. There, judges ruled that the *Google Suggest* algorithm is not automatic, owing to the possibility for Google to ban certain terms or content from its product. Yet, the interpretation of the

[34] Drafted by the students of Master PIDAN (UVSQ)

[35] *TGI* Paris, 15 February 2012, *Kriss Laure/Larry P, Google Inc*

Cour de cassation goes against the decision of the courts of first instance[36], which considered that this service is automated, and thus that *Google* cannot be liable for unlawful content put forward via *Google Suggest*.

After Google Spain, French case law tends to verify the **proportionality** of the rights in issue. There, judges examine the balance between the legitimate interest of the public to know the information published and referenced, and the right of data subjects to data protection.

For this purpose, tribunals and courts examine the veracity, the date of publication, the intimacy and the prejudicial aspect of personal data disclosed[37]. For instance, when an issue concerns the functioning of public institutions, the de-listing would be an infringement of freedom of expression.[38]

For example, a judgment of the *Tribunal de Grande Instance de Paris* refused to order Google to de-list URLs leading to publications concerning the conviction of a doctor, sentenced on 23 December 2015. There, those Internet links allowed the public to be informed about a criminal case that resulted in a significant conviction. Otherwise, the referencing concerned accurate information on a recent event. The processing could not have become inadequate or irrelevant. A balance of interest was preserved between the rights of the person concerned and the legitimate interest of Internet users in expression and information.[39]

The Tribunal uses the same reasoning as the CJEU in the *Google Spain* case but adds that requests to be de-listed are only possible if the search engine has previously been approached and has unlawfully refused.

Judicial tribunals and courts directly refer to the *Google Spain* decision to examine whether the operator of a search engine must be ordered to de-list URLs. The judges specify that Articles 38 (right of opposition for legitimate reasons concerning the processing of personal data) and 40 (rectification or erasure of personal data that is inaccurate, equivocal or outdated) of the Law of 6 January 1978[40] must be interpreted accord to the case law of the CJEU.[41]

One decision by the *Cour de cassation*[42] examined a decision of a court of appeal that considered that a newspaper publisher cannot be forced to delete the reference to a publication on its website, or to make it unaccessible. Thus, the *Cour de cassation* admitted that imposing a modification of the normal reference of a newspaper publisher goes beyond limitations on the freedom of the press. Thus, it seems clear that the right provided under the *Google Spain* case can only be claimed against a search engine provider, and not a newspaper publisher.

---

[36] *C. cass. civ. 1ère*, 19 June 2013, no 12-17.591

[37] See for example, TGI Paris, ord. réf., 24 November 2014; TGI Toulouse, ord. réf. 21 January 2015, Franck J. c.. SARL Google France et Google Inc., légipresse 2015, no 324, p. 107; TGI Paris, ord. réf. 24 November 2014, David T.SA Google Inc., légipresse 2015, no 326-15, p. 209; TGI Paris, ord. réf. 13 May 2016, M. x c. Google France et Google Inc.; TGI Paris, ord. réf. 12 May 2017, Mme. X c. Google France et Google Inc., RLDI, no 138, 1 June 2017. On this issue, see also Anne DEBET, « Mise en oeuvre de Google Spain par les tribunaux français », in Comm. com. électr., no 9, September 2016, comm. 75

[38] In this connection see, *Cour d'appel de Paris*, 28 May 2014, where a judge condemned for corruption asked for the de-listing of a press article on the website of the press editor

[39] *TGI* Paris, 10 February 2017, *M. X c/ Google France, Google Inc.*

[40] *L. n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*

[41] See for example, *TGI* Paris, 10 February 2017, *M. X c/ Google France et Google Inc.*; CA Lyon, 8th chamber, 28 February 2017, RG no 15/05788.

[42] *C. cass., ch. civ. 1ère*, 12 May 2016, no 15-17.729

It can be considered that the decision of the *Cour de Cassation* demonstrates that de-referencing can only be imposed on a search engine, and cannot be applicable to the people generating the information. This is based on the principle that the modification of a normal reference in a press organ (website archives) goes against the freedom of the press, even though an infringement could undermine the rights of a person who would be justified in asking for the de-listing of the press article highlighted by a search engine.

Judges also use the same construction as in the *Google Spain* case. They consider that a search engine provider cannot be liable for defamatory statements contained in links it has referenced.

The French decisions have also ruled that Google France, the French establishment of Google Inc., is to be held responsible for the data processed by Google Inc., after an economic analysis of the activities of the French establishment.[43]

French administrative courts also hear cases concerning the de-listing of personal information. In this regard, the assembly of the *Conseil d'État* directly refers to the Google Spain case.[44] Judges were required to examine the refusal of Google Inc. and the French administrative authority to de-list several links redirecting to websites concerning personal data of data subjects. The *Conseil d'État* first recalls that the right to be de-listed is recognized by the *Google Spain* case, as the right to seek the removal by a search engine provider of information that could infringe privacy, reputation and personal data protection. Here, the courts emphasise that this right is not absolute and can be balanced by the right to information.

Confronted with several issues of interpretation, the *Conseil d'État* asked for a preliminary ruling by the European Court of Justice, seeking clarification of the obligations of search engine providers to de-list, notably concerning sensitive data, which were not covered by the *Google Spain* judgment. It did not discuss whether there should be an automatic de-listing of sensitive data.

In the same way, the *Conseil d'État* also submitted several questions for preliminary ruling to the CJEU, before deciding whether Google must 'de-list' information on all extensions of its search engine, or in some countries only.[45] In this case, the French data protection authority ordered Google to apply the removal to the list of results obtained from a search, and also to all extensions of Google's domain name.

Yet French judges have allowed some exceptions. The *Conseil d'État* (*Conseil d'État, sous- sections 2 et 7, 15 février 2016, n°389140*) considered that a decree establishing a procedure to block access by Internet users to websites with child pornography or which encourage terrorism, is justified by legitimate interests. There, the decree allows an administrative authority to ask the publisher or website host to de-list the unlawful content.

Still, even if courts allow injunctions against a publisher of content or against a website host, the de-listing only applies to illegal content, not content referring to personal information, such as in the *Google Spain* case.

<u>On other types of remedies:</u> *Cour de cassation*, commercial chamber 25 June 2013, no 12-17037:

Even if the law does not expressly so state, the sale of a file including personal data that has been unlawfully collected and processed (no declaration to the French data protection authorities) is void since the object of the sale -- the undeclared processing of data -- is unlawful and thus cannot be seen as being available for trade.

---

[43] *TGI* Paris, 16 September 2014, *M. et Mme. X et M. Y c/ Google France*

[44] See, for instance, *Conseil d'État*, plenary session, 24 February 2017, *Mme. Chupin et autres*, no 391000; *Conseil d'État,* 19 July 2017, *Google Inc.*, no 399922

[45] *Conseil d'État*, 19 July 2017, *Google Inc.*, no 399922

This decision implicitly relies on the principles of effectiveness and dissuasiveness since it deprives a file including unlawfully processed personal data of any commercial interest. From the perspective of the principle of effectiveness, a parallel issue arises as to whether invalidity of a contract represents an adequate remedy as an *ex post* measure where it might not prevent the material transfer of data, albeit subject to subsequent "restitution". Indeed, data protection is a field in which the civil remedies normally applied to market transactions may fail to effectively protect the personal interests at stake.

Italy[46]

The Italian case law before *Google Spain* appeared to be fairly strict in assessing the obligations owed by search engine providers. Such providers were indeed regarded as mere "intermediaries", which could not be held responsible for the processing and publishing of personal data by the "source websites". Thus, the obligation to ensure that the data processing was in accordance with the relevant legal provisions rested only on the shoulders of the publishers of the data (i.e., the source websites).[47]

By contrast, Italian case law after *Google Spain* unanimously embraces the view, upheld by the CJEU, that search engine providers must be regarded as data controllers. Moreover, when the provider has its own subsidiary set up in a Member State, which only engages in marketing activities and thus not the finding, indexing and storing of information on the internet — which are instead carried out by the parent company situated outside the EU – such provider can nevertheless be regarded as subject to EU law[48] according to Article 4 of Directive 95/46. It is worth mentioning, nonetheless, that the Italian decisions based their reasoning also on the circumstance that the NDPA decision of 10 July 2014, referring to an official 2010 determination by Google Inc., ruled that Google Italy S.r.l., should be considered as the Italian representative of Google Inc., for the purposes of the legislation concerning data protection (i.e., Legislative Decree no 196/2003).

The Italian case law also contains an interesting development with regard to the obligations owed by an internet service provider (ISP) such as the manager of a social network service (i.e., Facebook) employed by third parties to process and publish personal data (the so-called "hosting providers"). A decision from an Italian court[49] ruled that, whereas Directive 2000/31 on electronic commerce — to which ISP are subject — explicitly excludes the liability of the provider engaging in activities of *mere conduit*, caching and hosting, the provider must instead be regarded as liable when, after being informed of the publishing, on its own hosting platform, of information not compliant with the data protection provisions, it does not ensure, even without a specific order from the authorities, that such information is removed. In other words, while there is no *ex ante* obligation on the ISP to control the content of the information published, a proper balancing between the right to information and the right to data protection, as laid out by the CJEU in *Google Spain*, can only occur when the provider plays an active role, thus intervening, *ex post*, in order to remove information not compliant with the data protection legislation and contested by the data subjects. As a consequence, it should be pointed out that the Italian

---

46 Drafted by Gianmatteo Sabatino and by C. Angiolini

47 See Court of Cassation, decision no 5525/2012

48 See, in particular, Milan *Tribunale*, decision of 5 October 2016 and decision no 618 of 2014 of the Italian National Data Protection Authority. Both decisions upheld that Google Italy S.r.l. could indeed be considered as representative of Google Inc. in Italy. On the issue, see also RICCIO, *Il difficile equilibrio tra diritto all'oblio e diritto di cronaca*, in *Nuova Giur. Civ.*, 2017, 4, 549.

49 North Naples Tribunal, decision of 3 November 2016.

courts have devised a "double level of protection"[50] for subjects whose data is published on the internet and indexed by search engines: on the one hand these subjects can directly ask the Internet Service Provider (such as a search engine provider) to prevent personal data from being too easily accessible to the public and, as already pointed out, this request will be fulfilled by removing the websites containing contested information from the results displayed by inserting the data subject's name in the search engine research bar[51]; on the other hand, any complaint regarding the erasure, removal or adjustment of information must be addressed to the publisher of such information,[52] since that is the party solely responsible for the content of the information displayed.

Moreover, the Court of Cassation in its decision n. 19681/2019, expressly mentioning *Google Spain* (C-131/2012) affirmed that with regard to the relationship between the right to be forgotten and the right to the historical evocation of facts and events concerning past events (as part of the freedom of expression), the mention of personal data concerning persons who were protagonists of those facts and events is lawful only in the hypothesis in which that information refers to people whose activities in the present moment is in the interest of the community, both for reasons of fame and for the public role covered. Otherwise, the right of the interested parties to confidentiality with respect to past events that may hurt them in dignity and honour and of which the collective memory is now extinguished would prevail.

The Court of Cassation, in its decision n. 9147/2020, relying on *Google Spain* (C-131/12) and on *GC and Others* (C-136/17), stated that the right to be forgotten consists in not being exposed without time limits to a representation of one's person that is no longer current, with prejudice to reputation and confidentiality, due to the republication, after an important time interval, of a piece of news relating to past events. The Court pointed out that the protection of the mentioned right has to be balanced with the public interest to the knowledge of the fact (freedom of expression), also considering the need of preservation of the news for historical-social and documentary purposes. Furthermore, the Court stated the result of the above mentioned balance may the de-listing of the article from a search engine, without the erasure from the newspaper webpage. In this respect, in its decision no. 15160 of 31 My 2021, the Court of Cassation, relying on European case law, stated that the right to be forgotten must be considered in strict connection with the rights to privacy and personal identity and that in balancing the public interest in information and personality rights, the former becomes recessive when the information is illicit, false, or unsuitable to provoke or feed a debate on events of public interest, for historical, scientific, health or national security reasons (this last requirement requires the quality of public character of the subject to whom the events in question refer. In the absence of at least one of these requirements, the conservation of the information in the database is unlawful, and the data subject may request for the erasure of the data, to which the service provider is obliged to give effect. Furthermore, the Court stated that where there is a public interest in the news, the data subject, whose data are not indispensable for the purposes of the accessibility of the news on the database, can request

---

[50] See RUSSO, *Diritto all'oblio e motori di ricerca: la prima pronuncia dei tribunali italiani dopo il caso Google Spain – Il commento, in Danno e Resp.*, 2016, 3, 299.

[51] The connection between the results displayed and the name inserted in the search bar must be interpreted broadly: for instance, when a web page containing contested information is displayed as a result of inserting in the search bar the name of the data subject plus some additional related terms, the request for the removal of such results is still admissible and can be scrutinised and upheld by the NDPA or a Court when the ISP does not comply. On this issue, see Italian NPDA decision no 277 of 15 June 2017.

[52] See Rome *Tribunale*, decision of 3 December 2015.

and obtain the "de-indexing", thus balancing freedom of expression with personality rights (On balancing fundamental rights at stake see also: Cass., No. 7559/2020; Cass. No. 19 May 2020 no. 9147). Moreover, regarding the data subject's request, in its decision no 20861, 21 July 2021, the Court of Cassation stated that the request for de-indexing requires the precise identification of the search results that the plaintiff intends to remove, and therefore, normally, the indication of the URL, of the contents relevant for this purpose, even if it is not excluded that a precise representation of the single information that is associated to the keywords may prove, according to the circumstances, suitable to give precise knowledge of the thing that is the object of the request, so as to allow the defendant to provide adequate and precise defences on the point.

Furthermore, on the basis of what the CJEU established in *Manni* (decision of 9 March 2017, C-398/15), the Court of Cassation, in its decision no 19761/2017, considered that with the establishment of the business register and the exclusion of a rule of exception, as required by the CJEU, the Italian legislature had achieved a correct balance between individual and collective needs. Therefore, the Court upheld the legitimacy of registering and retaining in the register information relating to the role of administrator and liquidator performed by a person in a company, even if the company went bankrupt and was struck from the register, as the requirements of business registration must prevail over the private interest in preventing its functioning, and also to satisfy the need for certainty in commercial relations addressed by the setting up of the business registry. The decision expressly refers to the *Google Spain* judgment and to the provisions of the ECHR.

With regard to *Eva Glawischnig-Piesczek* (C-18/18) the decision of the Tribunal of Milan with regard to the appeal against the order no. 15584 issued on 10.5.2019 by the Italian DPA is of particular interest. In that case, the Tribunal, relied on the CJEU case C-18/18. The Italian court, with reference to the identification of the person required to delete the data, considered that Facebook Ireland provides hosting services in accordance with Article 14 of Directive 2000/31, and that the purpose of Article 14(1) of the directive is to exempt the hosting service provider from liability if it meets one of the two conditions listed in that provision, namely a) not being aware of the unlawful activity or information, or b) acting immediately to remove such information or to disable access to it as soon as it becomes aware of it. The Court stated than that according to Article 14(3) of Directive 2000/31, read in light of recital 45 thereof, this exemption is without prejudice to the possibility for national courts or administrative authorities to require the hosting service provider concerned to bring an infringement to an end or to prevent it, including by removing or disabling access to the unlawful information. Therefore, the Court, relying on *Eva Glawischnig-Piesczek v Facebook Ireland Limited*, (C-18/18) ordered Facebook Ireland Ltd to remove and block all unlawful Facebook posts containing personal data relating to children.

POLAND

Typically, claims for content removal arising from the online publication of personal information are based not on the data protection law, but rules on infringement of personality rights (Article 23 and 24 of Polish Civil Code). Under these provisions the person can request removal (or de-listing) of the content (also personal data) from e.g., a given online platform.

However, there are numerous issues — both related to the procedural technicalities and the court's approach — that undermine the effectiveness of such a claim in practice.

The optimal starting point for the analysis of Polish case law related to the right to be forgotten is the case of Tadeusz Węgrzynowski and Szymon Smolczewski ended by judgment of the ECtHR of 16.7.2013 (Action no. 33846).[53] The dispute started with a publication of article which caused damage to the

[53] In the case the judicial dialogue between Polish national courts and European courts (namely: European Court of Human

reputation of the applicants. After winning a case against the journalists who wrote the text Mr Węgrzynowski and Smolczewski found that it was still accessible on journal's website and requested its removal. Polish courts dismissed the claim due to the *res indicata* principle. However, it was underlined that removal of the article would amount to censorship and to rewriting history and was not justified anyway — in such a case it would be appropriate to supplement the text with a link to the information on the first judgement. This manner of balancing between the rights guaranteed under Article 10 (freedom of expression) and under Article 8 (right to respect for private life) of the Convention was approved by the ECHR.

A similar approach was adopted in the Judgement of Court of Appeal in Warsaw, I ACa 74/14, issued shortly after CJEU's award in *Google Spain*.[54] The court ascertained that the publisher of the website does not have to remove from it the archival publication containing outdated and unflattering information about the person who requests it. Accepting such a way would in fact be an unlawful form of censorship and interference with the autonomy of the press, expressed in the possibility of collecting and archiving journalistic materials.

The next judgement of the right to be forgotten in the online environment illustrates how problematic its realisation might be.[55] In this case the applicant requested the defendant to "take steps to remove a telephone recording from web portals, including in particular requesting the owners or administrators of portals for this purpose". His request, however was not granted due to the fact that its imprecision rendered its execution impossible.

The analysis of the judgement allows to identify what are the main **practical obstacles of the application of the right to be forgotten** in case of online materials according to the Polish judiciary.[56] The first difficulty lies in the accuracy of the claim request as well as the precision[57] and independence of the decision on that request, the second — editing the operative part of the judgment in a way that enables its concretisation by either party; deciding when the behaviour of third parties, not controlled by the defendant, can be seen as a result of the violation of the good by the latter (e.g., sharing content by others); determining the activities that the plaintiff may require under Article 24 of the Civil Code (what can be classified as a measure to remedy the effects of the infringement). Yet another issue is the liability limitation of the entities intermediating in sharing content provided by the rules on online service providers.

A change in the manner of approaching claims related to the right to be forgotten is to be observed in the judgement of Supreme Administrative Court, I OSK 2926/13, 9 April 2015,[58] which — in contrast to the previous judgements — explicitly refers to the ***Google Spain*** case. The claim was lodged against an operator of an internet browser, which allows to access entry to an online encyclopaedia on the

---

Rights can be observed. https://trybunal.gov.pl/uploads/media/Sprawa_Wegrzynowski_i_Smolczewski_przeciwko_Polsce__skarga_nr_33846_07___wyrok_z_dnia_16_lipca_2013_r..pdf

[54] 17 June 2014. http://orzeczenia.waw.sa.gov.pl/content/$N/154500000000503_I_ACa_000074_2014_Uz_2014-06-17_001.

[55] Judgement of Supreme Court, II CSK 747/13, 14 January 2015.

[56] See : B. Baran, K. Południak-Gierz, Perspektywa regulacji prawa do bycia „zapomnianym" w Internecie. Zarys problematyki, Zeszyty Naukowe Towarzystwa Doktorantów UJ Nauki Społeczne, No 17 (2/2017), p. 139-159. https://depot.ceon.pl/bitstream/handle/123456789/13711/Baran,%20Po%20udniak-Gierz%20Perspektywa%20regulacji%20prawa%20do%20bycia%20zapomnianym.pdf?sequence=1

[57] This issue appeared also in the Judgement of Court of Appeal in Warsaw, 15 February 2017, VI ACa 1935/16. In the opinion of the regional court, the request to remove the articles from the defendant's website was unfounded, since the entire publication could not be considered as prejudicial to the plaintiff's personal rights — the plaintiff should have indicated relevant fragments of the article in his request.

[58] https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/i-osk-2926-13-wyrok-naczelnego-sadu-administracyjnego-522555584.

claimant (the latter has not been generated by the browser operator). The court addressed the issue of the territorial scope of the right to be de-listed. It ascertained that — under the Google Spain doctrine — the geographic "location" of data or its processing cannot affect the possibility to claim that this data is removed from the search results. Thus, storing data on a server located abroad neither excludes Polish jurisdiction nor influences the applicability of the right to be forgotten. The Court underlined that it should be verified whether the processing of data cannot be understood as "creation of such technical premises, that make it *de facto* possible to get access to personal data without their physical retention." By this the Court reinforced the view that trans-border data processing can take a form of analysis and display of data — it is not necessary to determine the physical (geographic) location of the data storage. This line of reasoning was followed in the subsequent judgement (Judgement of Court of Appeal in Warsaw, 27 August 2015, II SA/Wa 900/15), in which the case was re-examined. The fact that the data processed are not stored by the processing entity does not in itself exclude the possibility of recognising this entity as their administrator as it would allow to easily circumvent data protection law.

Another issue is that **the removal claims are in Poland mostly based on the rules on personality rights which are not appropriate to guarantee personal data protection**. Here, the key judgement was issued by the common court (see: Judgement of District Court in Warsaw, 12 October 2015, I C 1164/13). Here the claimant requested obliging the defendant to remove the consequences of the violation of the plaintiff's personal rights by ceasing to display in the search engine — after entering the name, surname and place of residence of the plaintiff — a link to a particular website and a fragment of press material appearing at the indicated reference. The way of display of data suggested that claimant is a gangster whereas he participated in crushing a criminal group, which was obvious from the text to which the link lead. Though the claim was based on the personality rights protection regulation (Article 23 and 24 of Polish Civil Code), the court underlined that the functioning of a search engine operator is based on personal data processing and, thus, the operator can be considered to be the data controller within the meaning of the Article 2 letter d of the directive 95/46. The premises of claims related to the infringement of personality rights are as follows: either the infringement of personality rights or their endangerment, and illegality (understood as being contrary to the legal order or principles of social coexistence) of the infringer's actions. In the case at hand defendant's actions could not have been considered illegal. When the user enters the search into the search engine window, the search engine identifies and displays search results at specific positions according to its own algorithms that have been developed to identify relevant and useful search results. Shaping the content of links and descriptions (snippets) from search results lies primarily with entities administering websites displayed on search results lists. The search results and snippets therefore do not contain any statements from the search engine operator. Thus, the defendant cannot be held responsible for thereof. Secondly, the infringement of personality right of the claimant was not significant and temporary. In light of the above, the claim was dismissed by the court of the first instance.

The court of appeal, basing on the ***Google Spain*** judgement, challenged this way of reasoning,[59] underlining that the fact that the search results create a negative picture of the person, while the article towards which the link leads does not, is sufficient to conclude that the search results infringe claimant's personality rights (reputation). Though the display for search results for a phrase containing the name, surname and place of residence of the plaintiff was lawful, and the publication of the article itself did not infringe the plaintiff's personal rights, it was still justified to request removal of a particular link from the displayed list of search results, especially that the search results infringed his reputation. Secondly, the search engine operator, by setting the mechanisms of search results display, can be held liable for thereof (as the personal data controller) and is obliged to remove a link in question if processing of personal data is contrary to the data protection regulation. Not fulfilling this request rendered his behaviour illicit in

[59] Judgement of Court of Appeal in Warsaw, I ACa 2462/15,3 April 2017.

light of the Article 23 of Polish Civil Code. Finally, the removal of links should not be seen as a censorship, but as a proportionate remedy for personal rights infringement.

The dispute reached the third instance and was sent by the Supreme Court for re-examination after GDPR came into force.[60] The focal point of the justification of the award is **the interplay between the personality rights and personal data protection regimes**. The personal data are not personality rights, though can be seen as elements of the identity and privacy. Due to the relationship between personal data and some personality rights, the application of the provisions on the protection of personality rights may, in certain situations, ensure protection of personal data, and *vice versa*. However, this does not change the fact that the person seeking protection under Articles 23 and 24 (and 448 in case of compensation) of Polish Civil Code must prove that its requirements are met. The fact that, when the redress is sought within personal data protection regime — in light of the *Google Spain* judgement "the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful" does not mean that the same scope of protection can be obtained by a person who asserts claims against the internet search engine operator in the regime of personality rights protection identifying the infringed right as the reputation, not privacy. The Court did not observe infringement of the former, as it ascertained that the content displayed as a search result, though suggesting that the claimant was a gangster did not have a negative impact on his good name and reputation, as the Internet users are aware of the automatic way of functioning of the browser and does not attribute value to the snippets but verify the information on the page to which the link leads. Thus, the judgement of the Court of Appeal was set aside and the case was submitted for re-examination.

The interplay between the data protection rules and protection of personality rights regulation was also addressed in the judgement of Court of Appeal in Warsaw, I ACa 1565/15, issued on 25 November 2016.[61] Firstly, the court underlined that these protective regimes are independent from each other. In order to verify whether the publication of personal data constitutes an infringement of personality rights (in this case: reputation) and therefore justifies removal or compensation claim, it is crucial to prove that the information is false or outdated. In contrast, this might not be necessary when the person bases their claim on the data protection rules. Also, the fact that personal data is processed without the consent of the person concerned does not in itself constitute the infringement of personal rights and protection under Article 23 and 24 of Polish Civil Code. Finally, in light of the provisions on the liability of provider of electronic services, the Internet operator's liability for processing or storing unlawful personal data is excluded unless he knew that the data processing was illegal.

Another matter which caused difficulties to the Polish courts **was establishing the person against which the delisting claim should be directed** (see: Judgement of District Administrative Court in Warsaw, 20 March 2018, II SA/Wa 1035/17). In the case at hand the decision of the data protection authority (Generalny Inspektor Ochrony Danych Osobowych) obliging limited liability company based in W. remove personal data of M. K. from search engine results was challenged based on the argument that this entity does not process nor is involved in processing of personal data by the search engine. The data protection authority claimed that the company should be considered an entity established by the search engine operator. In cases concerning complaints of natural persons residing in Poland about the refusal to delete their personal data disclosed in search results in the internet search engine, the decisions

---

[60] Judgement of Supreme Court, I CSK 690/17, 13 December 2018, http://www.sn.pl/sites/orzecznictwo/Orzeczenia3/I%20CSK%20690-17-1.pdf

[61] https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/orzeczenia-sadow/i-aca-1565-15-wyrok-sadu-apelacyjnego-w-krakowie-522099694

can be directed to this Polish based company as the entity established by the search engine operator, not the search engine operator established abroad. The court ascertained that the decision should be addressed to the personal data controller, as only he can be requested for de-listing of certain content and this entity was not established in the proceeding. The processing of personal data takes place as part of the activities carried out by the data controller responsible for this processing in the territory of a given Member State, if the operator of an internet search engine establishes a branch or a subsidiary in a given Member State, whose purpose is to promote and sell advertising space offered for through this search engine, and the activities of this branch or subsidiary are targeted at people residing in that country. In this case, the data protection authorities are entitled to issue a decision against the search engine operator as the data processing in takes place in that member state. It does not however, mean, that the decision of this authority can be directed to the branch or subsidiary of the search engine operator in that Member State.[62]

After GDPR came into force, another issue emerged that is: **in case of the claim of personal data removal based on the data protection rules, which courts should have material jurisdiction**? This question was addressed by the District Court in Łódź in the judgement issued on 25 July 2019, III Ca 396/19. Firstly the court observed that, though on certain occasions personal data processing might lead to the infringement of personality rights, in situations in which data processing (even unlawful) does not infringe personality rights, the data subject should request their removal from the database in an administrative proceeding. Thus, in such cases the administrative courts have jurisdiction, not the common courts. This conclusion, though accurate at the time of lodging the claim, became inaccurate with the GDPR's entry into force on 25 of May 2018, as the Court found. Article17 clause 1 point d of GDPR provides that the data subject has the right to request the administrator to immediately delete personal data concerning him, and the administrator is obliged to delete the data without undue delay if they were processed unlawfully. At the same time Article 79 paragraph 1 of GDPR grants such a person — without prejudice to available administrative or extrajudicial remedies (including the right to lodge a complaint with a supervisory authority) — the right to an effective remedy before a court. Therefore, the judicial protection provided for in the latter provision also applies to the exercise of the right of the person to whom the personal data pertains to demand of data removal. There is no doubt that such a request was made by the plaintiff in this case. The Polish provisions implementing the GDPR provide that to the extent not covered by Regulation 2016/679, to claims for violation of the provisions on the protection of personal data, the provisions of the Polish Civil Code shall apply. Thus, Article 79 of GDPR provides for a new civil law claim, independent for the protection of personality rights. This claim can take different forms, including the one specified in the Article 17 of GDPR. Also, in case of proceedings initiated by lodging such a claim, the provisions of the Polish Code of Civil Procedure shall apply. Therefore, from 25 May 2018 this case has become a civil law case within the meaning of Article 1 of the Code of Civil Procedure and the common courts have jurisdiction in this regard.

[62] Same reasoning in: Judgement of District Administrative Court in Warsaw, 24 July 2018, II SA/Wa 1332/17.

7.2.2. Question 2: Effective remedies and the principle of full compensation

In order to ensure the effective protection of personal data within the EU and full compensation of victims, should courts award compensation for material and non-material damages for any infringement of EU data protection law regardless of whether specific harm is found to have been caused by the infringement?

A focus on compensation under the GDPR:

Article 82 GDPR provides that any person who has suffered material or non-material damage as a result of an infringement of the Data Protection Regulation shall have the right to receive compensation from the controller or processor for the damage suffered. More precise provisions follow, distinguishing between the controller's and processor's liability. The burden of proving the absence of liability is placed on the controller/processor, similarly to what was provided in the 95/46/EC Directive.
Unlike other pieces of EU legislation (compare, e.g., the Antitrust Damages Directive) there is no provision for the principle of full compensation. By contrast, compensation for non-material damages is specifically provided for.
How to deal with non-material losses is a matter on which national legislation is applicable, possibly leading to different outcomes depending on legal traditions and rules, including those dealing with punitive damages and any sanction-like function of damages. Together with national specificities, the principles of effectiveness, proportionality and dissuasiveness may play a major role in this respect. On the one hand, overcompensation may be banned under the principle of proportionality (see, again, for comparison, article 3, Antitrust Damages Directive); on the other hand, punitive damages may be used within certain limits to increase deterrence and, to some extent, effectiveness.

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

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

Relevant EU case law

➢ Judgment of the EU Civil Service Tribunal (First Chamber), 5 July 2011, Case F 46/09, *V. and EDPS v European Parliament*

➢ Judgment of the General Court (Sixth Chamber), 3 December 2015, Case T 343/13, *CN and EDPS v European Parliament*

➢ Request for a preliminary ruling from the Varhoven administrativen sad (Bulgaria) lodged on 2 June 2021 — *VB v Natsionalna agentsia za prihodite*, Case C-340/21, (**VB**) [pending]

➢ Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 12 May 2021 — UI v Österreichische Post AG, Case C-300/21 (**UI**) [pending]

➢ Request for a preliminary ruling from the Landgericht Saarbrücken (Germany) lodged on 1 December 2021 — GP v juris GmbH (Case C-741/21), (**GP**) [pending]

Relevant national case law

➢ Judgement of the Italian Court of Cassation (Corte di cassazione), Third Civil Chamber, 15 July 2014, n. 16133 (University of "Rome Three" v. Pieraccini et al.)

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

➢ Judgement of the Italian Court of Cassation, 20 August 2020, n. 17383

Relevant legal sources:

EU Level

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

See, for comparison, article 82, GDPR

National Level

Legislative Decree n. 196/2003, Italian Data Protection Code, implementing article 95/46/EC Directive

Article 15

This provision admits a claim for damages for economic and non-economic loss by referring to Civil Code article 2050 on liability for dangerous activities. That article makes those who carry on dangerous activities liable for damages caused unless they prove they adopted all necessary measures to avoid the occurrence of those damages.

The case(s):

Three university students filed a complaint with the Tribunal of Rome since their names were included in an Excel file listing 3724 students enrolled at the University, showing their personal data, including tax codes, University student status, employment positions and wage status. The file could be accessed via Internet by a Google search based on the students' names. The Tribunal found there was an infringement of the Italian Privacy Code (the data processing being disproportionate in respect of the aim pursued), ordered the personal data to be taken down from the web and awarded €3,000 in damages for non-economic loss to each plaintiff.

The case was brought before the Court of Cassation by the University of Rome, which challenged the decisions by lower courts especially in regard to the award of damages for non-economic loss, as its seriousness or gravity were not ascertained.

Reasoning of the Court:

Relying on its previous case law (see partial decision no 26972/2008 by Joint Chambers), the Court stated that non-economic losses may be recovered only if: i) fundamental rights are violated or the law expressly allows for recovery of non-economic losses, ii) the infringement is serious and iii) the damages are not trivial (*"futili"*). Damages have to be proved and may not be ascertained *ex se* (automatically). The criteria of seriousness of infringement and gravity of consequences are based on a balance between the principle of solidarity towards the victim and the principle of tolerance imposed within human society. Reference is made to Article 2 of the Constitution, on the protection of fundamental rights and the principle of solidarity, as well as to the case law of the ECtHR (decision no 77/07, 7 January 2014) with regard to the principle of "*de minimis non curat praetor*" (the judge does pay attention to trivial matters), intended as a "European rule of tort law".

Moreover, the Court establishes a link between the principles of solidarity and of effectiveness (of fundamental rights). Indeed, the effective protection of these rights through compensation becomes sustainable within society only if the infringement is serious and the consequences are not trivial.

The Court also highlights the distinct role of injunctions and damages, and the possibility of a modular enforcement in which the remedial response is adjusted against the material needs of protection of the victim. Whereas injunctions mainly have a preventive function, damages will be used only if prejudice is concrete, effective and substantial.

Conclusion of the Court:

The Court concludes that in data protection cases, non-economic losses may be recovered if the infringement is serious and the consequences are substantial and concrete.

Elements of judicial dialogue:

- *Horizontal dialogue (national level)*

The decision follows the position taken by the Italian Court of Cassation in the last 10-15 years on compensation for non-economic damages (see partial decision no 26972/2008 by Joint Chambers). It is confirmed by recent judgements. For example, in the decision no. 3311/2017, upholding a decision dismissing a data subject's claim for damages suffered by having received ten unsolicited email messages in three years. In that case the Court additionally condemns the claimant for abuse of the process of the court under article 96 of the Italian civil procedure code. More recently, in its decision of 20 August 2020, n. 17383 the Court of Cassation reiterated that, with regard to non-economic damages, the violation of the fundamental right to the protection of personal data is subject to compensation only if the breach is serious and the consequences of that breach (the damage) are of significative gravity (see also: Cass. 27301 of 7 October 2021; Cass. No. 16402, 26 February 2021).

As to other countries, as the following decisions are of particular interests:

Germany:

- judgement of Amtsgericht Diez, 07-11-2018, 8 C 130/18 (claimant received spam email and asked for compensation of 500 EUR, and the court held that the infringement of GDPR without damages as a consequence thereof does not give rise to a claim for damages and that "minimal damages" do not give raise to damages under Article 82 GDPR);
- judgement of Amtsgericht Bochum, 11-03-2019, 65 C 485/18 (A misdirected email does not constitute a damage for the purposes of Article 82 GDPR.);
- judgement of Oberlandesgericht Dresden, 4. Zivilsenat, Beschluss vom 11-06-2019, Az.: 4 U 760/19 (a minor loss does not give rise to claims for non-material damages under 82 GDPR);
- Landgericht Karlsruhe; 02-08-2019; 8 O 26/19 (a mere infringement of GDPR provisions does not give rise to the claims under Article 82 of GDPR); - judgement of Landsgericht Munich, 07.11.2019, 34 O 13123/19 (damage claim cannot be justified only by the fact that personal data processing was contrary to data protection provisions).

Austria:

- judgement of Oberlandesgericht Innsbruck; 13-02-2020 ("A data protection violation must in any case intervene in the emotional sphere of the victim, … a minimum level of personal impairment will have to be required for the existence of non-material damage")

Netherlands:

- judgement of Rechtbank Overijssel; 28-05-2019; AK_18_2047 (500 EUR of damages awarded for sharing a document without required anonymization — pursuant to article 82 of GDPR and national provisions of Civil Code);
- judgement of Rechtbank Amsterdam; 02-09-2019; 7560515 CV EXPL 19-4611 (damages of 250 EUR awarded — pursuant to article 82 of GDPR and national provisions of Civil Code);
- judgement of Rechtbank Noord-Nederland; 15-01-2020; C / 18 / 189406 / HA ZA 19-6 (All damage should be compensated and the concept of damage should be interpreted broadly — rejection of claim should not be based on the fact that the damage cannot be precisely specified or is relatively small.);

United Kingdom:

- the decision of the Court of Appeal in Lloyd v Google LLC [2019] EWCA Civ 1599 (02 October 2019) (damages can be claimed also when there was no pecuniary loss or distress (under the provisions implementing directive 95/46).

Poland:
On the one hand, compensation claims based solely on the infringement of data protection rules have not been found. There are no judgements where the claim would be based on Article 82 of GDPR. However, there is a substantial amount of cases in which the publication of content (e.g., personal data) constituted an infringement of personal rights[63]. In these instances the court focused on the protection of personal rights and compensation for harm caused by it, not compensation for infringement of data protection rules. The issues concerning the non-material character of damage and the doubt as to what may constitute the harm in a particular situation are discussed by the judiciary.

As a rule, the courts did not take into consideration the possibility of awarding compensation for non-material damages for any infringement of EU data protection law regardless of whether specific harm is found to have been caused by the infringement.

- *Vertical dialogue (between EU and national courts) and horizontal among foreign national courts*

The judgment examined here also refers to the case law of the ECtHR (decision no 77/07, 7 January 2014) with regard to the principle of "de minimis non curat praetor" (the judge does pay attention to trivial matters), intended as a "European rule of tort law" followed in other EU jurisdictions either in legislation or case law.
Moreover, though not referred in the judgment examined; other decisions of EU courts are worth mentioning in the field of compensation of data subjects for non-material damages. In particular, in Case F 46/09 (*V. and EDPS v European Parliament*), the EU Civil Service Tribunal addressed the issue of whether the annulment of an act of the Parliament (namely, a decision refusing an offer of employment based on the unlawful processing of medical data of the candidate) may in itself constitute appropriate and, in principle, sufficient reparation for non-material damage and, if not, how non-material damage should be assessed. Based on long standing EU case law, the Tribunal concludes that the annulment of the administration's unlawful act cannot constitute full reparation for the non-material damage: (*i*) if that act contains an assessment of the abilities and conduct of the person concerned which is capable of offending them (see judgment of 7 February 1990 in Case C 343/87 *Culin v Commission*, paragraphs 25 to 29, and in *Pierrat v Cour de Justice*, paragraph 62); (*ii*) where the illegality committed is particularly serious (judgments of 30 September 2004 in Case T 16/03 *Ferrer de Moncada v Commission*, paragraph 68, and of 7 July 2009 in Joined Cases F 99/07 and F 45/08 *Bernard v Europol*, paragraph 106); (*iii*) where the annulment of an act has no practical effect. Since the non-material damage to the applicant is not entirely compensated for by the annulment of the decision at issue, the Tribunal engages in an assessment of the fair amount of compensation the Parliament must pay to the applicant for that damage, in the light, in particular, of the *illegalities* established and of their *consequences*. These two elements resemble the assessment criteria used in the Italian decision examined above.

[63] Judgement of the Court of Appeal in Warsaw, 25-11-2016, I ACa 1565/15, judgement of the Supreme Court, 13-12-2018, I CSK 690/17, judgement of the Supreme Court, 28-09-2011, I CSK 743/10, judgement of the Court of Appeal in Cracow, 22-12-2016, I ACa 1080/16, judgement of the Court of Appeal in Bialystok, 30-09-2015, I ACa 403/15, judgement of Court of Appeal in Warsaw, 3 April 2017, I ACa 2462/15, judgment of the Polish Supreme Court, 15 May 2019, II CSK 158/18.

Moreover, the pending case *VB* (C-340/21) concerning the interpretation of Article 80 GDPR is of particular interest with regard to non-material damages. In such a case, the referring court asked to the CJEU whether, according to Article 82(1) and (2) GDP, read in conjunction with recitals 85 and 146 thereof, in a case involving a personal data breach consisting in unauthorised access to, and dissemination of, personal data by means of a 'hacking attack', the worries, fears and anxieties suffered by the data subject with regard to possible misuse of personal data in the future fall *per se* within the concept of non-material damage, which is to be interpreted broadly, and entitle them to compensation for damage where such misuse has not been established and/or the data subject has not suffered any further harm.
Furthermore, in the pending case *UI* (C-300/21) the national Court asked to the CJEU the following questions:
"1. Does the award of compensation under Article 82 of Regulation (EU) 2016/679 (1) (the GDPR) also require, in addition to infringement of provisions of the GDPR, that an applicant must have suffered harm, or is the infringement of provisions of the GDPR in itself sufficient for the award of compensation?
2. Does the assessment of the compensation depend on further EU-law requirements in addition to the principles of effectiveness and equivalence?
3. Is it compatible with EU law to take the view that the award of compensation for non-material damage presupposes the existence of a consequence of the infringement of at least some weight that goes beyond the upset caused by that infringement?"

Lastly, in the pending case GP (C-741/21) the referring court asked to the CJEU whether
i) In light of recital 85 and the third sentence of recital 146 GDPR, the concept of 'non-material damage' in Article 82(1) of the GDPR covers any impairment of the protected legal position, irrespective of the other effects and materiality of that impairment?
iii) it is permissible or necessary to base the assessment of compensation for non-material damage on the criteria for determining fines set out in Article 83 of the GDPR, in particular in Article 83(2) and 83(5) of the GDPR?
iv) the compensation must be determined for each individual infringement, or are several infringements — or at least several infringements of the same nature — penalised by means of an overall amount of compensation, which is not determined by adding up individual amounts but is based on an evaluative overall assessment

7.2.3. Question 3: Impact of the principle of effectiveness on the array of full compensation

How do the principle of effectiveness and Article 47 CFREU influence the array of full compensation in the case of unlawful collection and processing of data?

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

➢ Judgment of the EU Civil Service Tribunal (First Chamber), 5 July 2011, *V. and European Data Protection Supervisor (EDPS)*, F 46/09

Relevant CJEU case law

➢ Judgment of the EU Civil Service Tribunal (First Chamber), 5 July 2011, *V. and European Data Protection Supervisor (EDPS)*, F 46/09

➢ Judgment of the General Court (Sixth Chamber), 3 December 2015, *CN and European Data*

Protection Supervisor (EDPS), T 343/13

Relevant legal sources:

EU Level

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data
(Act no longer in force, date of end of validity: 10/12/2018, repealed by Regulation (EU) 2018/1725)

Article 2 Definitions; Article 4.1.; Article 5 Lawfulness of processing; Article 6 ; Article 7.1.; Article 10. 1.; Article 18 The data subject's right to object

The case:

V, after passing the contract agent selection tests for the 25 Member States in the secretarial field, underwent pre-recruitment medical examination in June 2006, after which she lodged a complaint on the examiner — dr K. Subsequently, she was declared physically unfit for the position she applied — firstly by dr K, and then by the medical committee. As a result, she was not employed. She brought an action *inter alia* against this decision of Commission (Case F-33/08), which was dismissed.
On 9 December 2008 the European Parliament made the applicant an offer of employment as a member of the contract staff, which was accepted by her on the following day. The offer was made subject to compliance with the conditions of engagement laid down in Article 82 of the CEOS and to the positive outcome of the pre-recruitment medical examination (appointment set on the 7 January 2009). On 12 December 2008, the Parliament's medical service received a copy of the applicant's pre-recruitment medical file from the previous proceeding. Based on the medical examination from June 2006, the Parliament's medical officer declared the applicant physically unfit to perform 'any duties in any European [i]nstitutions' and the Parliament withdrew the offer of employment of 10 December 2008.
V brought the action against the European Parliament seeking annulment of the decision by which the Director for Administrative Management of Personnel of the European Parliament withdrew, on the ground of unfitness for recruitment, the offer of employment which had been made to her on 10 December 2008 and of the opinion of the Parliament's medical officer of 18 December 2008, as well as compensation for the damage suffered.

Reasoning of the Court:
The Court observed that the medical officer's opinion was issued with disregard to the applicant's right to respect for private life and that the decision at issue is, accordingly, also unlawful for that reason (127 - infringement of the right to respect for privacy). By asking the Commission for the transfer of those medical data, the Parliament's medical officer infringed Articles 6 and 7 of Regulation 45/2001 (143).
The administration can be held liable for damages because the allegedly wrongful act committed by the institutions was illegal, the applicant suffered actual harm, and there was a causal link between the act and the damage.
The Court found that the required causal link is attained if the unlawful act committed has deprived a person of a chance of being recruited, resulting in material damage for the person concerned in the form of loss of income. In the case at hand, the recruitment decision was already made — the applicant's engagement depended solely on establishing her physical fitness. It was not proved that, provided that the medical examination for recruitment had been conducted in a regular manner, the applicant would

not have been recruited due to the information collected by the Parliament's medical service on the applicant's state of health in January 2009. The Court underlined also that a candidate for recruitment cannot be required to disclose all his medical history to his future employer. In addition, the knowledge of disorders other than physiological disorders does not automatically justify a refusal of recruitment.
As to the non-material damage, though the annulment of an act which has been challenged may in itself constitute appropriate and sufficient reparation for the damage, it should be assessed whether the act contained a possibly offensive assessment of the abilities and conduct of the person. Being that the case, the annulment of the administration's unlawful act cannot constitute full reparation.
Also, if the illegality of actions committed by the administration was particularly serious, it justifies the award of compensation for the non-material damage. In the case the infringement of the right to respect for private life and of Regulation 45/2001 were seen as particularly serious.
Finally, it was observed that in situations where the annulment of the act lacks practical effect, it cannot in itself constitute appropriate and sufficient reparation. The Court underlined the permanent effect which an unlawful processing of subject's data — namely bringing certain information relating to the applicant's health — might have. The information, once unlawfully provided, might have a continuous impact on the person to which it was revealed. Therefore, annulment of the act at issue might not effectively protect applicant rights, as it cannot erase the doubts as to the fitness of the applicant which have already emerged, hindering objective analysis of her health in the future.

Conclusion of the Court:
For these reasons, the Court ascertained that the applicant have the right to compensation for material damage caused by the above. In order to establish the height of compensation the Court assessed that the chances of being recruited were *ex aequo et bono* 50%, the remuneration for the period in question - EUR 15 600.60, the unemployment benefits the applicant received amounted to EUR 960 a month, and therefore ordered the defendant to pay the applicant the sum of EUR 5 000 for the material damage.
Furthermore, as the annulment of the act did not entirely compensated for the non-material damage (in particular the infringement of the right to respect for private life and of Regulation No 45/2001), the Court awarded the applicant with the compensation of EUR 20 000.

Elements of judicial dialogue:
- Horizontal (within CJEU)

➢ Judgment of the General Court (Sixth Chamber), 3 December 2015, *CN and European Data Protection Supervisor (EDPS)*, T 343/13.
V. and EDPS (F 46/09) was complemented by the decision of the Court in *CN and EDPS* (T 343/13). **In this judgement, the Court addressed the impact of the principle of effectiveness on establishing the entity legitimised to claim compensation for unlawful collection and processing of data as well as the scope of costs which can be considered damages caused by the unlawful act in question.**
CN, an official of the Council of the EU, submitted an online petition to the European Parliament, on the support granted to disabled family members of a European official and the difficulties encountered by European officials suffering health problems during their careers. The document which summarised the petition and Council's answer to it was published online. It included the name of the applicant as well as data on his serious illness and the disability of his son. CN requested removal of the notice in April 2012 and on 20 April 2012 the Parliament informed that the content was removed. Nevertheless, the notice remained accessible for some time. CN claimed that from the information he was given when consenting to processing of his data was not clear. For this reason, he lodged an application requesting

award of EUR 1000 of compensation for material damage and EUR 40 000 in compensation for non-material damage suffered.
The Union incurs the non-contractual liability under the second sentence of Article 340 TFEU for unlawful conduct of its institutions if the allegedly wrongful act committed by the institutions is illegal, the applicant suffers actual harm, and there us a causal link between the act and the damage. In order for the liability to arise, all the aforementioned premises must be fulfilled.
Firstly, the Court examined the unlawfulness of the institutions' conduct. Publication of the applicant's data on the website by the Parliament constituted processing of personal data within the meaning of Article 2(b) of Regulation 45/2001. As a rule, the processing of personal data revealing data concerning health is prohibited under Article 10(1) of Regulation 45/2001, unless the data subject has given his or her express consent (see: Article 10(2)(a)). This consent must be freely given specific and informed (Article 2(h) of Regulation 45/2001). Also, the scheme and the purpose of the right of petition to the Parliament should be taken into account — being the instrument of democratic participation it should be transparent so that it can trigger a public debate as to the issue at hand. The specific content of the petition was the key element that was aimed to be brought to public discussion by the applicant — and it was to be considered in public. In light of the above, the Court ascertained that the applicant had unambiguously provided a 'freely given specific and informed indication' of his wishes in relation to the processing of his personal data by the Parliament, including their disclosure in the context of the processing of a petition by the Parliament. Thus, the Parliament's actions cannot be deemed unlawful and the applicant cannot be awarded a compensation on this basis.
Accordingly, the Court ascertained that the fulfilment of premise of consent for data processing must be interpreted in light of the circumstances of the case. In order for the liability to arise, the breach of rule of law must be sufficiently serious. In this case, the Court — after examining the interests at hand as well as the circumstances and the function of the petition — holds that the Parliament did not commit a sufficiently serious breach of law by disseminating the personal data in question on the internet.
Another issue which was raised during the proceeding regards the entity entitled to claim damages — the applicant claimed that also his son's sensitive data had been processed unlawfully, for what the applicant demanded compensation. However, neither the applicant was a representative of his son in the proceeding nor was the son the party to the action. The Court ascertained that in order to ensure the effectiveness of the condition relating to the breach of legal provision conferring rights on individuals, the protection offered by the rule invoked must be effective *vis-à-vis* the person who invokes it, and that person must therefore be among those on whom the rule in question confers rights. A rule which does not protect the individual against the unlawfulness invoked by him, but protects another individual, cannot be accepted as a source of compensation. The applicant cannot, therefore, invoke unlawfulness resulting from the alleged breach of rights of a third party, namely his son. Thus, one cannot claim compensation for the damaged caused to another.

➢ Lastly, in the pending case GP (C-741/21) the referring court asked to the CJEU whether
i) In light of recital 85 and the third sentence of recital 146 GDPR, the concept of 'non-material damage' in Article 82(1) of the GDPR covers any impairment of the protected legal position, irrespective of the other effects and materiality of that impairment?
iii) it is permissible or necessary to base the assessment of compensation for non-material damage on the criteria for determining fines set out in Article 83 of the GDPR, in particular in Article 83(2) and 83(5) of the GDPR?
iv) the compensation must be determined for each individual infringement, or are several infringements — or at least several infringements of the same nature — penalised by means of an overall amount of compensation, which is not determined by adding up individual amounts but is based on an evaluative overall assessment.

7.3. The impact of the principle of proportionality on remedies and sanctions

7.3.1. Question 4: Sanctions and the principle of proportionality

Which is the role of the principle of proportionality in the application of sanctions?

A short view on the GDPR rules:

Compared with Directive 46/95, Regulation (EU) 2016/679 (GDPR), as shown in the introduction to this chapter, has paid much greater attention to the application of general principles (and specifically effectiveness, dissuasiveness and proportionality) to sanctions and other measures (for an overview, see the introduction of this chapter).
The legislator has acknowledged that the task of a supervisory authority is not an easy one and needs guidance. Such guidance, mainly provided through the lens of general principles (effectiveness, proportionality and dissuasiveness) should also steer enforcers when combining administrative fines with other measures (namely the so called "corrective" measures, see Article 58(2)), since administrative fines are conceived as alternative or complementary to these measures "depending on the circumstances of each individual case" (see Article 83(2)).
Similar guidance could apply to the other sanctions that, aside from these administrative fines, Member States may adopt under Article 84 in order to sanction infringements of this Regulation, having particular (but not exclusive) regard to those not addressed by administrative fines pursuant to Article 83. Those penalties should also be effective, proportionate and dissuasive. It seems plausible to state that, when applying these principles, the enforcer (administrative or judicial authority) should take into account whether or not other penalties or measures are available.

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

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

The case:

The facts of the case, as well as the relevant legal sources, have been described in Chapter 2, question 2. To sum up, Mrs. Lindqvist, who was a maintenance worker, had infringed Swedish law on data protection by setting up pages on the internet, after she had followed a data processing course. The internet pages, meant to allow parishioners preparing for their confirmation to obtain information they might need, displayed personal data on a number of people working with her on a voluntary basis in a parish of the Swedish Protestant Church. As soon as Mrs Lindqvist became aware that these pages were not appreciated by some of her colleagues, she removed them.
She was nevertheless prosecuted and charged with breach of the law. The amount of the fine was SEK 4,000, which was arrived at by multiplying the sum of SEK 100, representing Mrs Lindqvist's financial position, by a factor of 40, reflecting the severity of the offence. Mrs Lindqvist was also sentenced to pay SEK 300 to a Swedish fund to assist victims of crimes.

Preliminary question referred to the Court:

Several questions were referred to the Court, but none focusing on the issue of the proportionality of the sanction. However, the Court addressed that issue in its reasoning under question 6, by which the referring court asked whether the provisions of Directive 95/46 introduce a restriction that conflicts

with the general principles of freedom of expression or other freedoms and rights, which are applicable within the EU and are enshrined *inter alia* in article 10 of the ECHR.

Reasoning of the Court:

While the main part of the reasoning concerns the balance between the freedom of expression of the controller, and the right of the data subject to the protection of private life and personal data (on which see Chapter 3, question 2), the Court addresses the issue of the **proportionality** of the sanction in what seems to be an *obiter* statement. After recalling that Member States should, at the stage of the application at national level of the legislation implementing Directive 95/46 in individual cases, find a balance between the rights and interests involved, the Court also deals with the issue of the sanction by stating: "Whilst it is true that the protection of private life requires **the application of effective sanctions** against people processing personal data in ways inconsistent with Directive 95/46, **such sanctions must always respect the principle of proportionality.** That is so a fortiori since the scope of Directive 95/46 is very wide and the obligations of those who process personal data are many and significant (§88).

It is for the referring court to take account, in accordance with the principle of proportionality, of all the circumstances of the case before it, in particular the duration of the breach of the rules implementing Directive 95/46 and the importance, for the persons concerned, of the protection of the data disclosed" (§89)

The Court thus puts both *principles of effectiveness and proportionality* into perspective, and which should be considered together when imposing a sanction. Sanctions are to be effective, but they should not be disproportionate. And national courts or authorities should take into account all circumstances of the case in order to assess what should be the adequate sanction. Although the Court only refers to the duration of the breach and to the importance of the protection of the data disclosed, it seems that other circumstances could be considered, such as the awareness of the controller that he was infringing the law, the purpose he was pursuing, or his good faith.

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

France

French *Conseil d'Etat*, 28 September 2016, no 389448: the *Conseil d'Etat* observes that when the French supervisory authority imposes, in addition to the main sanction, a measure consisting of publicising the sanction imposed on the controller, such additional sanction is necessarily subject to the principle of proportionality, even if the law does not expressly so state. The legality of the sanction should be assessed, in particular, in light of the type of publishing medium, and of the time during which the publication is available to the public. In the case considered, the additional sanction (publicity of the main sanction) is, because of the seriousness of the infringement, justified in principle since it tends to reinforce the dissuasiveness of the main sanction. However, because it does not define the time period during which the publication will be online and available to the public, the sanction is excessive. It should be annulled, insofar as it does not define for how long the publication should stay online in a non-anonymous manner.

Cour de cassation, Commercial Chamber 25 June 2013, no 12-17037: Even if the law does not state expressly so, the sale of a file including personal data that has been unlawfully collected and processed (no declaration to the French data protection authorities) is void since the object of the sale — the undeclared processing of data — is unlawful and thus cannot be seen as being available for trade.

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

Belgium

Decision no. 2020/AR/1333 of 27 January 2021 decided by the Court of Appeal of Bruxelles is of particular interest. In that decision, the Court of Appeal assessed the proportionality of a sanction established by the DPA according to Article 83 GDPR. The Court stated that by immediately imposing an administrative fine - a very substantial one — on a private individual who sent e-mails mentioning the e-mail addresses of all the persons to whom the e-mail was addressed, the Authority disregarded the fundamental principles of the proportionality of the sanction. In its reasoning the Court considered that where the decision is to be adopted on a case-by-case basis, starting from the principle of good faith, in the absence of a prior warning and of any precedent, and where the infringer immediately apologise (the day after the applicant was informed of the problem of which he was unaware), the sanction of immediately imposing an administrative fine, in addition to the fact that it is set from the outset at a significant sum of 5,000 euros, is disproportionate. The Court criticised the fact that the Authority did not consider the possibilities of achieving the goal of the European legislation by another decision, considering that several elements that demonstrate that the infringer did not show any intention to disregard the principles of personal data protection, but rather that the violation he committed was the result of negligence or inadvertence and that he immediately rectified the situation and apologised. Accordingly, the Court affirmed that the imposition of fines from the first inadvertent infringement does not correspond to the principles governing the matter, taking into account that several kind of sanctions exists (from the warning to the financial sanction). Moreover, the Court considered that the Authority failed to take into account the presumption of good faith.

7.3.2. Question 5: the principle of proportionality and the right to be de-listed

Which is the role of the principle of proportionality in applying the right to be de-listed, which stems from the right to erasure provided for by Article 17 GDPR?

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

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *G.C., A.F., B.H., E.D.* v *Commission nationale de l'informatique et des libertés* (CNIL), Case C-136/17 (***GC and Others)***

Cluster of cases:

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

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

➢ Judgment of the Court (Grand Chamber), 24 September 2019, *G.C., A.F., B.H., E.D.* v *Commission nationale de l'informatique et des libertés* (CNIL), Case C-136/17 (***GC and Others)***

➢ Judgement of the Court (Grand Chamber), 24 September 2019, Google LLC v. Commission nationale de l'informatique et des libertés (CNIL), C-507/17 (***Google v. CNIL***)

➢ Judgment of the Court (Third Chamber) of 3 October 2019, *Eva Glawischnig-Piesczek v Facebook*

Ireland Limited, C-18/18

➢ Request for a preliminary ruling from the Bundesgerichtshof (Germany) lodged on 24 September 2020 — *TU, RE v Google LLC*, Case C-460/20 (**TU, RE v Google LLC**) [pending]

➢ Request for a preliminary ruling from the Hof van beroep te Brussel (Belgium) lodged on 2 March 2021 — *Proximus NV v Gegevensbeschermingsautoriteit*, Case C-129/21, (**Proximus**) [pending]

The case

The facts of the case are explained in the question 1 of this Chapter.

Preliminary questions referred to the Court

For our analysis the second question referred to the CJEU is of particular importance. In this question, the national court essentially asked whether:

i) the operator of a search engine is required to accede to requests for de-referencing in relation to links to web pages containing sensitive data;

ii) such an operator may refuse to accede to a request for de-referencing if he establishes that the links at issue lead to content comprising sensitive data but whose processing is covered by one of the exceptions to the prohibition of processing of such data;

iii) whether that the operator of a search engine may also refuse to accede to a request for de-referencing on the ground that the links whose de-referencing is requested lead to web pages on which sensitive data are published solely for journalistic purposes or those of artistic or literary expression and the publication is therefore covered by the related exception.

Reasoning of the Court

The Court observed that according to Article 17(3) of Regulation 2016/679 the right to erasure (being the right to be delisted a part of it) is not to apply to the extent that the processing is necessary on one of the grounds set out in Article 17(3), among which there is the exercise of the right of freedom of expression and information.

The Court, in deciding on the application of the right to be de-listed in case of processing of sensitive data, considered then that the explicit mention, in Article 17 GDPR, of freedom of expression, guaranteed by Article 11 CFR, demonstrates that "the right to protection of personal data is not an absolute right but (…) must be considered in relation to its function in society and be balanced against other fundamental rights, **in accordance with the principle of proportionality**". The CJEU referred to **Article 52(1) CFR,** according to which limitations to fundamental rights may be imposed as long as the limitations are provided for by law, respect the essence of those rights and freedoms and, **subject to the principle of proportionality, are necessary and genuinely meet objectives of general interest recognised by the EU or the need to protect the rights and freedoms of others**. Then, the Court stated that Article 17(3)(a), expressly lays down the requirement to strike a balance between the fundamental rights to privacy and protection of personal data guaranteed by Articles 7 and 8 of the Charter, on the one hand, and the fundamental right of freedom of information guaranteed by Article 11 of the Charter, on the other hand.

Conclusion of the Court

The Court stated that the operator of a search engine is in principle required to answer to requests for de-referencing in relation to links to web pages containing personal data falling within the special categories referred to by those provisions. Nevertheless, where an exception to the prohibition of the

processing of this kind of data apply, such an operator may refuse to answer to a request for de-referencing, provided that the processing satisfies all the other conditions of lawfulness laid down by the directive, and unless the data subject has the right to object to that processing on compelling legitimate grounds relating to his particular situation.

Furthermore, where the operator of a search engine has received a request for de-referencing relating to a link to a web page on which sensitive data are published, the operator must, on the basis of all the relevant factors of the particular case and taking into account the seriousness of the interference with the data subject's fundamental rights to privacy and protection of personal data laid down in Articles 7 and 8 CFR, ascertain, having regard to the reasons of substantial public interest and in compliance with the conditions laid down in EU data protection laws, whether **the inclusion of that link in the list of results** displayed following a search on the basis of the data subject's name **is strictly necessary for protecting the freedom of information of internet** users potentially interested in accessing that web page by means of such a search, protected by Article 11 CFR.

Impact on the follow-up case

French Council of State, 6 December 2019, No. 401258.
In the paragraph concerning question 4 the decision of the Council of State has already been summarised. With regard to the specific question of the role of the proportionality principle, the Council of State affirmed that in order to assess whether the right to de-referencing can be legally defeated on the grounds that access to personal data relating to criminal proceedings on the basis of a search for the name of the person concerned is strictly necessary to inform the public, the CNIL must take into account, in particular, the nature of the data in question, their content, their more or less objective nature, their accuracy, their source, the conditions and date on which they are put online and the repercussions that their listing is likely to have for the person concerned and, on the other hand, the notoriety of that person, their role in public life and their function in society. Moreover, according to the Council of State, it must also take into account the possibility of accessing the same information from a search on keywords that do not mention the name of the data subject. In the particular case where the link leads to a web page which refers to a stage of a judicial procedure which no longer corresponds to the current judicial situation of the data subject but it appears, after the balance carried out under the conditions set out previously, that the maintenance of its referencing is strictly necessary to inform the public, the operator of a search engine is required, at the latest at the time of the request for de-referencing, to arrange the list of results in such a way that the disputed links are preceded on this list of results by at least one link leading to one or more web pages containing up-to-date information, so that the resulting image accurately reflects the current legal situation of the person concerned. Even though, under the Code of Criminal Procedure, access to data relating to a person's criminal convictions is in principle possible only under restrictive conditions and for limited categories of persons (relating to the lack of notoriety of the person concerned, the length of time the facts have been known, the criminal conviction and the repercussions on the applicant's rehabilitation), by finding that the applicant who alleges that he has lost two jobs as a result of the link in question, the CNIL could not legally consider that maintaining the links based on a search carried out on its name (given the nature and content of the disputed information, which gives the public direct and permanent access to the applicant's conviction, even if this information comes from press articles whose accuracy is not disputed) was strictly necessary to inform the public for the sole reason that the judicial columns allow the public to exercise a right of oversight over the functioning of criminal justice.

Elements of judicial dialogue

CG and Others (C-136/17) should be read in light of the CJEU case law, and in particular of *Google Spain* (C-131/12), *Google v. CNIL* (C-507/17), *Manni* (C-398/15) .
In *Google Spain* (C-131/12) Google referred to the **principle of proportionality**, arguing that, by virtue of that principle, any request seeking the removal of information must be addressed to the publisher of the website concerned because it is he who takes the responsibility for making the information public, who is in a position to appraise the lawfulness of that publication and who has available to him the most effective and least restrictive means of making the information inaccessible. **The Court rejected this argument.**
In *Google v. CNIL* (C-507/17) the Court, defining the territorial scope of the right to be de-listed, affirmed that the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of **proportionality** (on this judgement and the right to be de-listed see also Question 1a of Chapter 1).
GC and Others (C-136/17) is interestingly complemented also by the decision of the Court in ***Manni*** (C-398/15). Mr Manni requested that the personal data related to him be erased from the public companies register, after the elapse of a certain period of time. In these registers it was mentioned that he had been the director of a company which had been declared insolvent 15 years before. He claimed that that information caused him prejudice in the course of his current business. After recalling that the transcription of certain information into a public companies register, imposed by Directive 68/151, qualifies as "processing of personal data", the Court observed that such a processing, by the authority responsible for keeping the register, satisfies several grounds for legitimacy set out in Article 7 of Directive 95/46, namely: those set out in subparagraph (c) thereof, relating to compliance with a legal obligation; subparagraph (e), relating to the exercise of official authority or the performance of a task carried out in the public interest; and subparagraph (f) relating to the realisation of a legitimate interest pursued by the controller or by the third parties to whom the data are disclosed. However, the issue at stake was whether the authority responsible for keeping the register should, after a certain period had elapsed since a company ceased to trade, and on the request of the data subject, either erase or anonymise that personal data, or limit its disclosure.

In relation to this issue, the Court noted that according to EU data protection laws personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data was collected or for which it is further processed; when the availability of data is no longer necessary, data subjects have a right to obtain from the controller the erasure or blocking of the data. Such right is to be considered in light of the purpose of the processing or, here, the registration.

The Court observed that the purpose of the disclosure provided for by Directive 68/151 is, in particular, to protect the interests of third parties in relation to joint stock companies and limited liability companies, since the only safeguards they offer to third parties are their assets, and to guarantee legal certainty in relation to dealings between companies and third parties in view of the intensification of trade between Member States following the creation of the internal market. The Court observed moreover that for several reasons, it is absolutely necessary to access data concerning a company, long after its dissolution. For the Court, given 'the considerable heterogeneity in the limitation periods provided for by the various national laws in the various areas of law, highlighted by the Commission, it seems impossible, at present, to identify a single time limit, as from the dissolution of a company, at the end of which the inclusion of such data in the register and their disclosure would no longer be necessary'.

For this reason, Member States cannot guarantee that the natural persons referred to in Directive 68/151 have the right to obtain, as a matter of principle, after a certain period of time from the dissolution of the company concerned, the erasure of personal data concerning them, which has been entered in the register pursuant to the latter provision, or the blocking of that data from the public. Such a situation does not result in disproportionate interference with the fundamental rights of the persons concerned, and particularly their right to respect for private life and their right to protection of personal data as guaranteed by Articles 7 and 8 of the Charter, because the disclosure concerns only a limited amount of data, because other legitimate interests are at stake, and because persons engaging in such activity are aware of these requirements. Finally, national courts are to engage in a case-by-case analysis to decide if, exceptionally, it is justified, on compelling legitimate grounds relating to their particular situation, to limit, on the expiry of a sufficiently long period after the dissolution of the company concerned, access to personal data relating to the natural person referred to in Directive 68/151, entered in that register, to third parties who can demonstrate a specific interest in consulting that data.
With regard to the balancing between fundamental rights and interests at stake, in the pending case *TU, RE v Google LLC* (C-460/20) the referring court asked the CJEU whether in the case of a request for de-referencing made against the data controller of an internet search engine, which in a name search searches for photos of natural persons which third parties have introduced into the internet in connection with the person's name, and which displays the photos which it has found in its search results as preview images, within the context of the weighing-up of the conflicting rights and interests arising from Articles 7, 8, 11 and 16 of the Charter pursuant to Article 17(3)(a) of the GDPR, the context of the original third-party publication should be conclusively taken into account, even if the third-party website is linked by the search engine when the preview image is displayed but is not specifically named, and the resulting context is not shown with it by the internet search engine.

Lastly, in the pending case *Proximus* (C-129/21) the referring Court asked to the CJEU whether Article 17[(2)] GDPR must be interpreted as precluding a national supervisory authority from ordering a provider of public directories and directory enquiry services which has been requested to cease disclosing data relating to an individual to take reasonable steps to inform search engines of that request for erasure. The principle of proportionality may play a significant role in interpreting Article 17(2) according to which, where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. In particular, the question arises as to whether the concept of "reasonable steps" could or should be interpreted in light of the principle of proportionality, and/o in light of the data subjects' right to an effective remedy (on the latter see Section XX in this chapter).

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

See Question 1 of this Chapter.

7.3.3. Question 6: Proportionality, effectiveness, data/privacy protection and the information obligations

What is the relationship between data protection/privacy and information to be provided to the data subject, considered the importance of the latter for the exercise of data subjects' rights? Do Article 47 CFREU and the principles of effectiveness and proportionality play a role in this regard?

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

➢ Judgment of the Court (Third Chamber), 7 May 2009, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, C-553/07 (***Rijkeboer***)

Relevant CJEU caselaw

➢ Judgment of the Court (Third Chamber), 7 May 2009, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer*, C-553/07 (***Rijkeboer***)

➢ Judgment of the Court (Third Chamber), 17 July 2014, *YS (C-141/12) v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel (C-372/12)*, Joined Cases C-141/12 and C-372/12 (***YS and Others***)

➢ Judgment of the Court (Third Chamber), of 1 October 2015, *Smaranda Bara and Others v Casa Națională de Asigurări de Sănătate and Others*, C-201/14 (***Bara and Others***)

➢ Judgment of the Court (Second Chamber), 26 July 2019, *Fashion ID Gmbh & Co.KG* v. *Verbraucherzentrale NRW EV*, Case C-40/17 (***Fashion ID***)

➢ Judgment of the General Court (Sixth Chamber), 3 December 2015, *CN and European Data Protection Supervisor (EDPS)*, T 343/13 (***CN v Parliament***)

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

➢ Request for a preliminary ruling from the *Itä-Suomen hallinto-oikeus* (Finland) lodged on 22 September 2021 — J.M., Case C-579/21, (**Itä-Suomen**) [pending]

➢ Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 9 March 2021 — *RW v Österreichische Post AG*, Case C-154/21, (**RW**)

See also: WP 29 Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227

Relevant legal sources:

EU Level

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

Section I Principles relating to data quality (Article 6); Article 10 Information in cases of collection of data from the data subject; Article 11 Information where the data have not been obtained from the data subject

SECTION V - THE DATA SUBJECT'S RIGHT OF ACCESS TO DATA Article 12 Right of access; Article 13 Exemptions and restrictions; Article 14 The data subject's right to object; Article 22 Remedies; Article 23 Liability

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data

(In force since: 25/05/2018)

Section 2 Information and access to personal data; Article 13 Information to be provided where personal data are collected from the data subject; Article 14 Information to be provided where personal data have not been obtained from the data subject; Article 15 Right of access by the data subject; Article 78 Right to an effective judicial remedy against a supervisory authority; Article 79 Right to an effective judicial remedy against a controller or processor; Article 80 Representation of data subjects; Article 82 Right to compensation and liability

National Level
Article 110 of Wet gemeentelijke basisadministratie persoonsgegevens, Stb. 1994, No 494; 'the Wet GBA'

The case:
Mr Rijkeboer requested the College (municipal authority) to inform him of all instances in which his personal data from that local authority personal records had, in the two years preceding the request, been disclosed to third parties. He wanted to know the identity of these entities and the content of the disclosed data. The College complied partly with this request, providing him with the data relating to the period of one year preceding the request, as the previous information was automatically erased, in accordance with national provisions (Article 110 the Wet GBA). Mr Rijkeboer lodged a complaint with the College against the refusal and the national court (the Raad van State) referred the following question to the Court for a preliminary ruling.

Preliminary question referred to the Court:
Can, pursuant to the Directive and, in particular, to Article 12(a) thereof, an individual's right of access to information on the recipients or categories of recipient of personal data regarding them and on the content of the data communicated be limited to a period of one year preceding his request for access? (31)

Reasoning of the Court:
The CJEU considered that the case involved two categories of data, personal data kept by the local authority on a person, such as his name and address, which constitute, in the present case, the basic data, and information concerning recipients or categories of recipient to whom those basic data are disclosed and thus concerning the processing of the basic data.
In accordance with the national legislation at issue in the main proceedings, the latter information was stored for only one year. The time-limit on the right of access to information on the recipient or recipients of personal data and on the content of the data disclosed concerned that second category of data, in so far as those data were stored for only one year.
The CJEU, in order to determine whether or not Article 12(a) of the Directive authorised such a time-limit, interpreted that article having regard to its purposes of protecting the fundamental rights and freedoms of natural persons, and of permitting the free flow of personal data between Member States. The CJEU relied on its previous case law and pointed out the importance of protecting privacy with respect to the processing of personal data (*Österreichischer Rundfunk and Others*, Joined cases C-465/00, C-138/01 and C-139/01, §70; *Lindqvist*, C-101/01 paragraphs 97 and 99; *Promusicae*, C-275/06, §63; *Satamedia*, C-73/07, §52).
The CJEU stated that the data subject should be sure that his personal data are processed in a correct and lawful manner, that is to say, in particular, that the basic data regarding him are accurate and that they are disclosed to authorised recipients. **The CJEU highlighted that the right of access is necessary to enable the data subject to exercise its other rights** . The CJEU affirmed that the right to access to information on the recipients or categories of recipient of personal data and on the content of the data

disclosed may concern the past, in order to ensure that the data subject can **effectively exercise** her rights. With regard to the question of the scope of that right in the past, the CJEU stated that the setting of a time-limit with regard to the right to access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed must allow the data subject to exercise the different rights laid down in the Directive. In this respect, the CJEU affirmed that the length of time the basic data are to be stored may constitute a useful parameter without, however, being decisive.
The CJEU gave some elements for striking the balance between data subjects rights and the obligations of the controller. On the one hand the court considered that where the length of time for which basic data are to be stored is very long, the data subject's interest in exercising the rights to object and to other remedies may diminish in certain cases. On the other hand, the CJEU stated that if, for example, the relevant recipients are numerous or there is a high frequency of disclosure to a more restricted number of recipients, the obligation to keep the information on the recipients or categories of recipient of personal data and on the content of the data disclosed for such a long period could represent an excessive burden on the controller. In this respect, the CJEU recalled Article 12(c) of the Directive, which expressly provides for an exception to the obligation on the controller to notify third parties to whom the data have been disclosed of any correction, erasure or blocking, namely, where this proves impossible or involves a disproportionate effort. The CJEU stated that in accordance with other sections of the Directive, the **disproportionate** nature of other possible measures should be considered, taking into account the number of data subjects and the age of the data. Furthermore, in accordance with Article 17 of the Directive concerning security of processing, Member States are to provide that the controller must implement appropriate technical and organisational measures which, regarding the state of the art and the cost of their implementation, are to ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

Conclusion of the Court:

Article 12(a) of Directive 95/46/EC requires Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed in respect of the present and of the past. Therefore, Member States should determine a time-limit for storage of these information which would provide for a fair balance between the interest of the data subject in protecting his privacy and the burden which the obligation to store that information represents for the controller. The Court stated that:
"Rules limiting the storage of information on the recipients or categories of recipient of personal data and on the content of the data disclosed to a period of one year and correspondingly limiting access to that information, while basic data is stored for a much longer period, do not constitute a fair balance of the interest and obligation at issue, unless it can be shown that longer storage of that information would constitute an excessive burden on the controller. It is, however, for national courts to make the determinations necessary."

Impact on the follow-up case

➢ ECLI:NL: RVS:2009: BK4335 – continuance of national proceedings after preliminary ruling in Rijkeboer.

The follow-up case to the Rijkeboer decision was heard by the Dutch Council of State. After citing an extract from Rijkeboer, the Council of State stated that in its appeal the College had not plausibly demonstrated that a retention period of longer than one year entails an excessive burden. The Council of state considered that the Rotterdam court (of first instance) had therefore correctly considered the limitation of the right to information on the provision of data in the year prior to the request, as provided for in Article 103 (1) of the Municipal Personal Records Database Act, to be contrary to Article 12 of the

directive. The appeal on that ground therefore failed. The Dutch judgment does not refer to Articles 7, 8 or 47, or the principles of effectiveness and proportionality.

Elements of judicial dialogue:

- Horizontal (within CJEU)

The right to access data is subject of analysis by the CJEU in *YS and Others* (joined cases C-141/12 and C-372/12, issued on 17 July 2014) and in *Smaranda* (C-201/14).

In *YS and Others* (C-141/12 and C-372/12) the dispute originated in the Netherlands and concerned denial of access to the draft decision ('the minute') issued by an officer of the Immigration and Naturalisation Service responsible for dealing with an application for a residence permit which included personal data of the applicant and an assessment of these information in light of the applicable legal provisions. The national courts referred the several questions to CJEU, between other as to the scope of the right to access to the processed data. With regard to the question whether the data subject was entitled to have access to the entire document, the Court, recalling that the right of access is provided for in Article 8(2) CDFUE, stated that the form in which the data are processed must enable the data subject to verify that they are accurate and processed in a manner consistent with the legislation in order to enable him to exercise his rights.

In *Smaranda* (C-201/14) there was a communication of data from one public administration to another, and the person concerned brought a claim before a court, questioning the lawfulness of that communication in several respects, including that the national legislation did not provide to the data subject the information on the communication of personal data. The national court asked whether national provisions may restrict information both on the communication of the data and on their subsequent processing. In answering that question, t**he CJEU stated that that information necessarily affects the exercise of the data subject's rights. Moreover, the Court notes that the principle of fair processing requires the data subject to be informed.**

In the cases considered in this section Articles 8, 47 and 52 of the CDFEU seems to be relevant. In particular, the right to an effective remedy (Article 47 CFR) comes into play with respect to the necessity of information to be provided to the data subject in order to allow her to exercise her rights. Moreover, the relevance of the principle of proportionality, recalled by the CJEE in *Rijkeboer* (C-553/07) is twofold: on the one hand, it is provided as a balancing criterion within the wording "**disproportionate effort"** of the data controller (now Article 14 GDPR), and, on the other hand, in relation to Article 52 CFR, which requires the application of that principle in limiting the exercise of the rights and freedoms provided for in the Charter, such as the data subject's right to access to personal data, set forth in Article 8(2) CFR.

The scope of the information which should be provided in order to ensure that the data subjects' rights is capable of exercising his rights was tackled in the case *Fashion ID* (C-40/17). The company "Fashion ID" embedded in its website a plugin from third party platform (Facebook). Once the Fashion ID website was accessed the user's website requested content from Facebook, transmitting at the same time data on the user. Nevertheless, the Fashion ID did not control the scope of transmitted data nor its further processing. However, the Court ascertained that the duty to inform under Article 10 of Directive 95/46 is incumbent also on the operator of the website in which a plugin from a third party platform is embedded, with regard to the processing operations where he is to be qualified as a controller (see Chapter 2). Thus, it could be argued that Fashion ID is obliged only to provide information the collection and transmission of personal data — the processing activities for which it is a (joint) controller. Those duties do not emerge in case of operations involving the processing of personal data at other — previous or subsequent — stages. (paras 100-101).

Furthermore, in *La Quadrature du Net* (C-511/18, C-512/18, C-520/18), the CJEU, in a case concerning the application of Directive 2002/58, stated that where exceptionally a national public authority collect in real time traffic and location data, that authority must notify the persons concerned, in accordance with the applicable national procedures, to the extent that and as soon as that notification is no longer liable to jeopardise the tasks for which those authorities are responsible. According to the CJEU, that notification is, indeed, necessary to enable the persons affected to exercise their rights under Articles 7 and 8 CFR, to request access to their personal data that has been processed, and where appropriate, to have the latter rectified or erased, as well as to exercise the right to an effective remedy, in accordance with Article 47 CFR, of an effective remedy before a tribunal.

Furthermore, in relation to data subject's information the right to access, provided for by Article 15 GDPR may play a role. In this respect, in *RW* (C-154/21), the referring court asked the CJEU as to whether Article 15(1)(c) GDPR is to be interpreted as meaning that the right of access is limited to information concerning categories of recipients where specific recipients have not yet been determined in the case of planned disclosures, but that right must necessarily also cover recipients of those disclosures in cases where data has already been disclosed. In answering this question, the CJEU might take into account, in light of the right to an effective remedy, that the information concerning the specific recipients may be necessary in order to allow the data subject to exercise her rights *vis-à-vis* the recipients of personal data concerning her.

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

Italy
The Italian case law addressed the question of the relationship between information provided to the data subject and the effective possibility for the data subject to exercise her rights. For example, in a dispute concerning the violation of the data subject's right of access, the Court of Rome, in its judgment of 12 April 2012, stated that, "the omission or incompleteness of information [may] result in an obstacle to the exercise of the right against whom that right has been violated". The Court affirmed that a function of the right of access is to allow the data subject to exercise their claims in relation to unlawful data processing and to know, according to a principle of transparency, the manner in which the processing of personal data concerning them has taken place.
Furthermore, the Supreme Court of Cassation in the judgement of 16 April 2015, n. 7755, stated that Article 2, recognising fundamental rights and Article 24, providing the right to bring an action before the court of the Italian Constitution require that when personal data is processed unlawfully or incorrectly there should be the possibility of seeking for an injunction.

Spain
Spanish Courts considered the right to know at all times who is processing personal data and what use is being made of it as part of the fundamental right to data protection, as provided also by Article 18(4) of the Spanish Constitution (*Tribunal Constitutional,* n. 292, 30 novembre 2000).

Poland
Within the judgements on the provision of information about data processing, Polish court has explicitly referred to the interplay between data/privacy protection and information to be provided to the data subject considering the importance of the latter for the exercise of data subjects' rights (Judgement of the of District Administrative Court in Warsaw of 11 December 2019, case No. II SA/Wa 1030/19).

A company, whose main activity was provision of information services, ran a database with information of natural persons who were self-employed (either conduction economic activities in past or currently). The data processed in this system were obtained from publicly available sources, including public registers. Prior to the GDPR coming into force, the company informed data subjects about data processing using the e-mail addresses stored within the above system (682 439 persons out of 7 594 636) and published an information in this regard on its website. With respect to 181,142 people, the company only had mobile phone numbers, and with regard to 6,499,226 people — mailing addresses, of which 2,924,443 records related to inactive business activities. The company explained that the implementation of the information obligation in its basic form (i.e., individual contact with each data subject) would cause a "disproportionate effort" on the part of the company, as referred to in Article 14 paragraph 5.b of Regulation 2016/679. It would constitute an organisational burden which would critically disrupt the functioning of the company, and possibly even result in its closure. In light of the above, the company decided not to inform remaining data subjects individually.

Polish Data Protection Authority saw this decision as infringing the information obligations under Article 14 paragraph 1 and paragraph 2 of Regulation 2016/679. In this context, the court followed the view presented by the Data Protection Authority and stated that sending the information referred to in Article 14 Regulation (EU) 2016/679 by traditional mail, to the address of the self-employed person (regardless of whether this activity has been suspended) as well as contacting this person via telephone is neither impossible not requires a disproportionate effort in the case of the company processing the addresses and the telephone numbers of these data subjects. However, the sanction applied by the Data Protection Authority (fulfilment of the information obligation was supposed to be accompanied with payment of an administrative fine of 943.470,00 PLN) could not be considered proportionate. Not only the seriousness of the infringement at hand (namely, the persons who were individually informed could have been deprived of the possibility to exercise their rights under data protection law) should be taken into account when deciding on the administrative fine, but also the effectiveness, dissuasiveness and proportionality of the sanction must be granted. However, the sanction must correspond with the characteristics of the infringer so that it is effective, dissuasive and proportionate in this particular case. Thus, the sanction (especially the height of fine) cannot be determined so that it is dissuasive not only for the infringer but also for all the potential and future administrators.

The Netherlands

The decision issued by the Council of State, on 2 October 2019, 201802949/1/A3 is of particular interest. In this case, the appellant requested a copy of his personal data which had been processed by the Mayor and Municipal executive (College). The College had used his data to send three letters, and shared this information with the appellant as requested. The Association of Dutch Municipalities (VNG) posted a copy of the access request made by the appellant on their forum, as an example to show municipalities how to deal with such requests. This forum post was wrongly not anonymised. The appellant requested the College to provide a list of people who had received his information, which was denied. The College argued that it lacked the authority to share details of the people who had received the appellants information. Instead, the appellant should request VGN to provide this information. The Court of first instance ruled that the College could not be held responsible. The appellant appealed this decision, claiming that the College should be held to be responsible.
The Court is tasked with deciding whether the College, in their capacity as data controller, is responsible for the appellant's data becoming available on the VGN forum. In that regard, the Court referred to a previous decision made by the Supreme Court which dictates that the College is responsible for personal data made available on the VGN forum. Secondly, the Court determines whether the College should

have provided the appellant with a list of the recipients of his personal data. The Court followed the CJEU's reasoning in *Holstein* that joint responsibility does not mean that both parties have the same responsibility, as the parties may be involved in different stages of the data processing. Thus, the level of responsibility must be assessed in light of all the relevant circumstances of the case. The Court then goes on to cite the CJEU's reasoning in *Fashion ID* that parties only have the same responsibility under Article 2(d) of Directive 95/46 if they jointly determine the purpose of the processing of the data. A party is not responsible for operations which took place later or earlier in the processing chain. In light of these judgments, the Court considers that the College had the authority to post messages on the forum, as well as delete them. VGN managed access and provided the general accounts and passwords. The College did not have the requisite control over the forum and did not have insight into the recipients of the applicant's data. The Court concludes that for these reasons the College does not have the responsibility to provide a list of recipients to the applicant; he should instead submit a request VGN for this list.

Decisions and opinions of the supervisory authorities, also in light of the GDPR

Working Party Article 29 and EDPB

With regard to the interpretation of information duties the supervisory authorities seem to adopt a broad interpretation, which takes into account its importance in order to grant the effectiveness of data subject's rights. Within the WP29's *Guidelines on Transparency under Regulation 2016/679*, endorsed by the EDPB on 25 May 2018, the principle of transparency has been interpreted as a concretisation of the principle of fairness, enshrined in Article 8(2) CFREU. Moreover, the Working Party Article 29, also on the basis of recital 39 EU Regulation 2016/679 states that on the basis of the information provided, the data subject should be able to understand in advance what the scope of the processing is and what its consequences are, and they should not be surprised by the way personal data concerning them are used.

In relation to the "right to an explanation" in case of automated decision making (Article 22, 13 and 14 GDPR) the *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, adopted by the Working Group Article 29 and endorsed by the EDPB*, provides, with regard to the information on the logic involved, that the data controller must find easy ways to communicate to the data subject the logic or criteria on which the decision is based, without necessarily proving a complex explanation of the algorithms used or the disclosure of the complete algorithm. The information should, however, enable the data subject to understand the reasons for the decision. According to the interpretation of recital 63 EU Regulation 2016/679 given by the Article 29 Working Party, there is no need to explain a particular decision, but rather its consequences. Furthermore, the data controller should provide to the data subject general information useful to contest the decision based on the processing.

With regard to the application of the criterion of the "**disproportionate effort"** set forth in Article 14 EU Regulation 2016/679, according to the WP29's *Guidelines on Transparency under Regulation 2016/679*, endorsed by the EDPB on 25 May 2018, the "disproportionate effort must be directly connected to the fact that the personal data was obtained other than from the data subject", because of the absence of such a criterion in the case of data collected from the data subject (Article 13 GDPR). With regard to the parameters according to which proportionality is to be assessed, the guidelines provide for a comparison, on the one hand, of the effort which the data controller would involve informing the data subject and, on the other hand, of the impact and effects of the failure to inform the data subject.

Italy

With regard to the importance of the information provided to the data subject, the Italian Data Protection Supervisor in several decisions where EU Regulation 2016/679 is applied (GPDP, 19 July 2018, n. 9039945; Decision, 22 February 2018 *Indicazioni preliminari di cui in motivazione volte a favorire la corretta applicazione delle disposizioni del Regolamento UE 2016/679,* n. 8080493) stated the need to inform the person

concerned about the methods of data processing, also in application of the principle of fairness and transparency as per Article 5, paragraph 1, letter a) EU Regulation 2016/679.
With regard to the application of the concept of "**disproportionate effort**", the Italian data protection supervisor (GPDP) referred to its precedents. The GPDP, before the entry into force of the GDPR, had identified some elements to be considered in assessing the existence of a "disproportionate effort" of the data controller. Firstly, the data subject's awareness of the processing is to be considered (GPDP, 26 November 1998, n. 39624). Other elements to be take into account are the nature of the processing (GPDP, 4 April 2001, n. 40763), its purpose (GPDP, 7 February 2001, n. 40967, GPDP, 12 February 2004, n. 634369; GPDP, 24 April 2013, n. 2404305), the nature of data (GPDP, 12 January 2017, n. 6033934), the manner in which the processing is carried out, the number of data subjects (GPDP, 5 July 2017, n. 6845231; GPDP, 31 May 2017, n. 6531135; GPDP, 16 November 2017, n. 7490004; GPDP, 19 January 2017, n. 6093240), the activities necessary to trace them, the date of collection, and the particular high costs for the data controller (GPDP, 26 November 1998, n. 39624; GPDP, 5 July 2017, n. 6845231; GPDP, 12 January 2017, n. 6033934; GPDP, 18 December 2014, n. 3716039).
In practice, the measures taken by the Italian Data Protection Authority focus in most cases on the assessment of the burden of the data controller, and not on the impact on the position of the data subject. In some cases, Italian Data Protection Authority has applied publication as an appropriate measure to protect the data subject.

France
The French data protection authority (*Commission Nationale de l'Informatique et des Libertés,* CNIL) identified some elements to be considered in assessing the existence of a "disproportionate effort", both before and after the entry into force of EU Regulation 2016/679. The CNIL considered the number of data subjects involved (CNIL, délib. 2018-300, 19 July 2018; CNIL, delib. n. 2017-106, 13 April 2017), the technical difficulty (CNIL, délib. n. 2018-151, 3 May 2018), the cost of the measures (CNIL, delib. n. 2018-151, 3 May 2018; CNIL delib. 2016-047, 25 February 2016) and the purposes of processing (CNIL, delib. n. 2011-423, 15 December 2011; CNIL, delib. 2014-301, 10 July 2014). The French authority also considers publication on the data controller's website, even in addition to publication by other means, to be an appropriate measure to protect data subjects (CNIL, delib. n. 2018-360, 13 December 2018; CNIL, delib. 2018-300, 19 July 2018; CNIL, delib. n. 2017-305, 7 December 2017; CNIL, delib. 2015-073, 26 February 2015).

7.4. BOX: Impact of fundamental rights on automated decision-making and profiling

Automated decision-making and profiling may pose a serious risk to fundamental rights (primarily: privacy and data protection, right to an effective remedy and right to a fair trial and due process[64] and prohibition of discrimination), especially due to the lack of transparency and the likelihood of discrimination. As a result, the GDPR sets forth a protective framework which is aimed at minimising a negative impact automated decision-making and profiling might have on the fundamental rights of data subjects.
The GDPR protection mechanisms cover: transparency and fairness requirements, specific accountability obligations, specified legal bases for the processing, rights for individuals to oppose profiling (specifically

[64] See box: : AI, the black box and data subjects' rights: the role of Article 47 CFR

profiling for marketing), and, if certain conditions are met, the need to carry out a data protection impact assessment.

In order to assure lawfulness, fairness and transparency the controller is obliged to provide data subjects with concise, transparent, intelligible and easily accessible information about the processing of their personal data (Article 12(1) GDPR). However, especially in the online environment, the practical efficiency of the safeguards based on the protection by information model is limited due to the information overload effect. Information is likely to be disregarded, unless it is highly specific and corresponds with the interests of the particular data subject. Yet, in light of the Article 13 and 14 GDPR, the catalogue of data that must be provided is lengthy. Thus, the obligation is probable to create a fiction of the data subject knowing and understanding the whole context of data processing instead of *e.g.,* enabling the data subject to make an informed choice in regard to consenting to profiling (Article 6(1) GDPR). In addition, the process of both automated decision-making and profiling are difficult to comprehend by a non-professional and are likely to constitute company's trade secret. Nevertheless, as the Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 suggests, *the controller should find simple ways to tell the data subject about the rationale behind, or the criteria relied on in reaching the decision.* In this context, the right of access (Article 15 GDPR) might also play a significant role, as it allows data subject to effectively learn about the scope and quantity of personal data which is being processed by the controller.

In addition, use of big data-empowered tools increases the risks of objectionable or illegal discrimination (both direct and indirect).[65] The first obstacle, when aiming at limiting these risks, is the fact that the process of profiling and automated decision-making is opaque which hinders detection of discriminatory patters. Also, their emergence can be caused by different factors: definition of the "target variable" as well as the "class labels", the content and scope of training data, collecting these data, selection of the indicators on which the decision of the AI is based, and proxies. Finally, AI systems can intentionally be used for a discriminatory purpose.[66] Another issue is that the discrimination cannot be easily eradicated with i.a. eliminating certain factors (e.g., ethnicity), as there are usually other indicators, supposedly non-discriminatory (such as home address) which incorporation is likely to lead to the same effect.

As a result, when assessing the impact of fundamental rights on regulation of automated decision-making and profiling, it seems that a key role is played by the automatic and objective safeguards, namely, processing and purpose limitation (Article 5(1) GDPR), data minimisation (Article 5(1) (c) GDPR), storage limitation (Article 5(1)(e) GDPR). They supplement the individual protective toolset (right to rectification, to erasure, to restriction of processing, and right to object) which requires the data subject to actively exercise his rights. Finally, Article 22 of GPDR prohibits decision-making based solely on automated processing in cases where the decision has a legal effect on or similarly significantly affects someone, unless specific requirements are met. It is argued that this provision should be interpreted as encompassing the right to explanation, so that the data subject can learn about the reasoning behind certain decision, and, effectively challenge it in the due procedure (an aspect of the right to an effective remedy and to a fair trial, once the automated decision-making and profiling is used in judicial proceeding).

[See also: Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01)].

[65] For in-depth analysis see: Jon Kleinberg, Jens Ludwig, Sendhil Mullainathany and Cass R. Sunstein, Discrimination in the age of algorithms, Journal of Legal Analysis 2018, Vol. 10, 113.

[66] Frederik Zuiderveen Borgesius, Discrimination, artificial intelligence, and algorithmic decision-making, https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73.

7.5. BOX: AI, the black box and data subjects' rights: the role of Article 47 CFR

The opaqueness of the automated decision-making (so-called AI black box) may endanger the individual's right to an effective remedy and to a fair trial stipulated in Article 47 CFR. The lack of transparency in this regard is observed on different levels and may equally regard the basis for a decision, factual background taken into account during the decision-making process, the data subject's consent, and the effect of the decision.[67]

Thus, it becomes crucial to interpret Article 22(3) GDPR as granting the data subject a right to explanation. Under Article 22(3) GDPR the data controller is obliged implement *suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision*. However, without understanding the reasons behind a decision, it might be impossible to effectively challenge the outcome of the automated decision-making process. Thus, in order to be able data subject to, first, present one's view, and then, to contest a decision which was taken solely automatically, the data subject must know the rationale behind the decision as well as the argumentation and facts upon which it was based. As a result, the data subject should be provided with the concise, transparent, intelligible information on the process of decision-making carried out automatically as only in then they dispose of the data crucial for exercising data subject's rights. As a result, without providing the justification of the decision taken automatically, the guarantees provided for in Article 47 CFREU could be endangered. This issue becomes especially pressing as the application of AI and automated decision-making is being considered not only within private sphere but also in the judicial system.[68]

7.6. BOX: Balancing multiple individuals' rights under article 47 of the Charter. The example of the right to access

The cases where data concerns several data subjects are becoming more and more frequent. An example consists in credit-related data: the information that Mr. Smith owes a sum to Mrs. White concerns both of them. Another case is that of genetic data which concern several individuals, as also recognized by the ECtHR in the case *Marper v. United Kingdom*, 4 December 2008, Rec. n. 30562/04 and 30566/04 and by the Working Group Article 29 in the *Working Document on Genetic Data* of 17 March 2004. Another example is provided by the CJEU in the *Nowak* case, C-434/16, 20 December 2017 where the Court qualified the notes to a written examination test made by an examiner as personal data concerning both the candidate and the examiner.

Personal information in these hypotheses concerns a relationship, for this reason that it seems impossible or highly problematic to distinguish the data concerning each data subject from the information on the relationship. For example: communicating to a bank who is the creditor, but not who is the debtor, is certainly less useful than communicating both names.

The right to access protected by Articles 8(2) CDFUE and 15 GDPR is an example for showing the issue related to the interplay of data subjects' entitlements which have the same data as an object. The

[67] Study on the Human Rights Dimensions of Automated Data Processing Techniques (In Particular Algorithms) And Possible Regulatory Implications Prepared by the Committee of Experts on Internet Intermediaries (MSI-NET) 2018, https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5, 23-26.

[68] In regard to criminal justice see i.a.: Aleš Završnik, Criminal justice, artificial intelligence systems, and human rights, ERA Forum 20, 567–583 (2020). https://doi.org/10.1007/s12027-020-00602-0; and to civil proceeding: *Maria Dymitruk, The right to a fair trial in automated civil proceedings, Masaryk University Journal of Law and Technology 2019,* 13(1), 27.

GDPR already gives account to this issue: the last paragraph of Article 15 (right to access and to copy) states: "the right (...) must not infringe the rights and freedoms of others".
The question arises of how the right to access can be exercised, taking into account the right to access and the right to data protection of each data subject. In this respect, the exercise of the right to copy or portability that does not include relational information, which are personal to various data subjects, would be very weakened, because the information is relational, as seen in the examples above. Furthermore, a risk of veto emerges with respect to the reciprocal exercise of rights, which could put in nothing — or at least significantly weaken — the exercise of the right to access. This may result in the difficulty to take legal action based on the information obtained through the exercise of this right. Article 47 comes into play.
Therefore, in order to coordinate the right to access with the right to data protection to other data subjects, the last paragraph of Article 15 EU Regulation 2016/679 could be interpreted in light of Articles 8 and 47 CDFUE. From this perspective, if the collection of data by a data subject, necessary to the exercise of the right to access falls within the scope of application of the GDPR and data are not of sensitive nature, it could be argued that the data subject exercising the right to copy pursue a legitimate interest in the collection of data that also concerns other data subjects (Article 6(1)(f) GDPR).