FRICoRe

Judicial Training Project

Fundamental Rights In Courts and Regulation

CASEBOOK

JUDICIAL PROTECTION OF HEALTH AS A FUNDAMENTAL RIGHT

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)

Judicial Protection of Health as a Fundamental Right

Edited by Paola Iamiceli, Fabrizio Cafaggi, Chiara Angiolini

Publisher: Scuola Superiore della Magistratura, Rome – 2022

ISBN 9791280600233

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*)

Edition: May 2022

Scientific Coordinator of the FRICoRe Project:

Paola Iamiceli

Coordinators of the team of legal experts on Health Law:

Fabrizio Cafaggi - 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; sec. III: Lucia Busatta
Chapter 1: Lucia Busatta
Chapter 2: Lottie Lane and Tobias Nowak
Chapter 3. Matteo Ferrari and Gianmatteo Sabatino
Chapter 4: Chiara Angiolini
Chapter 5: Lottie Lane and Tobias Nowak
Chapter 6. Simone Penasa
Chapter 7: Chiara Angiolini

Note on national experts and contributors:

The FRICoRe team would like to thank 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)*:

Maria Abbruzzese
Nicoletta Bezzi
Alexandr Biagioni
Līga Biksiniece-Martinova
Dominik Dworniczak
Sébastien Fassiaux
Benedicte Favarque Cosson
Alejandro Fernández
Maxence Fontaine
Franco Frattini
Annabelle Fröhlich
Alexia-Maria Giakkoupi
Inès Giauffret
Guillaume Halard
Mareike Hoffmann
Christopher Hristov
Nikoleta Kiralyova
Heike Koehler
Maria Laura Maddalena
Meron Mekonnen
Marita Miķelsone
Kate Murphy
Sonia Ramos
Donna Savolainen
Verena Schneider
Ana Beatriz Silva de Sa
John Sorabji
Markus Thoma
Patrícia Vargová
Boštjan Zalar
Szimon Zaręba
Christina Zatka

Table of contents

Introduction: A Brief Guide to the Casebook

The FRICoRe Casebook on *Judicial Protection of Health as a Fundamental Right* aims to provide guidance to judges in their complex task of adjudicating cases in which the right to health is at stake, as enshrined not only in most MSs' constitutions but also in Article 35 of the Charter of Fundamental Rights of the European Union (hereinafter CFR). The right to health covers a broad spectrum that includes but does not coincide with the right to health care. Hence right holders are not only patients but also consumers, migrants, and prisoners, to name a few. Its definition results from common constitutional traditions and from EU primary and secondary legislation and refers to both individual and collective interests. The collective dimension of health protection emerges in the field of prevention, but it may also have relevant implications in relation to care and treatment.

Health is a dynamic concept that evolves according to scientific and cultural developments. Governing collective health-related risks entails decision making in situations of uncertainty by both policy makers and Courts. Courts must decide cases on the basis of available scientific knowledge, medical and technical knowledge in particular. But knowledge and technology evolve rapidly and Courts must define principles and rules that can adapt to this evolution and innovation. These changes are reflected in the legal domain both at the EU and national level.

Within the framework of the FRICoRe Project, this Casebook mostly reflects the European dimension of the right to health with a main focus on the judicial dialogue between national Courts and the Court of Justice of the European Union, as well as, in specific instances, the European Court of Human Rights. Such dialogue is likely to increase with the development of litigation concerning matters related to Covid-19.

Covid-19 posed new challenges that are modifying the modes of interaction between EU institutions and MSs. Developed within the framework of Art. 168 TFEU, the EU vaccine policy and the EU Digital COVID Certificate[1] provide good examples of a much broader set of issues generated by the pandemic that are shaping a new institutional equilibrium (see Commission Communication, *Building a European Health Union*, 11 November 2020, COM (2020)724 final). National judiciaries have been guardians of the rights of citizens and have reviewed government choices in the context of the pandemic emergency. The scope of judicial review in times of a pandemic acquired further relevance, given the delegation of powers to executives by legislators. It is too soon to say whether the principles emerging from this case law are likely to remain or whether they will be associated with times of emergency. Clearly the challenges at both the national and EU levels are unprecedented and call for a conceptual legal framework different from that used for previous health crises that are also examined in this Casebook (in Chapter 3 and Chapter 7).

Based on the awareness of States' competence in the organisation of healthcare systems (see below in this Introduction), prior attention has been paid to areas in which the European Union has carried out actions to support, coordinate, or supplement the actions of Member States for the protection and improvement of human health under Article 6, TFEU, or has exercised its legislative competence in fields such as the internal market, consumer protection, cross-border healthcare, and the like, with a view to ensuring, under Article 168 TFEU, a high level of human health protection in the definition and implementation of all Union policies and activities. This choice has allowed us to consider the impact of

[1] Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification, and acceptance of interoperable COVID-19 vaccination, test, and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic.

4 Health and Data Protection[100]

Disclaimer: data protection issues related to COVID-19 are addressed in the data protection section of Chapter 7

4.1. Health Data and their Regime under the GDPR

4.1.1. The Notion of Health Data and their Regime

Under EU law, the GDPR defines the notion of Health data and sketches their legal regime.

Art. 4 (15) Reg. EU 2016/679 defines 'data concerning health' as:

> "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."

In this respect, the CJEU stated that the expression "data concerning health" must be interpreted widely, "so as to include information concerning all aspects, both physical and mental, of the health of an individual" (*Lindqvist,* C-101/01, 6 November 2003). In the same vein, the European Data Protection Board (hereinafter: EDPB) considered that data concerning health can be derived from different sources (*e.g.*, information collected by a health care provider in a patient record, information that becomes health data by cross-referencing with other data thus revealing the state of health or health risks; information from a "self-check" survey, where data subjects answer questions related to their health; information that becomes health data because of its usage in a specific context, such as information regarding a recent trip to or presence in a region affected with COVID-19 processed by a medical professional to make a diagnosis).

Moreover, Art. 4(13) GDPR also defines **genetic data** as:

"personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question."

Genetic data fall into the special category of personal data provided for by Art. 9 GDPR, and the peculiarity of such data is that it concerns **multiple data subjects**, as the ECtHR recognized in *Marper v. United Kingdom*, 4 December 2008, ric. n. 30562/04 e 30566/04. In this respect, the Working Party Art. 29 (now repealed by the EDPB) in its *Working Document on Genetic Data*, adopted on March 17, 2004 recalled that:

"while genetic information is unique and distinguishes an individual from other individuals, it may also at the same time reveal information about and have implications for that individual's blood relatives (biological family) including those in succeeding and preceding generations. Furthermore, genetic data can characterize a group of persons (*e.g.*, ethnic communities)."

Genetic data are a category of data that shows **the complexity of the individual and collective dimensions of data and health protection: the same data may concern several persons and the processing of such data may be necessary for protecting the health of one among the**

[100] This Chapter has been drafted by C. Angiolini.

data subjects or may be used in order to make decisions concerning collective health (*e.g.,* for defining a better therapy for patients with the same genetic characteristics).

The interactions between the individual and collective dimensions of health and data protection go beyond genetic data: health data may concern multiple individuals (*e.g.*, the tumor rate of residents in an identified polluted area), and their processing may be conducted for collective health purposes (*e.g.*, measures to be taken in order to face an epidemic or to minimize health risks in a polluted area).

As to their regime, **health data are qualified by Art. 9 GDPR as special categories of personal data**, which are subject to specific rules for processing set forth in the same Art. 9 (in the European context with regard to the special regime of health data, see also the Council of Europe, Recommendation CM/Rec(2019)2, *Protection of Health-Related Data*).

According to Art. 9 Reg. UE 2016/679, the processing of such data is prohibited, except where the conditions provided for by the second paragraph of that Article are met (*e.g.*, explicit consent; personal data were manifestly made public by the data subject). It should be recalled that in order to legally process special categories of applicable data, both an exception to the prohibition in Art. 9 and a legal basis for its processing, among those provided for in Art. 6 EU Reg. 2016/679, must be applied. In other words, **the processing of special categories of personal data that falls under Art. 9 GDPR should only be done if i) an exception to the prohibition of processing provided for by Art. 9 GDPR is applicable and ii) a legal basis provided for by Art. 6 GDPR applies** (in that regard see: the EDPB, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR) (Art. 70.1.b)* of 23 January 2019, § 28, p. 8; EDPB; *Document in response to a request from the European Commission for clarifications on the consistent application of the GDPR focusing on health research*, 2 February 2021, § 13; European Data Protection Supervisor, *Preliminary Opinion 8/2020 on the European Health Data Space,* 17 November 2020, §§ 15-16).

Moreover, according to Art. 35 GDPR, a data protection impact assessment should be conducted in case of processing of special categories of data on a large scale referred to in Article 9(1), including data concerning health.

4.1.2. Data Processing for Health-Related Purposes

Personal data may be processed for health-related purposes. Generally speaking, in these cases, a legal basis among those provided for by Art. 6 GDPR must be applied. Among the exceptions provided for by Art. 9 GDPR the following are of particular interest:

- processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent (Art. 9(2)(c));

- **processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnoses, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to conditions and safeguards** (Art. 9(2)(h));

- **processing is necessary for reasons of public interest in the area of public health**, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy (Art. 9(2)(i));

- processing is necessary for archiving purposes in the **public interest, for scientific** or historical **research purposes, or statistical purposes** in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. (Art. 9(2)(j)).

An example of application of Art. 6 and 9 is provided for by the EDPB in its *Guidelines 03/2020 on the processing of health data for the purpose of scientific research in the context of the COVID-19 outbreak*, adopted on April 21, 2020. The Board referred to consent (Art. 6, lett. a) and affirmed that Article 6 (1) e)[101] or 6 (1) f)[102] GDPR in combination with the derogations under Article 9 (2) (j) or Article 9 (2) (i) GDPR can provide a legal basis for the processing of personal (health) data for scientific research (for more on scientific research see Question 3 in this chapter).

In this respect, in the pending case ***ZQ v. Medizinischer Dienst der Krankenversicherung Nordrhein, Körperschaft des öffentlichen Rechts*** (C-667/2021) the referring judge asked the CJEU some questions concerning the interpretation of the exception to the prohibition on the processing of health data provided for in Article 9(2)(h) of Regulation (EU) 2016/679, according to which data processing is possible when it is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnoses, the provision of health or social care or treatment, or the management of health or social care systems and services, on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in Art. 9(3). In particular, the referring judge asked whether Article 9(2)(h) of Regulation (EU) 2016/679 is to be interpreted as prohibiting a medical service of a health insurance fund from processing its employee's health data which are a prerequisite for the assessment of that employee's working capacity.

Moreover, the referring judge asked whether in case Art. 9 lett. h) applies, i) the lawfulness of the processing of health data depends on fulfilment of at least one of the conditions set out in Article 6(1) GDPR; ii) if there are data protection requirements beyond the conditions set out in Article 9(3) GDPR, that must be complied with and, if so, which are such requirements.

[101] Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

[102] Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Main question addressed

Question 1 What is the role of the principles of effectiveness and proportionality and Art. 8 ECHR in assessing the lawfulness of the sharing of patients' personal data and of their public disclosure?

Question 2 How do the principle of mutual cooperation and the right to data protection (Art. 8 CFR) influence the processing of health data carried out or to be carried out by MSs in cross-border healthcare?

Question 3 What is the relationship between the right to data protection and the collective dimension of the right to health related to scientific research? In particular: i) What is the relationship between informed consent for participating in medical research and consent as a legal basis for processing? ii) what is the impact of the principles of proportionality and Art. 8 CFR in relation to health and the "compatibility presumption" concerning the processing purpose of scientific research (Article 5 (1) (b) GDPR)? iii) what is the role of proportionality in interpreting Art. 89 GDPR, with regard to safeguards and derogations relating to processing for scientific research purposes or statistical purposes?

Question 4 How health and data protection, in light of the principles of effectiveness, proportionality, and the right to data protection (Art. 8 CFR) may influence the definition of the processing of personal health data to be carried out within Health Data Spaces?

Question 5 What is the role of the principles of effectiveness, proportionality, and necessity with respect to personal data processing within the framework of the EU Digital COVID Certificate?

4.2. Health Data Processing between Individual and Collective Interests.

Question 1 - Access to health data by health professionals, public institutions and the public in light of effective data protection

What is the role of the principles of effectiveness and proportionality and Art. 8 ECHR in the legal assessment of the sharing of patients' personal data among institutions and of their public disclosure?

The following decisions of the European Court of Human Rights (hereinafter: ECtHR) are considered:

- ECtHR, *J.M. and A.T. v. North Macedonia*, App. no. 79783/13, of 22 October 2020.
- ECtHR *S. and Marper v. the United Kingdom*, App. nos. 30562/04 and 30566/04, 4 December 2008
- ECtHR *Avilkina and Others v. Russia*, no. 1585/09, 6 June 2013
- ECtHR, *Radu v. the Republic of Moldova*, 50073/07, 15 April 2014
- ECtHR, *Mockutė v. Lithuania*, app. no. 66490/09, 27 February 2018
- ECtHR, *I v. Finland,* app. no. 20511/03, 17 July 2008

- ECtHR, *Z. v. Finland*, App. No. 22009/93, 25 February 1997
- ECtHR *M.S. v. Sweden,* app. No. 74/1996/693/885, 27 August 1997

The analysis is mainly based on the **ECtHR case *J.M. and A.T. v. North Macedonia*, App. no. 79783/13, of 22 October 2020.**

The case

After a public health center for drug addiction reported to the police that an unspecified quantity of methadone was missing, the police visited the hospital and seized the original copies of lists used to identify daily methadone patients. The national DPA conducted an onsite inspection of the hospital, and stated, in its report, that the police had seized the two original lists, which contained the applicants' names, surnames, and the methadone they had received during treatment. The police were also allowed to examine a "methadone-reporting book" and individual patient files in order to verify the quantities of methadone that they had been prescribed. The DPA concluded that the police had acted lawfully, and in accordance with the Criminal Procedure Act. After some time, the police stated that there had been no elements of a crime with regard to the missing methadone and returned the seized lists to the hospital.

Afterwards, the applicants, together with four other patients of the hospital, submitted a request to the DPA for the protection of personal data against the hospital and the police. They argued that the hospital had disclosed sensitive medical data to the police without a Court order. The DPA rejected their claim, stating that data processed by the police were anonymized. The Administrative Courts before which the applicants contested the DPA's decision upheld the DPA decision. Meanwhile, a civil action for compensation of non-pecuniary damages was brought. The applicants argued that the hospital had unlawfully given access to their medical data to the police. The Court dismissed the claim stating that data processed by the police were anonymized, and the decision was confirmed in the appeal judgment.

Fundamental rights violation addressed by the Court

The applicants complained that the hospital had unlawfully disclosed their medical data to the police, thereby violating their right to a private life as protected under Article 8 ECHR, according to which:

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

Reasoning of the Court

As to the facts, the Court considered that the hospital had disclosed patients' personal data to the police.

With regard to legal reasoning, first, the Court, relying on previous case law, stated that **the disclosure by a state hospital of applicants' medical data to the police constituted an interference with the applicants' right to respect for their private life as secured by Article 8 § 1 ECHR**.

Second, the Court examined whether that interference was justified in terms of Article 8 § 2 of the Convention, that is, whether it was in accordance with the law, pursued a legitimate aim, or was "necessary in a democratic society."

In this respect, the Court stated that the disclosure at issue i) **had a basis in domestic law** (§§ 44-45); and ii) **pursued a legitimate aim** of detection and prevention of crime.

The Court then addressed the question whether the disclosure of the applicants' data was **"necessary in a democratic society."** In this respect, the Court stated that the Government did not prove why it was **necessary** for the police to obtain full access to medical data regarding the applicants, taking into account that: i) the police took no investigative measures on the basis of the medical data; ii) the police had other options for following up on the complaint with regard to the missing methadone, (*i.e.*, they could have interviewed hospital staff before examining applicants' medical data). In that regard, the Court noted that it was an interview with one of the doctors at the hospital that was relied upon by the police in their decision to terminate the investigation into the alleged offence; iii) the domestic Courts failed to balance the protection of patients' rights against the right of the police to access sensitive medical data without a Court order.

Conclusion of the Court

The Court concluded that the collection by the police of the applicants' confidential medical data was not accompanied by sufficient safeguards to prevent disclosure which was inconsistent with the respect for the applicants' private life guaranteed under Article 8 ECHR. Accordingly, **the Court stated that there was therefore a violation of Article 8 ECHR.**

Elements of judicial dialogue - ECtHR

On the basis of Art. 8 (2) ECHR, the Court assessed the justification of interference by evaluating whether it was "**in accordance with the law**," **pursued one or more of the legitimate aims** specified therein, and to that end it was "**necessary in a democratic society**." As to **States' obligations,** in ***I v. Finland,* app. no. 20511/03, of 17 July 2008** the Court reiterated that Art. 8 ECHR is applicable in case of processing of personal data relating to a patient as this information belongs to his or her private life. Furthermore, the Court considered that this Article does not merely compel the State to abstain from arbitrary interference, but that **there may be positive obligations inherent in the effective respect for private or family life.**

In several instances the ECtHR applied this provision in cases concerning health data. The following aspects, considered within case law, are of particular interest with regard to the application of Art. 8 ECHR:

i) Assessment concerning the existence of interference with Art. 8 ECHR

In *J.M. and A.T. v. North Macedonia* the Court relied on previous judgements, recalling, with regard to the general principles applicable to the case, *S. and Marper v. the United Kingdom* App. nos. 30562/04 and 30566/04, 4 December 2008, and *Avilkina and Others v. Russia* (no. 1585/09, §§ 43-46, 6 June 2013; *Radu v. the Republic of Moldova*, 50073/07, § 27, 15 April 2014).

In ***S. and Marper v. the United Kingdom*** the Court, in determining whether the personal information retained by authorities involved any aspects of private-life, took the specific context in which the

information at issue was recorded and retained into account such as the nature of the records, the way in which such records were used and processed, and the results that could be obtained.

In ***I v. Finland,*** app. no. 20511/03, of 17 July 2008, with regard to the importance of confidentiality of health data, the Court stated that:

> "respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general" (see also, in the same vein, *M.S. v. Sweden,* app. No. 74/1996/693/885, of 27 August 1997; *Z. v. Finland*, App. No. 22009/93, of 25 February 1997; *Avilkina and Others v. Russia* no. 1585/09, 6 June 2013).

In the same vein, in ***Mockutė v. Lithuania***, app. no. 66490/09, of 27 February 2018, the Court affirmed that in case of a lack of health data confidentiality, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby **endangering their own health and, in the case of transmissible diseases, that of the community** (In the same vein see also, *Z. v. Finland*, App. No. 22009/93, of 25 February 1997).

As for examples of cases where the Court stated that there was an interference with Art. 8 ECHR:

- In ***Radu v. the Republic of Moldova,*** (50073/07, 15 April 2014) the Court stated that disclosure of sensitive details about the applicant's pregnancy and her state of health by a Center for family doctors to the applicant's employer constituted interference with her right to private life;

- In ***M.S. v. Sweden,*** (app. No. 74/1996/693/885, of 27 August 1997) the Court stated that the Hospital's disclosure of medical records containing highly personal and sensitive data about the applicant, including information relating to an abortion, to another public authority and therefore to a wider circle of public servants constituted an interference with Art. 8 ECHR.

- In ***Z. v. Finland,*** (App. No. 22009/93, of 25 February 1997) the Court stated that there was an interference with Art. 8 ECHR with respect to the following processing of health data consisting in the applicant's condition as a carrier of HIV: 1) the orders requiring her doctors to give evidence in the criminal proceedings against her husband, (2) the seizure of her medical records and their inclusion in the investigation file, (3) the decision to make the material in question accessible to the public from the year 2002 and (4) the disclosure of her identity and medical condition in a judgment by the Court of Appeals.

- in ***Mockutė v. Lithuania***, app. no. 66490/09, of 27 February 2018, the Court pointed out that the disclosure to journalists of highly personal and sensitive confidential information about the applicant, obtained during her involuntary hospitalisation and treatment, by a psychiatrist doctor of the Vilnius Psychiatric Hospital entailed an interference with the applicant's right to respect for her private life guaranteed by Article 8 (1) ECHR. The Court affirmed that the disclosure of medical data by medical institutions to a newspaper, to a prosecutor's office, and to a patient's employer, as well as the collection of a patient's medical data by an institution responsible for monitoring the quality of medical care constituted an interference with the right to respect for private life.

ii) In accordance with the law

In *Mockutė v. Lithuania*, app. no. 66490/09, of 27 February 2018, the Court found that, as the disclosure of the data at stake was prohibited under national law, and exceptions to that prohibition were not applicable to the case, the processing was not in accordance with the law.

iii) Existence of a legitimate aim

As for examples of a "legitimate aim" which could justify the processing, the Court considered: i) the needs of processing within a trial (*Z. v. Finland*, App. No. 22009/93, of 25 February 1997); ii) the detection and prevention of crimes (*S. and Marper v. the United Kingdom*, App. nos. 30562/04 and 30566/04, 4 December 2008); iii) protecting the economic well-being of the country in deciding on the allocation of public funds (*Mockutė v. Lithuania*, app. no. 66490/09, of 27 February 2018).

iv) Necessity in a democratic society

The ECtHR's judgment ***Z. v. Finland*,** (App. No. 22009/93, of 25 February 1997) is of particular interest for our analysis, as it shows **the importance of collective and individual interests in the Court's application of proportionality**. In such a case, concerning the disclosure of health data relating to the fact that the applicant was an HIV carrier, the Court considered both the **collective and individual dimension of the impact on fundamental rights of the disclosure regime**. As to the position of the data subject, from an individual point of view, the Court considered that the disclosure of such data may dramatically affect the applicant's private and family life, as well as social and employment situation, by exposing her to opprobrium and the risk of ostracism. As for the **collective point of view**, the ECtHR pointed out that the individual risks of disclosure also discourage persons from seeking diagnosis or treatment and thus undermine any preventive efforts by the community to contain the pandemic. With regard to the public interest that could override the interests of confidentiality, the Court considered that i) **any State measures providing the disclosure of such information without the consent of the patient call for the most careful judicial scrutiny, as do the safeguards designed to secure effective protection;** ii) the confidentiality of medical data may be outweighed by the interest in **investigation and prosecution of crime** and in the publicity of Court proceedings, where such interests are shown to be of even greater importance; iii) as to the data disclosure to the public, the Court recognized the national authorities' **margin of appreciation in striking a fair balance** between the interest of publicity of Court proceedings, on the one hand, and the interests of a party or a third person in maintaining the confidentiality of such data, on the other. Moreover, the Court stated that the scope of this margin depends on such factors as the nature and seriousness of the interests at stake and the gravity of the interference.

In ***Avilkina and Others v. Russia*** (no. 1585/09, 6 June 2013) the Court pointed out that **the interests of a patient and the community as a whole in protecting the confidentiality of medical data may be outweighed by the interest of investigating and prosecuting crime and in the publicity of Court proceedings, where such interests are shown to be of even greater importance.** Moreover, the Court stated that in determining whether the impugned measures were "necessary in a democratic society," the Court considered whether, in light of the case as a whole, the reasons adduced to justify them were relevant and sufficient and the **measures were proportionate to the legitimate aims pursued**. Furthermore, the Court stated that in cases concerning the disclosure of personal data, the competent national authorities have a **margin of appreciation** in striking a fair balance between the relevant conflicting public and private interests. However, the Court stated that this margin goes hand in

hand with European supervision and the scope of this margin depends on such factors as the nature and seriousness of the interests at stake and the gravity of the interference.

In ***M.S. v. Sweden*** (app. No. 74/1996/693/885, of 27 August 1997) the Court assessed the **proportionality of the interference** (the disclosure of health data, including data concerning an abortion, to the Social Services office) and stated that there was no violation of Art. 8 ECHR. The Court took into account that the data were communicated to the office to assess whether the applicant satisfied the legal conditions for obtaining a benefit which she had requested and that in deciding whether to accept the applicant's compensation claim, the Office had a legitimate need to check information received from her against data in the possession of the clinic. Furthermore, the Court considered that in the absence of objective information from an independent source, it would have been difficult for the Office to determine whether the claim was well-founded. Moreover, the Court took into account that the processing was subject to important limitations and was accompanied by effective and adequate safeguards against abuse (*e.g.*, the duty of confidentiality of public authorities processing data; civil and/or criminal liability had they failed to observe the provided safeguards).

Another important aspect is that of remedies the data subject can rely on in case of violations. In this respect, in ***I v. Finland,*** **app. no. 20511/03, of 17 July 2008** the Court stated that:

> "the mere fact that the domestic legislation provided the applicant with an opportunity to claim compensation for damages caused by an alleged unlawful disclosure of personal data was not sufficient to protect her private life. **What is required in this connection is practical and effective protection to exclude any possibility of unauthorised access occurring in the first place.** Such protection was not given here."

Elements of judicial dialogue – national

France

With regard to the access regime to health data, French Council of State judgment no. 428451, of 25 November 2020 is of particular interest. In that decision the Council of State quashed the Decree No. 2018-1254 of December 26, 2018, on medical information departments insofar as it did not provide: i) technical and organizational safeguards suitable for ensuring pseudonymization and the absence of processing of identifying data during the access of auditors to personal health data collected during the analysis of healthcare activity; ii) technical and organizational measures to ensure that only the identifying data necessary for the purposes of the processing are processed with sufficient guarantees when external service providers have access to these data, and provisions to ensure that they actually perform their activities under the authority responsible for medical information.

Italy

With regard to the balancing of the collective interest with that of the data subject, the judgment of the Italian Court of Cassation no. 9382 of 4 April 2019 is of particular interest. In that decision, the Court stated that the protection of sensitive data prevailed over a generic need for administrative transparency. Furthermore, as to the collective dimension of health data protection, the Italian Court of Cassation's decision no. 16816 of 26 June 2018 must be considered. The case concerned the sensitivity of data relating to the health of a child with respect to their parents. The Court stated that the state of health of a family member (in the present case, of a minor daughter and a cohabiting sister), considered as the basis of a competitive privilege concerning admission to school courses for minors (as such potentially capable of being translated into information that immediately relates to the sphere of family life), was characterized by the same intrinsic sensitivity that identifies vulnerability and a consequent need for confidentiality, similar to those referring to a sick person when she exposes her illness to a third party, or to a Public Administration. According to the Court, therefore, the sensitive data related to the health condition of the child, as it characterizes the overall status of rights, as well as personal and social conditions which belong to the parents and, in general, to family members linked by ties of the community of family life or the home, is also sensitive data referable to the latter.

Spain

With regard to the notion of "health data" Tribunal Supremo **judgment No 129/2019** (ECLI:ES:TS:2019:3739), of 26 November 2019, concerning penal evidence constating in health data, used in a proceeding against a soldier who affirmed that he was at hospital on a specific day is of particular interest. The Tribunal stated that everyone has the right to respect the confidential nature of the data concerning their health and that no one can access them without prior authorization protected by law, as part of their right to privacy (Art. 7.1 of Law 41/2002 of November 14, 2002, on patient autonomy). Furthermore, the Court considered that clinical history, defined in Art. 3 of this law as the set of documents containing the data, assessments, and information of any kind on the situation and clinical evolution of a patient throughout the care process, would be included in this right to privacy and would also form part of the sensitive data, the core of privacy. Nevertheless, the tribunal pointed out that what is certainly not subject to legal protection are the data that could be considered "innocuous" and that would therefore be outside legally protected privacy, which is what happened in the present case. Considering that the information provided by the employee of a Medical Center, who was obliged to provide the information about the attendance of the defendant at the said center, turned out to be a completely innocuous piece of information within the patient's history that in no way affected his privacy, nor was it part of the content of his medical history as set forth in Article 15 of the Law on Patient Autonomy. Furthermore, the Court considered that the defendant himself provided this information, which in the end turned out to be false. Therefore, according to the Court, in the absence of any unlawfulness in the evidence incorporated into the proceedings, it would be redundant to rule on any type of connection of unlawfulness with the rest of the proceedings, provided that the information provided to the commanders of the then appellant did not constitute, from any point of view, a piece of information concerning his health, so it can hardly be argued that the right to privacy enshrined in Article 18 of the Law was undermined. The fact that he did not go to the private health center and that, therefore, he was not assisted on a certain day, and this without providing any details of a strictly sanitary or clinical nature, were circumstances that did not support the appellant's thesis.

With regard to the balance between the protection of health data and the right to be informed, in **the judgment of the Audiencia Nacional, of 29 November 2019** (ECLI:ES:AN:2019:4627) the Court

stated that the right to privacy of the people who were victims of the terrorist attack of March 11, 2004, in Madrid must prevail over the right to information.

Sweden
In December 2020 the EDPB communicated the news that the Swedish Data Protection Authority had audited eight health care providers in how they governed and restricted access by personnel to the main systems for electronic health records. The DPA discovered insufficiencies that in seven of the eight cases led to administrative fines of up to SEK 30 million (see https://edpb.europa.eu/news/national-news/2020/deficiencies-how-healthcare-providers-control-staff-access-patient-journal_en).

The Swedish Data Protection Authority primarily examined whether the health care providers had conducted the needs and risk analysis required in order to assign adequate access authorization for personal data in electronic health records. The DPA stated that i) Health care providers must carry out an assessment of personnel's need to access information in health records and the risks of accessing patient data; ii) if such an assessment is not carried out, health care providers cannot assign the personnel a correct level of authorization, with the consequence that the organizations cannot guarantee patients' right to privacy. As seven of the health care providers had not carried out a needs and risk analysis, the authority concluded that such providers did not limit user access authorization to the respective patient journal system to what is strictly necessary for the performance of their tasks.

The deficiencies of these providers resulted in administrative fines between SEK 2.5 to 30 million. The Swedish Data Protection Authority developed guidelines summarizing the conclusions from the audits with regard to the obligation to conduct needs and risk analyses.

Question 2 – Cross border health care and MSs' role with regard to health data: the eHealth Network

How do the principle of mutual cooperation and the right to data protection (Art. 8 CFR) influence the processing of health data carried out or to be carried out by MSs in cross-border healthcare?

EU legislation: Art. 14 of the EU directive on patients' rights: the eHealth network and the related data processing

Art. 14 'eHealth' of dir. 2011/24 on the application of patients' rights in cross-border healthcare reads as follows:

> "1. The **Union shall support and facilitate cooperation and the exchange of information among Member States** working within a voluntary network connecting national authorities responsible for eHealth designated by the Member States.
>
> 2. The objectives of the eHealth network shall be to: (a) work towards delivering sustainable economic and social benefits of European eHealth systems and services and interoperable applications, with a view to achieving a high level of trust and security, enhancing continuity of care, and ensuring access to safe and high-quality healthcare;
>
> (b) draw up guidelines on: (i) a non-exhaustive list of data that are to be included in patients' summaries and that can be shared between health professionals to enable continuity of care and patient safety across borders; and (ii) effective methods for enabling the use of medical information for public health and research;

(c) support Member States in developing common identification and authentication measures to facilitate transferability of data in cross-border healthcare.

The objectives referred to in points (b) and (c) shall be pursued in due observance of the principles of data protection as set out, in particular, in Directives 95/46/EC and 2002/58/EC.

3. The Commission shall, in accordance with the regulatory procedure referred to in Article 16(2), adopt the necessary measures for the establishment, management, and transparent functioning of this network."

Since the entry into force in 2018 of Reg. EU 2016/679 (GDPR), by reason of Art. 94(2) of that regulation, the references to repealed Directive 95/46 must be red as references to the Regulation.

Moreover, recital 25 of dir. 2011/24, **underlines, on the one hand, that the right to the protection of personal data is a fundamental right recognised by Article 8 CFREU and, on the other hand, that ensuring continuity of cross-border healthcare depends on the transfer of personal data concerning patients' health.** Accordingly, this recital provides that such personal data should be able to flow from one Member State to another, but at the same time the fundamental rights of the individuals should be safeguarded.

As for data protection roles with regard to data processing within the context of the eHealth Network, Art. 7 of the Commission Implementing Decision 2019/1765 of 22 October 2019 providing the rules for the establishment, the management, and the functioning of the network of national authorities responsible for eHealth, as modified by the Commission Implementing Decision (EU) 2020/1023 of 15 July 2020, states that:

"1. **The Member States**, represented by the relevant National Authorities or other designated bodies shall be regarded **as controllers of personal data** they process through the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services and **shall clearly and transparently allocate the responsibilities between controllers.**

2. **The Commission shall be regarded as data processor for patients' personal data processed through the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services**. In its capacity as processor, the Commission shall manage the core services of the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services and shall comply with the obligations of a processor laid down in the Annex I to this Decision. The Commission shall not have access to patients' personal data processed through the eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services.

3. The Commission shall be regarded as controller of the processing of the personal data necessary to grant and manage access rights to the core services of eHealth Digital Service Infrastructure for Cross-Border eHealth Information Services. Such data are contact details of users, including name, surname and email address and their affiliation."

According to recital 20 of this EU Commission decision, the respective responsibilities between controllers should be defined in a separate arrangement (on the notion of controller and joint controllership in light of the CJEU case law, including *Fashion ID,* C-40/17, see the FRICoRe Casebook

Effective Data Protection and Fundamental Rights, Chapter 2, question 3; on the position of Member States and of the Commission see also the *EDPB-EDPS Joint Opinion 1/2019 on the processing of patients' data and the role of the European Commission within the eHealth Digital Service Infrastructure (eHDSI).*

Question 3 – Principle of proportionality, the protection of collective and public health, and the processing of health data for purposes of public research

What is the relationship between the right to data protection and the collective dimension of the right to health related to scientific research?

In particular:

- What is the relationship between informed consent for participating in medical research and consent as a legal basis for processing?

- What is the impact of the principles of proportionality and Art. 8 CFR in relation to health on the "compatibility presumption" concerning the purpose of processing for scientific research (Article 5 (1) (b) GDPR)?

- What is the role of proportionality in interpreting Art. 89 GDPR, with regard to safeguards and derogations relating to processing for scientific research purposes or statistical purposes?

The legislative framework

The Articles of Reg. UE 2016/679 do not specifically define data processing for scientific research purposes (On the complex definition of scientific research boundaries, see EDPS, *A Preliminary Opinion on data protection and scientific research*, 6 January 2020). Nevertheless, according to recital 159 of the GDPR,

> "the processing of personal data for scientific research purposes should be interpreted in a broad manner including, for example, technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of **public health**. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular with regard to the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular **in the health context** gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures."

Several specificities of (health) data processing for scientific purposes may be recalled:

i) the presumption of compatibility of "further processing" according to Art. 5 GDPR.

Art. 5(1)(b) GDPR provides that personal data must be:

> "collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')."

ii) specific rules on data storage:

According to Art. 5(1)(e) GDPR data must be:

> "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')."

iii) Art. 89 GDPR regulates safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

Art. 89 reads as follow:

> 1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled accordingly.
>
> 2. Where personal data is processed for scientific or historical research purposes or statistical purposes, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of those specific purposes, and such derogations are necessary for their fulfilment.
>
> 3. Where personal data is processed for archiving purposes in the public interest, Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18, 19, 20, and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of those specific purposes, and such derogations are necessary for their fulfilment.
>
> 4. Where processing referred to in paragraphs 2 and 3 serves another purpose at the same time, derogations shall apply only to processing for the purposes referred to in those paragraphs.

The regulation of data processing for scientific research purposes is relevant with regard to several fundamental rights. In this respect, the EDPB in its *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak,* adopted on April 21, 2020, stated that:

> "**Data Protection Rules nor the Freedom of Science pursuant to Article 13 of the Charter of Fundamental Rights of the EU have precedence over the other. Rather, these rights and freedoms must be carefully assessed and balanced, resulting in an outcome which respects the essence of both.**" (In the same vein, see EDPS, *A Preliminary Opinion on data protection and scientific research*, 6 January 2020, p. 11).

With regard to the specificities of processing health data for purposes of scientific research, recently the EDPB, in its *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, adopted on February 2, 2021, highlighted that **the specific processing regime** provided for within the GDPR with regard to scientific research **only aims to provide for exceptions to specific requirements in specific situations and that the use of such exceptions is made dependent on the existence of 'additional safeguards'** (see Article 89(1) GDPR). Moreover, the EDPS in its *Preliminary Opinion on data protection and scientific research*, adopted on January 6, 2020, pointed out that from a data protection viewpoint, **the principles of necessity and proportionality** are essential.

In particular, the following aspects were considered:

i) Informed consent for participating in the research, consent to the processing, and lawfulness of processing according to Art. 6 and Art. 9 GDPR

The EDPS in its *Preliminary Opinion on data protection and scientific research*, adopted on January 6, 2020, and the EDPB, in its *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, adopted on February 2, 2021, clarified that with regard to consent, **two different legal issues are at stake**: i) the existence and the conditions of informed consent for participation in a scientific research project and ii) the lawfulness of processing according to Art. 6 and 9 GDPR (on this issue, see above, the introduction).

Accordingly, where other legal bases and exceptions according to Art. 6 and Art. 9 GDPR apply (some examples are provided in the introduction to this chapter), health data could also be processed in the absence of consent to its processing. This does not imply that informed consent is not required (EDPB, *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, adopted on February 2, 2021; see also EDPB *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR),* adopted on January 23, 2019).

Moreover, with regard to a data subject's consent as a legal basis for processing, the EDPB, in line with recital 43 GDPR (according to which, in order to ensure consent is freely given, consent should not be used as a legal basis for processing where there is a clear imbalance between the data subject and the controller), stated that in clinical trials such an imbalance may exist depending on the circumstances, for instance, when the data subject is not in a good health condition and there is no available therapeutic treatment outside the clinical trial. Nevertheless, the EDPB stated that:

"Explicit consent as a legal basis can still be relied upon in medical research projects where it can be established that no imbalance of power between data subjects and researchers exists and the requirements for explicit consent in GDPR can be met. However, this will require a careful assessment on a case-by-case basis" (EDPB, *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, adopted on February 2, 2021).

Moreover, with regard to the Health Data Space, the EDPS in its *Preliminary Opinion 8/2020 on the European Health Data Space* on November 17, 2020 stated that, as the scope of the EHDS' creation is to enhance access to health data in order to allow for evidence-based policy decisions and for scientific research within the EU, the consent of the data subject, is not the most appropriate legal basis for processing. Rather, the EDPS considered that Article 6(1)(e) GDPR may possibly be the most appropriate legal basis for the processing of personal data in the context of the functioning of the EHDS, as the platform's main purpose will be to serve the public interest and the processing should be done in the exercise of official authority vested in the controller.

i) The presumption of compatibility of "further processing" according to Art. 5 GDPR.

The EDPB, in its *Document on response to the request from the European Commission for clarifications on the consistent application of the GDPR, focusing on health research*, adopted on February 2, 2021, stated that the presumption of compatibility can only be used under the condition that in such further processing for scientific research purposes adequate safeguards as required by Article 89(1) GDPR are respected.

Furthermore, according to the EDPB *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR),* adopted on January 23, 2019, where the compatibility presumption applies, the controller shall not be deemed exempt from the other obligations under data protection law, for example with regard to fairness, lawfulness, necessity, and **proportionality**.

ii) Specific rules on data storage

The EDPB in its *Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak,* adopted on April 21, 2020, stated that the storage period should be **proportionate**, taking into account also the length and the purpose of the research.

iii) Art. 89 GDPR regulates safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.

The EDPS in its *Preliminary Opinion on data protection and scientific research*, adopted on January 6, 2020 highlighted that the rights of access and rectification are set out in Article 8(2) CFR, and are generally considered essential components of the right to protection of personal data. Moreover, the EDPS considered that the right of access is of particular importance as it enables data subjects to exercise other rights. Accordingly, the EDPS stated that derogations from these rights are only possible if the conditions and safeguards required under Article 89(1) are essential data subject rights and must be subject to a particularly high level of scrutiny in line with the standards required by Article 52(1) CFR, including the **proportionality** test.

Question 4 – Looking forward: sharing health data in Health data spaces

How do health and data protection, in light of the principles of effectiveness, proportionality, and the right to data protection (Art. 8 CFR) influence the definition of the processing of personal health data to be carried out within Health Data Spaces?

Looking forward: Common European Health data spaces

Within the European strategy for data ('Data Strategy') one important objective is to create Common European data spaces in strategic sectors and domains of public interest for increasing the possibilities for public authorities and businesses to access high-quality data. An important field is health, where the creation of '**a Common European health data space**' (EHDS) is considered essential by the Commission for fostering advances in preventing, detecting, and curing diseases as well as for informed, evidence-based decisions to improve the accessibility, effectiveness, and sustainability of the healthcare systems (see Communication *A European strategy for data*, 19 February 2020).

The EDPS adopted the *Preliminary Opinion 8/2020 on the European Health Data Space* on November 17, 2020, where the EDPS recalled that EHDS will be "an essential tool to improve the accessibility, **effectiveness**, and sustainability **of health systems** as well as to allow informed, evidence-based policy decisions relating to them." However, it also affirmed the importance of data protection in light of Art. 7 and Art. 8 CFR. Moreover, in assessing the right to data portability, the EDPS stated that the right to data portability is essential to enhance "control" by data subjects over their data and that imperfect data portability mechanisms that currently exist can present an obstacle to the **effectiveness** of this right.

The EDPS **cited the proportionality principle** in assessing the possibility of data processing for scientific research purposes. According to the EDPS such processing must be, under Article 89(1), based on Union or Member State law which requires the processing to be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. Moreover, the EDPS referred to the principle of **proportionality, jointly with necessity,** also in assessing the sources of that data. Relying on these principles, the Board affirmed that the data made available within the EHDS should, as a general rule, be anonymized and aggregated. The EDPS considered that if this is not possible due to the nature of the data at stake and the purpose of the processing, the data should be pseudonymized.

On 3 May 2022 the European Commission presented a ***Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space***. In the Explanatory memorandum, the Commission affirms that the provisions of the proposal are complementary to data protection law and that:

"The proposal is expected to have a significant positive impact on fundamental rights related to the protection of personal data and free movement. (…) Natural persons will have additional possibilities to digitally access and transmit their electronic health data, building upon provisions in the GDPR. Market operators in the health sector (either healthcare providers or providers of digital services and products) will be obliged to share electronic health data with user-selected third parties from the health sector. The proposal will provide the means to enforce these rights (through common standards, specifications and labels) without compromising on the required safety measures to protect natural person rights under the GDPR. It would contribute to the increased protection of health-related personal data and the free movement of such data as enshrined in Article 16 TFEU and in the GDPR."

Looking at the text of the proposal, art. 3 establishes the "Rights of natural persons in relation to the primary use of their personal electronic health data". Furthermore, the proposal distinguishes between primary and secondary uses and regulates them. In particular, primary uses concerns "the processing of personal electronic health data for the provision of health services to assess, maintain or restore the state of health of the natural person to whom that data relates, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social security, administrative or reimbursement services" (Art. 2 (1)(d) of the proposal), while secondary uses are identified and regulated in chapter 4 of the proposal both with regard to the categories of data (art. 33 of the proposal) and the purposes of processing (art. 34 of the proposal).

Question 5 – Health data and COVID-19 Certificates

What is the role of the principles of effectiveness, proportionality, and necessity with respect to personal data processing within the framework of the EU Digital COVID Certificate?

Regulation (EU) 2021/953 built a framework for the issuance, verification, and acceptance of interoperable COVID-19 vaccination, test, and recovery certificates (EU Digital COVID Certificate) to facilitate freedom of movement during the COVID-19 pandemic.

The adoption of the "EU digital COVID certificate" system implies the processing of special categories of personal data, such as health data, for purposes that affect the exercise of freedom of movement. In this regard, in Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification, and acceptance of interoperable certificates on vaccination, testing, and recovery to facilitate freedom of movement during the COVID-19 pandemic (Digital Green Certificate) the EDPS and the EDPB stated that:

> "the general principles of **effectiveness, necessity, and proportionality** must guide any measure adopted by Member States or EU institutions that involve processing of personal data to fight COVID-19" (§ 12)

Moreover, the two Authorities affirmed that:

> "Pursuant to Article 52 of the Charter, '[s]ubject to the principle of **proportionality**, limitations to the rights and freedoms recognised by the Charter may be made only if they are **necessary** and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.' In accordance with this, compliance with the principles of **necessity and proportionality** by the measures introduced with the Proposal should carefully be analysed. In particular, the Proposal should achieve a fair balance between the objectives of general interest pursued by the Digital Green Certificate and the individual interest in self-determination, as well as the respect for her/his fundamental rights to privacy, data protection and non-discrimination, and other fundamental freedoms, such as freedom of movement and residence."

The Regulation applies until June 30, 2022, and the EU Commission adopted a proposal to amend Regulation 2021/953, and the EDPS and the EDPB issued joint Opinion 1/2022 on the proposal. In that Opinion, the Authorities stated:

> "(…) the **general principles of effectiveness, necessity and proportionality** must guide any measure adopted by Member States or EU institutions that involve processing of personal data

to fight COVID-19. A regular assessment on any measures to fight the COVID-19 pandemic should take place, having regard to the relevant scientific evidence and additional measures in place, **in order to continuously evaluate which actions remain effective, necessary and proportionate**."

In particular, the EDPB and the EDPS recalled that neither the original proposal for the Regulation nor the new Proposals have been accompanied by an impact assessment and that according to Art. 16 (2) of the Regulation, the Commission must submit a report to the European Parliament and the Council on the application of the Regulation by March 31, 2022, specifically containing an assessment of the impact of the Regulation on the facilitation of free movement, fundamental rights, and non-discrimination, as well as on the protection of personal data during the COVID-19 pandemic. In this respect, the Authorities stated that the new proposal should be accompanied by the abovementioned report, in order to provide a **clear justification for the necessity and proportionality** of the First Proposal, taking into account, among other things, the evolution of the epidemiological situation with regard to the COVID-19 pandemic together with the impact on fundamental rights and non-discrimination, particularly on the basis of the possession of a specific category of medical certificate.

Moreover, the Authorities affirmed **the need to continuously evaluate which measures remain effective, necessary, and proportionate with regard to the purpose of fighting the COVID-19 pandemic.**

4.3. Guidelines Emerging from the Analysis

Health data are qualified as "special categories of personal data" (Art. 9 GDPR), and accordingly, they are subject to a specific regime that takes into account the need to protect privacy and the right to data protection as well as the importance of data processing for health protection purposes (*e.g.*, the general prohibition on processing and exceptions related to health purposes).

The need to take both health and data protection into account emerges also in the interpretation and application of Art. 14 of the EU directive on patients' rights concerning data processing within the context of the eHealth network, with specific regard to the need to ensure continuity of care across Member States.

Furthermore, health and data protection are at stake in the interpretation of rules concerning data processing for purposes of scientific research, where the principle of proportionality may play a significant role (EDPS, *Preliminary Opinion on data protection and scientific research*, adopted on January 6, 2020; EDPB *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection Regulation (GDPR),* adopted on January 23, 2019).

Moreover, the principle of proportionality, alongside necessity, should play an important role in the current planning of data processing within Health Data Spaces (EDPS *Preliminary Opinion 8/2020 on the European Health Data Space* adopted on November 17, 2020), jointly with fundamental rights (Explanatory memorandum of the *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space*, adopted on 3 May 2022*).*

In defining the boundaries of lawful health data sharing and disclosure Art 8 ECHR, enshrining the right to respect of private and family life is of particular importance, as shown by case law. In the ECtHR case

law, the complementarity between data and health protection arises. As for complementarity, in several cases the Court stated that in cases of a lack of health data confidentiality, those in need of medical assistance may be deterred from revealing such information of a personal and intimate nature as may be necessary in order to receive appropriate treatment and, even, from seeking such assistance, thereby endangering their own health and, in the case of transmissible diseases, that of the community (*Mockutė v. Lithuania*, app. no. 66490/09, of 27 February 2018; *Z. v. Finland*, App. No. 22009/93, of 25 February 1997; see also *I v. Finland,* app. no. 20511/03, of 17 July 2008; *M.S. v. Sweden,* app. No. 74/1996/693/885, of 27 August 1997; *Avilkina and Others v. Russia*, no. 1585/09, 6 June 2013). Possible conflicts between the protection of health data and other interests emerge in assessing the "necessity in a democratic society" of existing interference with the right to private life where the Court applied the principle of proportionality (*Z. v. Finland*, App. No. 22009/93, of 25 February 1997; *Avilkina and Others v. Russia,* no. 1585/09, 6 June 2013; *M.S. v. Sweden,* app. No. 74/1996/693/885, of 27 August 1997).

Furthermore, **with regard to remedies**, the possibility of claiming compensation in cases of unlawful disclosure of personal data was considered by the ECtHR as insufficient for ensuring the respect of Art. 8 ECHR, as practical and effective protection should be provided to exclude any possibility of unauthorized access occurring in the first place (*I v. Finland,* app. no. 20511/03, of 17 July 2008).