ISSN 2281-5147

Opinio Juris in Comparatione

Studies in Comparative and National Law

Online First

A proactive GDPR-compliant solution for fostering medical scientific research as a secondary use of personal health data

Giorgia Bincoletto-Paolo Guarda

Pacini Giuridica

Online First ISSN 2281-5147

A proactive GDPR-compliant solution for fostering medical scientific research as a secondary use of personal health data

Giorgia Bincoletto and Paolo Guarda*

Abstract

The secondary processing of personal health data for scientific research in the medical field is fundamental for fostering innovation and growing knowledge that improves individual and public health. Personal health data that are primarily processed for healthcare purposes by healthcare providers may be secondarily used by researchers for scientific purposes. However, the data controller shall assess the applicable grounds and conditions and then comply with the data protection framework to safeguard fundamental rights and freedoms. In this paper we analyse the legal requirements laid down on these aspects by the General Data Protection Regulation at the European Union level, which harmonises the general rules, and by two national implementations at the Member State level, Italy and France, which further regulate with specific conditions. After this comparative investigation, we propose a proactive, legal-technical e-health solution that complies with the rules and principles of the legal frameworks and empowers the individual's control over personal health data while promoting medical research. To this end, the data protection by design concept plays a central role, and an interdisciplinary approach is fundamental in combining legal and technical perspectives.

---

* Paolo Guarda, Assistant Professor of Comparative Private Law at the Faculty of Law - University of Trento, paolo.guarda@unitn.it, authored paragraphs 2 and 3.

Giorgia Bincoletto, Ph.D., Post-Doc Research Fellow at the Faculty of Law - University of Trento, giorgia.bincoletto@unitn.it, authored paragraphs 4 and 5. They co-authored paragraphs 1 and 6. All links to websites were confirmed as of 24 September 2021. We gratefully acknowledge our debt to the "eHealth" Research Units within Fondazione Bruno Kessler, to the Competence Center on Digital Health "TrentinoSalute4.0" and "Laboratorio congiunto con la Facoltà di Giurisprudenza – Università di Trento" for the support received for our research. We would like to thank Lorenzo Gios for his valuable contributions and feedback. All errors remain our own.

Online First ISSN 2281-5147

Table of Contents

Keywords

Health Data - Scientific Research - Personal Data - GDPR - Data protection by design

1. Introduction

Scientific research represents an unavoidable prerequisite to ensure the development of knowledge in multiple fields. It is rooted at a constitutional level that justifies the relevance of the interests it supports, also in a perspective of balance with other rights and principles recognised and protected by legal systems[1]. Whilst science is conducted for the benefit of mankind, individuals' and public interests coexist in modern societies.

Scientific research is indispensable for the progress of the healthcare sector[2]. Medical research responds both to the need to achieve a high level of health protection and provision of care and to the opportunity to foster innovation and grow knowledge. Research studies can be prospective or retrospective and require data. Frequently, these projects use personal data. In the health sector the relationship between individual and collective interests is emphasized: the processing of data relating to the patient's health

[1] The Charter of Fundamental Rights of the European Union specifies that scientific research shall be free of constraints (Art. 13). In the Italian Constitution, for instance, Article 33 establishes the principle of freedom of science, and Article 9 proactively obliges the Republic to promote "the development of culture and scientific and technical research".

[2] According to the World Health Organisation (WHO), high-quality health research is indispensable for many reasons, including resolving global threats, developing vaccines and medicines, and generally for the attainment of the highest level of health. *See* the information provided at *https://www.who.int/health-topics/research/#tab=tab_2*.

status becomes, indeed, useful to the natural person in order to take care of the disease that afflicts her, but at the same time, it is also essential in contributing to scientific progress, meaning developing and evaluating strategies, services, solutions and policies.

The right to health of the individual, the right to protection of personal data concerning health, public health and the underlying public interests are all protected by modern legal frameworks[3]. This scenario is certainly characterized by a high level of complexity, and it is necessary to achieve a correct balance of the rights involved[4]. The obvious benefit in terms of individual care must, in fact, be balanced with the more general need to protect and enhance public health. Some criteria aimed at determining the correct point of contact between these needs should be identified.

From an ethical point of view, the processing of information in the health sector may be configured as a real right and duty of the individual to make the data relating to her health available to healthcare providers, including researchers[5]. The advantage will not only be for the natural person, who will benefit from health services provided in the light of an information framework as complete and advanced as possible, but for the entire community who will benefit from increased opportunities in terms of public (health) safety and scientific progress[6]. At the same time, privacy and confidentiality of research subjects

[3] At the EU level, the right to health, meaning the right of access to preventive healthcare and the right to benefit from medical treatment, is provided by Article 25 of the Charter of Fundamental Rights of the European Union. The definition of "public health" is established by Article 3 of Regulation (EC) No 1338/2008.

[4] *See* F. Di Ciommo, 'Il trattamento dei dati sanitari tra interessi individuali e collettivi' (2002) 2 *Danno e Resp.*, pp. 121-134. On balancing rights at the constitutional level *see ex multis* A. von Bogdandy and B. Jürgen, *Principles of European Constitutional law* (Hart Publishing, 2020); R. Alexy, *A theory of constitutional rights* (Oxford University Press, 2010).

[5] *See* M. Mostert *et al.*, 'From Privacy to Data Protection in the EU: Implications for Big Data Health Research' (2017) 25 *European Journal of Health Law* 1, p. 44, which refers to an "*ethical and scientific imperative*" of the individual to share personal data to be used for research activities; *see* also I.G. Cohen, 'Is There a Duty to Share Healthcare Data?' in I. Glenn Cohen and others (eds.), *Big Data, Health Law, and Bioethics* (Cambridge University Press, 2018). In the Communication on the European Data Strategy of 2020, the European Commission uses the term "data altruism", meaning the possibility of making "*easier for individuals to allow the use of the data they generate for the public good, if they wish to do so*". *See* European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data", 2020, p. 13. This approach of "data altruism" is even contained in the Proposal for a Regulation of the European Parliament of the Council on European data governance, COM/2020/767 final, which will improve the European Health Data Space.

[6] For further details with reference to scientific research and personal data protection issues, *see* R. Ducato, 'Data protection, scientific research and the role of information' (2020) 37 Computer Law and Security Review, available at *https://www.sciencedirect.com/science/article/pii/S0267364920300170*; D. Amram, 'Building

Online First ISSN 2281-5147

should always be guaranteed[7], as provided by the Helsinki Declaration[8] and the Oviedo Convention[9].

From a legal point of view, the processing of personal data for research is bound by European Union (EU) and national data protection requirements. Actually, many rules have been introduced to safeguard natural persons with regard to the processing of their health data. The data protection field provides conditions that limit the processing of information for scientific purposes and determine the lawful point of contact between the interests mentioned[10]. In fact, the perspective of availability of patients' data for scientific research is counterbalanced by obligations upon those who provide healthcare professionally and are also interested in medical scientific research activities. Healthcare providers should process the data that are necessary to provide the healthcare service to the individual and useful for managing high-quality health systems. Suitable measures and guarantees should be adopted to protect personal health data. In this context, where data are first collected for healthcare provision (primary purpose is healthcare), it is often not easy to identify later the grounds and conditions for lawfully processing personal data stored in Electronic Health Record systems (EHRs) or in other repositories for scientific purposes (re-use of data for the secondary research purpose)[11].

---

up the "Accountable Ulysses" model. The impact of GDPR and national implementations, ethics, and health-data research: Comparative remarks' (2020) 37 Computer Law & Security Review, available at *https://www.sciencedirect.com/science/article/pii/S0267364920300182*.

[7] In this sense following codes of conduct and best practices is very helpful. A Code of Conduct for health research is currently under development in the EU framework by BBMRI-ERIC, a European research infrastructure for biobanking, which is taking into account pivotal issues like consent of data subjects. *See* updated information on this initiative at *http://code-of-conduct-for-health-research.eu/*.

[8] According to Article 24 of the WMA Declaration of Helsinki - Ethical Principles for Medical Research, "every precaution must be taken to protect the privacy of research subjects and the confidentiality of their personal information".

[9] The Convention for the protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine (Convention on Human Rights and Biomedicine) includes Article 10 on "private life and right to information".

[10] According to the Council of Europe, "scientific research purpose" refers to a processing that is aimed "at providing researchers with information contributing to an understanding of phenomena in varied scientific fields (epidemiology, psychology, economics, sociology, linguistics, political science, criminology, etc.) with a view to establishing permanent principles, laws of behaviour or patterns of causality which transcend all the individuals to whom they apply". *See* Council of Europe, "Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", 2018, p. 9.

[11] The extensive and recent report TIPIK Legal, "Report on the implementation of specific provisions of Regulation (EU) 2016/679", European Commission, 2021, p. 70, in the section on "secondary use of health data for scientific or historical research" states: "*The literature shows that identifying the correct legal bases for use in*

Online First ISSN 2281-5147

This article focuses on issues relating to the determination of the legal basis and conditions that enable the secondary processing of personal health data for scientific purposes in the medical field under the EU law on data protection. A correct interpretation of the legal ground is crucial to set up the research since it impacts on the applicable rights of the data subjects and other conditions under which the researchers should work[12]. The analysis does not examine the processing situation where personal data are directly collected for research purposes, but rather its focus is on further processing of these data for medical research. Although the General Data Protection Regulation has harmonised the rules governing data processing, it has left room for further regulation on personal health data at the Member State level.

After a comparative law approach that highlights the differences between two Member States' legislation implementing the EU Regulation - Italy and France - the research proposes a proactive e-health solution that complies with the rules and principles of the General Data Protection Regulation and empowers the individual's control over personal health data while promoting medical research. So, the research uses both legal comparison and the interdisciplinary method of "law and technology".

The paper is organised as follows. After this introduction, the second paragraph will be dedicated to a brief overview of the general data protection framework that governs scientific research activity at the European level with particular attention to health data. Then the third and fourth paragraphs will analyse two national implementations of the EU data protection rules relating to research in the medical field: the Italian and the French legal systems. The fifth paragraph will be aimed at providing the conceptual foundations of a cardinal principle of the new European order, "data protection by design", that will be applied to a specific operating scenario in order to propose a proactive legal-technical solution based on an interdisciplinary approach. In the conclusive remarks we will try to summarise the juridical-conceptual approaches to the issue and propose possible future evolutions.

---

the context of research is in practice difficult. A major source of uncertainty for industry is the appropriate legal basis for processing data in the absence of explicit consent, and understanding what activities reasonably fall under the various exemptions provided by the GDPR. (...) It has also been highlighted that there is uncertainty to which extent existing national laws apply. (...) It is also worth keeping in mind some processing activities may fall under different legal bases simultaneously – particularly if an extremely narrow scope is assigned to each basis".

[12] The same remark is stressed by G. Schneider and G. Comandé, 'Differential Data Protection Regimes in Data-Driven Research: Why the GDPR Is More Research-Friendly Than You Think' (2021) *German law Journal* 2021, available at SSRN: *https://ssrn.com/abstract=3897258*, pp. 9-10.

Online First ISSN 2281-5147

2. Scientific research and personal health data in the EU framework: selected issues

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, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter: "GDPR")[13] confirms European legislators' preference for processing for research purposes, whether "secondary" or carried out for a primary purpose, following the approach of the former Directive 95/46/EC[14]. A special and privileged regime on data processing related to research activities has been provided in the GDPR.

Starting from the definition of the material scope, scientific research is very broadly defined. Recital 159 lists some examples such as: "*technological development and demonstration, fundamental research, applied research and privately funded research* [...]. *Scientific research purposes should also include studies conducted in the public interest in the area of public health*"; furthermore, "*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*". Hence, research can be promoted for both individual and public interests.

To enhance scientific research, the GDPR provides an exception to the cornerstone purpose limitation principle. Article 5, par. 1, letter b), states: "*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')*"[15]. A scientific research purpose is *a priori* considered compatible.

---

[13] On the GDPR *see ex multis* C. Kuner et al, *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020); B. Van der Sloot, *The General Data Protection Regulation in Plain Language* (Amsterdam University Press, 2020); V. Cuffaro, R. D'Orazio, and V. Ricciuto, *I dati personali nel diritto europeo* (G. Giappichelli Editore, 2019); P. Voigt and A. Von dem Bussche, *The EU General Data Protection Regulation (GDPR). A Practical Guide* (Springer International Publishing, 2017); G. Finocchiaro, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali* (Zanichelli, 2017).

[14] *See* G. Chassang, 'The impact of the EU general data protection regulation on scientific research' (2017) 11 Ecancermedicalscience, p. 709, available at *https://www.ncbi. nlm.nih.gov/pmc/Articles/PMC5243137/*); M.L. Manis, 'The processing of personal data in the context of scientific research. The new regime under the EU-GDPR' (2017) 3 BioLaw Journal, pp. 325-354.

[15] *See* C. De Terwangne, 'Chapter II Principles (Articles 5-11), Article 5. Principle relating to processing of personal data', in Kuner et. al (ed.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020), pp. 309-397. According to the purpose limitation principle, personal data shall be collected for specified, explicit and legitimate purposes. Personal data shall not be processed for incompatible purposes. According to this chapter, the concept of "compatible" is problematic. Some

Moreover, in Article 14, par. 5, letter b), a wide derogation is stated with reference to the informational obligation in the case of indirect collection of personal data; there is a series of options: disproportionate effort, impossibility or serious prejudice for the purpose of research, etc.

Finally, Article 89, the pivotal regulatory provision with reference to scientific research, allows a series of possible exceptions to the rights referred to in Articles 15 ff GDPR[16], on the assumption that adequate guarantees are adopted for to protect the rights and freedoms of the data subject. In this regard, the data controller may comply with the aforementioned obligation, in particular in order to guarantee compliance with the principle of data minimisation, by means of "pseudonymisation" techniques[17]. In addition to technical and organisational measures, research should follow "*recognised ethical standards*" as recommended by Recital 33 GDPR.

Turning now to the particular type of data generally processed in the medical scientific context, we define "data concerning health" those "*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*" (Article 4, pt. 15, GDPR)[18]. They are included in the list of special

criteria are provided by Article 6, par. 4, GDPR, but the data controller should evaluate the extent of the purpose on a case-by-case basis.

[16] *See* further on Article 89 GDPR, G. Comandé, 'Ricerca in sanità e data protection un puzzle... risolvibile' (2019) 1 Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario), pp. 189–207. On the implementation of Article 89 in Member States' legislation *see* TIPIK Legal, "Report on the implementation of specific provisions of Regulation (EU) 2016/679", *op. cit.*, pp. 29–39; DG Health and Food Security, "Assessment of the EU Member States' rules on health data in the light of the GDPR", European Commission, 2021, pp. 60-81.

[17] Article 4, no. 5, GDPR: "'*pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person*". *See* further on pseudonymisation ENISA, European Union Agency for Network & Information Security, 'Recommendations on shaping technology according to GDPR provision. An overview on data pseudonymisation', 2018; L. Tosoni, 'Chapter I General principles (Articles 1-4). Article 4(5). Pseudonymisation', in Kuner et. al (ed.), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press, 2020).

[18] *See* Lee A. Bygrave and L. Tosoni, 'Chapter I General principles (Articles 1-4). Article 4(15). Data concerning health', in Kuner et. al (ed.), *The EU General Data Protection Regulation (GDPR): A Commentary*. cit., pp. 215–224; T. Mulder, 'The Protection of Data Concerning Health in Europe' (2019) 5 Eur. Data Prot. L. Rev., pp. 209–220; M. Granieri, 'Il trattamento di categorie particolari di dati personali nel reg. UE 2016/679' (2017) 1 Nuove leggi civ. comm., 165-190; P. Guarda, 'I dati sanitari', in Cuffaro et al (ed.), *I dati personali nel diritto europeo* (G. Giappichelli Editore, 2019), pp. 591-626; G. Schneider, 'Disentangling Health Data Networks: a Critical Analysis of Art. 9.2 and Art. 89 GDPR' (2019) 9 International Data Privacy Law 4, pp. 253-271. An interesting in-depth analysis on "quasi-health data" defined as "*information that indirectly reveals data about health status*" in G. Malgieri and G. Comandè, 'Sensitive-by-distance: quasi-health data in the

categories of personal data referred to in Article 9 GDPR and, therefore, subject to the general prohibition of processing sanctioned in the first paragraph[19]. There are, however, some exceptions to this prohibition, which can be divided into three groups[20]: 1) the consent[21] of the data subject pursuant to Article 9, par. 2, letter a) and, closely related to it, the need to protect a vital interest of the data subject (letter c)), as well as the manifest publicity of personal data (letter e)); 2) processing needed for reasons of substantial public interest (letter g)), for the purposes of preventive or occupational medicine, medical diagnosis, provision of health or social care or treatment or management of health or social care and systems and services referred to in letter h) (hereinafter: "healthcare exception"), and for reasons of public interest in the field of public health pursuant to letter i); 3) the processing necessary for scientific or historical research purposes or for statistical purposes pursuant to Article 9, par. 2, letter j) (hereinafter: "research exception").

This discipline is complementary to the general requirements for lawful data processing pursuant to Article 6 GDPR (consent, pursuant to par. 1, letter a); execution of a task of public interest, pursuant to par. 1, letter e); legitimate interest, pursuant to paragraph 1, letter f)). The existence of a law of a general nature, then, becomes the prerequisite for processing particular categories of data.

---

algorithmic era, in Information & Communications Technology Law' (2017) 26 Information & Communications Technology Law 3, pp. 229–249.

[19] For further details on special categories of data, *see* L. Georgieva and C. Kuner, 'Art.9 Processing of special categories of personal data', in Kuner et al. (ed.), *The EU General Data Protection Regulation (GDPR). A Commentary*, cit., pp. 365-384.

[20] *See* G. Schneider, 'Health Data Pools under European Policy and Data Protection Law: Research as a New Efficiency Defence' (2020) 11 JIPITEC, p. 61. *See* further G. Schneider and G. Comandé, 'Differential Data Protection Regimes in Data-Driven Research: Why the GDPR Is More Research-Friendly Than You Think', cit., pp. 11-18.

[21] Consent has been defined as a "freely given, specific, informed and unambiguous indication" of the will of the data subject. See Article 2, par. 11, GDPR. Recital 33 specifies that "*It is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose*". It can then be argued that a flexibility in defining the purpose of the scientific study can be found in the words of the GDPR. On this matter see also EDPB, "Guidelines 5/2020 on consent under Regulation 2016/679", 2020, available at *https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf*. The Authority highlights that in the case of processing of a particular category of data, this flexibility should be subject to a stricter interpretation than in other cases. Then, a data processing with medical research purposes that processes personal health data the purpose of research should be narrowed down as much as possible.

Some critical profiles of "failed harmonisation" may emerge from the provisions of Article 9, par. 4, GDPR which allows Member States to decide whether or not to maintain the legal bases provided by the EU regulation or introduce additional conditions and limitations, with regard to the processing of particularly sensitive data, such as biometric, genetic, or health-related data[22]. Derogations and different national regimes may create barriers to research activities.

Lastly, the "Preliminary opinion on data protection and scientific research", adopted on 6 January 2020 by the European Data Protection Board[23] and the "EDPB Document on response to the request from the European Commission for clarification on the consistent application of the GDPR, focusing on health research", of 2 February 2021[24] complete the main regulatory framework. In the first document the EDPB reviews the ethical standards applicable to scientific research and analyses selected issues of the data protection framework. The right to information and the nature of informed consent play pivotal roles. The authority specifies that the presumption of compatibility requires a careful analysis by the controller, and it even requires the implementation of the safeguards of Article 89, such as a DPIA[25]. In fact, purpose specification (and compatibility) is a different requirement from the lawfulness of the data processing. The second recent document highlights the existence of legal grounds other than the explicit consent of the data subjects since this basis may be inappropriate in research studies where there is an imbalance of power between the controller and the individuals. Moreover, the EDPB clarifies that when personal health data are collected for a primary purpose based on the "healthcare exception", and the controller relies on the presumption of compatibility for a secondary

---

[22] According to Article 168(7) of the Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, actually, Member States have competence on the protection and improvement of human health, while the EU on carrying out actions to support, coordinate or supplement national actions. On this competence *see* G. Di Federico and S. Negri, *Unione Europea e Salute. Principi, azioni, diritti e sicurezza* (Cedam, Wolters Kluwer 2020); M. Flear, *Governing Public Health: EU Law, Regulation and Biopolitics* (Bloomsbury Publishing, 2015); T. K. Hervey and J. V. McHale, *European Union health law* (Cambridge University Press 2015); S.L. Greer *et al*, 'Everything you always wanted to know about European Union health policies but were afraid to ask', World Health Organization, Regional Office for Europe, 2014.

[23] The opinion is available at *https://edps.europa.eu/data-protection/our-work/publications/opinions/preliminary-opinion-data-protection-and-scientific_en*.

[24] Available at *https://edpb.europa.eu/sites/default/files/files/file1/edpb_replyec_questionnaireresearch_final.pdf*. This document promises the publication in 2021 of specific "Guidelines on processing personal data for scientific research purposes" by the EDPB.

[25] *See* EDPB, "Preliminary Opinion on data protection and scientific research", p. 22, and p. 24 on examples of safeguards.

scientific research purpose, the conditions and safeguards of Article 9 still apply, meaning an exception based on EU or Member State law must be found.

EU law does not define the safeguards under Article 9, par. 2, letter j), meaning different conditions may be established by Member States' law for scientific research in the medical field according to this provision and to Articles 9, par. 4, and 89 GDPR[26]. The EDPB reported that Member States' laws "*generally require prior informed consent from the participant in a research project for the processing of health data*" unless exceptional situations apply[27]. It should be stressed here that this consent is different from informed consent as a human participant in a scientific research study, which is also an ethical requirement.

In the following paragraphs, we will describe two examples of national implementation of the EU regulation, taking into account the Italian and the French legal systems that introduced specific rules on scientific research pursuant to the necessary adjustments to the GDPR and the possibility of derogation. A brief comparison between the two different approaches is provided at the end of section 4 that also highlights some criticalities and gaps left open by the EU and the two Member States' frameworks.

3. The Italian implementation

Within the Italian legal system, a framework dedicated to the processing of personal data for research purposes had already been provided in Title VII "Processing for historical, statistical and scientific purposes" of the former d.lgs. 30 June 2003, no. 196 "Personal Data Protection Code" (hereinafter: "IDPC"): in particular, on scientific research, Chapter III, Articles 104-110. The legislative decree 10 August 2018, no. 101[28] - the National

[26] On Member States' law *see* TIPIK Legal, "Report on the implementation of specific provisions of Regulation (EU) 2016/679", *op. cit.*, pp. 7–15; DG Health and Food Security, "Assessment of the EU Member States' rules on health data in the light of the GDPR", *op. cit.*, pp. 57–81.

[27] *See* EDPB, "Preliminary Opinion on data protection and scientific research", p. 14. Informed consent is the legal basis for clinical trials according to Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, OJ L 158, 27.5.2014. In particular, *see* Articles 28. On the interplay between this Regulation and the GDPR *see* 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)", European Commission, 2019.

[28] Legislative Decree No. 101 of 10 August 2018 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".

adaptation of the IDPC to the GDPR - has substantially preserved the previous provisions, but it has changed some terminology, regulatory references, and added an ethical requirement.

Article 110 IDPC represents here the pivotal provision with regard to research in the medical, biomedical and epidemiological fields. As mentioned, it mainly remained unchanged, but Italian legislators added some targeted adjustments to the GDPR (Articles 9 and 89 upfront) by highlighting the importance of the Data Protection Impact Assessment (DPIA) as regulated by Articles 35 and 36 GDPR. Research in the medical field is to be considered a *species* of the broader *genus* of scientific research. It could be declined in terms of "biomedical research" and "epidemiological research". On the one hand, the first category of research refers to an interdisciplinary approach that applies the principles of biology and natural sciences to clinical practice; on the other hand, the second one is the science that studies the phenomenon of the onset of diseases in the population, with particular regard to the study of the conditions and factors that determine them.

Before analysing the conditions of Article 110 IDPC, it is necessary to take into account the guidelines and requirements of the Italian Data Protection Authority (Italian DPA) specifically issued for scientific research. The Italian DPA, by means of the "Provisions identifying the requirements contained in the General Authorizations nos. 1/2016, 3/2016, 6/2016, 8/2016 and 9/2016 which are compatible with the GDPR and Legislative Decree no. 101/2018" specified the requirements contained in the general authorizations for data processing adopted in 2016 that are still compatible with the new European regulation and with the recent reform of the IDPC. In particular, Annex 1 of these Provisions at point 5 provides "Requirements relating to the processing of personal data carried out for scientific research purposes (hereinafter: "Scientific research requirements"), which concern processing performed by: a) universities, other research bodies or institutes and scientific societies, as well as researchers working in the field of those universities, organizations, research institutes and the members of those scientific societies; b) health professionals and health organizations; c) natural or legal persons, entities, associations and private bodies, as well as subjects specifically responsible for processing such as designated data processors (researchers, monitors, expert commissions, contract research organizations, analysis laboratories, etc.) (Art. 2-quaterdecies IDPC, and 28 GDPR) (point 5.1). These requirements concern the processing of personal data for medical, biomedical and epidemiological research purposes carried out when: the processing is necessary for studies conducted with data previously collected for healthcare purposes, meaning under the "healthcare exception"; the processing is necessary for the execution of previous research

projects or obtained from biological samples previously taken for health protection purposes or for the execution of previous research projects; and, the processing is necessary for studies conducted with data referring to people who, due to the seriousness of their clinical state, are unable to understand the information provided in the privacy policy and therefore validly given consent is not possible (point 5.2). Furthermore, Annex 1 Point 4 provides "Requirements relating to the processing of genetic data"[29].

Beyond the Scientific research requirements, it is also necessary to take into account the "Deontological regulation for processing for statistical or scientific research purposes published pursuant to Art. 20, paragraph 4, of legislative decree 10 August 2018, no. 101 - 19 December 2018" (hereinafter "Deontological Regulation") where the research activity does not concern "*processing for statistical and scientific purposes connected with health protection activities carried out by health professionals or health organizations, or with comparable activities in terms of significant personalized impact on the interested party, which remain governed by the relevant provisions*" (Art. 2, par. 2)[30].

So, taking into account the combination of all the requirements provided for scientific research activity in the medical field, it can be argued that consent represents a basic condition for data processing. In this sense, the Scientific Research Requirements in point 5.3, paragraph 2, ("Consent") establish that "*The obligation to collect consent to the processing of data of data subjects included in the research remains in all cases in which, during the study, it is possible to provide them with adequate information and, in particular, where they go to the treatment center, also for check-ups*". The same principle can be deduced by reading Articles 7, par. 2, and 8, par. 4, if applicable, of the Deontological Rules. Hence, the data controller should provide adequate information and collect consent of the data subjects involved in the scientific projects.

---

[29] For further details with reference to genetic data and scientific research, *see* K. Pormeister, 'Genetic data and the research exemption: is the GDPR going too far' (2017) 7 IDPL, pp. 137-146; P. Quinn and L. Quinn, 'Big genetic data and its big data protection challenges' (2018) 34 Computer Law & Security Review, pp. 1000-1018; M. Shabani and P. Borry, 'Rules for processing genetic data for research purposes in view of the new EU General Data Protection Regulation' (2018) 26 European Journal of Human Genetics, pp. 149-156; J. Kaye *et al.*, 'Dynamic consent: a patient interface for twenty-first century research networks' (2015) 23 European Journal of Human Genetics 2, pp. 141-146; J. H. Gerards, 'General Issues concerning Genetic Information', in Gerards *et al* (ed.), *Genetic Discrimination and Genetic Privacy in a Comparative Perspective* (Oxford University Press, 2005), p. 5.

[30] Art. 8 of the Deontological Regulation is dedicated to medical, biomedical and epidemiological research and states that research activity is carried out "*in compliance with the relevant international and community guidelines and provisions, such as the Convention on human rights and biomedicine of 4 April 1997, ratified by law 28 March 2001, no. 145, the Recommendation of the Council of Europe R (97) 5 adopted on February 13, 1997 on the protection of health data and the Declaration of Helsinki of the World Medical Association on principles for research involving human subjects*".

However, the first paragraph of Article 110, starting from the assumption that such a condition is required, defines some cases and situations in which consent is not necessary.

First of all, consent is not needed for data processing with scientific research purposes in the medical, biomedical and epidemiological fields that is carried out on the basis of a legal or regulatory provision at the national level, or at the European Union level under Article 9, par. 2, letter j) GDPR. Then Article 110 expressly mentions, as a paradigmatic example, the research that is part of a program pursuant to Article 12-bis of Legislative Decree no. 502/1992 ("Reorganization of the health legislation, pursuant to Article 1 of Law no. 421 of 23 October 1992")[31]. This provision, first of all, governs the "National Health Plan" (paragraph 2), which is envisaged with reference to the needs of the National Health Service and takes into account the objectives set out in the National Research Program. This Plan is regularly put in place by the Ministry of Health, after consulting the National Commission for Health Research, in agreement with the Permanent Conference for relations between the State, the Regions and the autonomous Provinces of Trento and Bolzano (paragraph 3). The Program aims to identify the objectives that are national priorities to improve the state of health of the person (paragraph 4) and it also promotes experimentation and methods of operation, management and organization of healthcare services, as well as clinical practices and assistance. Under the plan, the research activity can be classified as a "current" research or a "finalized" research (paragraphs 5 and 6). The current research is implemented through the institutional projects of research organisations within the guidelines of the national program, as approved by the Ministry of Health; the finalized research, instead, contributes to addressing the biomedical and health objectives of the National Health Plan.

Preliminary to a data processing with a research purpose under this first exception is that a DPIA is drafted and made public pursuant to Articles 35 and 36 GDPR. Therefore, this processing situation only requires a compliant risk assessment. Only if the condition of Article 36, par. 1, GDPR applies, meaning the processing would result in a high risk in the absence of mitigating measures, the data controller shall consult the DPA.

The other case of exemption enshrined in the second part of the first paragraph of Article 110 IDPC applies to data processing with a research purpose where "*for particular reasons, informing the data subjects is impossible or involves a disproportionate effort, or risks making it*

[31] *See* G. Raimondi, 'Ricerca medica, biomedica ed epidemiologica. Commento all'Art. 110', in Aa.Vv., *Codice della Privacy. Commento al Decreto Legislativo 30 giugno 2003, n. 196 aggiornato con le più recenti modifiche legislative*, Tomo I (Giuffrè, 2004), p. 1416.

impossible or seriously jeopardizing the achievement of the purposes of the research". In addition to this provision, point 5.3 of the Scientific Research Requirements specifies that in such a processing activity the data controller shall document the existence of the particular reasons mentioned in Article 110 directly in the research project (in line with the general principle of accountability). Hence, this subject shall define a reason, considered wholly particular or exceptional, for which informing the data subjects is impossible or involves a disproportionate effort, or risks making it impossible or seriously jeopardizing the achievement of the research objectives. If it applies, the information (and consent) can be avoided. In particular, the following options have been identified by the Italian DPA:

A. "ethical reasons", linked to the fact that the data subject ignores her condition. This situation applies when the information on data processing may involve the disclosure of information concerning the conduct of the study whose knowledge may cause material or psychological damage to the data subject herself[32];

B. "organisational impossibility reasons", where the failure to consider the data referring to the estimated number of data subjects, who cannot be contacted to be informed, compared to the total number of subjects intended to be involved in the research, would produce significant consequences for the terms of alteration of the relative results[33];

C. "health reasons", attributable to the seriousness of the clinical state in which the data subject is, due to which she is unable to understand the information provided in the privacy policy and provide valid consent. In addition, the study should aim to improve the same clinical state of the data subject, and the controller should provide proof of the impossibility of achieving the scientific purpose through a processing of data referring to persons who are able to understand the information and provide valid consent or by the use of other research methodologies.

---

[32] See for example epidemiological studies on the distribution of a factor that predicts or can predict the development of a morbid state for which there is no treatment.

[33] In this regard, it is necessary to consider in particular the inclusion criteria provided by the study, the enrolment methods, the statistical number of the chosen sample, as well as the period of time elapsed from the moment in which the data referring to the interested parties were originally collected (see for example the cases in which the study concerns individuals with pathologies with a high incidence of mortality or in the terminal phase of the disease or in old age and in serious health conditions); finally, in this context it is also necessary to include the processing of the data of those who are deceased or not contactable at the time of enrolment in the study, after every reasonable effort has been made to contact them, including by verifying whether they are alive, consulting the data reported in the clinical documentation, contacting any telephone numbers provided, as well as acquiring contact data at the registry office of the assisted persons or of the resident population.

Online First ISSN 2281-5147

As regards this second exception, a prerequisite for data processing with a research purpose is drafting a detailed research program with a sufficiently explicit research purpose and obtaining a reasoned favourable opinion from the competent ethics committee at the local level. Moreover, a DPIA must be drawn up, which must necessarily be submitted for consultation to the Italian DPA pursuant to Article 36 GDPR[34]. Here, the data controller shall consult irrespective of the risks involved and the measures implemented. This requirement does not define the request for consultation as a "request for authorisation". Therefore, the consequences of the silence of the Italian DPA on a specific request are open to interpretation. It might be argued that this silence may not interrupt the beginning of a lawful data processing since the provision should have made explicit the need for prior authorisation as established by Article 110-bis IDPC.

Whether the first or second exception applies, Article 110, par. 2, IDPC provides some exceptions to the application of the right of rectification under Article 16 GDPR, in light of the requirements (and possibility of derogations) of Article 89, par. 2 GDPR. If the data subject exercises the right to obtain without undue delay the rectification of inaccurate personal data or the right to have incomplete personal data completed, the activity of rectification and integration must be carried out without modifying the data by annotating a statement as long as the result of these operations does not produce significant effects on the research results[35].

For the sake of completeness, it is worth noting that Article 110-bis IDPC establishes that the Italian DPA may authorize further processing of personal data, including those of the special processing referred to in Article 9 of GDPR, for scientific research or statistical purposes by third parties. These third parties mainly carry out these activities when, for particular reasons, informing the interested parties is impossible or involves a disproportionate effort or risks, making impossible or seriously jeopardizing the achievement of the purposes of the research, provided that appropriate measures are taken to protect the rights, freedoms and legitimate interests of the data subject, in accordance

[34] The framework confirms the provisions at the European level regarding clinical trials of medicines for human use (*see* EU Regulation no. 536/2014) and the indications of the National Bioethics Committee (*see* National Bioethics Committee, pediatric biobanks 11 April 2014, 12). For further details, *see* C. Casonato and M. Tomasi, 'Diritti e ricerca biomedica: una proposta verso nuove conoscenze' (2019) 1 BioLaw Journal – Rivista di BioDiritto, pp. 343-358.

[35] The Deontological Regulations take up this provision and Art. 12 ("Exercise of data subject rights) provides that: "*If, in the event of the exercise of the rights referred to in Art. 15 and ff. of the Regulations, changes are necessary to the data concerning the data subject, data controller shall note, in the appropriate spaces or registers, the changes requested by the data subject, without changing the data originally entered in the archive*".

with Article 89 GDPR, including preventive forms of data minimisation and anonymisation.

As a result, such a processing situation is domain-limited since only particular data controllers that mainly carry out research activities can benefit from its application (Art. 110-bis, par. 1, IDPC); furthermore, they do not process personal data for a scientific purpose that is instrumental to healthcare services, meaning they are not private or public institutions of hospitalisation and care (Art. 110-bis, par. 4, IDPC). Specific safeguarding measures and a prior consultation with the Italian DPA are binding. Without an authorisation, which also defines the necessary safeguarding measures, starting the processing is unlawful (Art. 110-bis, par. 2, IDPC). It can be argued that the Italian legislator has implemented Article 16, par. 5, GDPR, which allows Member State law to require controllers to consult in advance in relation to processing. However, according to Article 110-bis, par. 3, IDPC the Italian DPA may issue general authorisations that specify conditions and measures for third parties who mainly carry out research and statistical activities.

Looking at a situation where personal health data are first collected and processed under the "healthcare exception" provision, and the data controller seeks to use these data for a secondary medical research purpose, without anonymising them, meaning carrying out a prospective or retrospective study, it can be argued that the basic condition of explicit consent applies, unless one of the situations of Article 110 IDPC is applicable (regulatory basis or particular proven reasons). In any case, it is highly likely that a DPIA will be required as an *ex ante* tool for compliance.

4. The French implementation

The French legal system provides rules dedicated to the processing of personal data for research purposes in the medical field and conditions and limitations for the data processing of personal health data in Law no. 78-17 of 6 January 1978 on information technology, data files and civil liberties (hereinafter: LIL)[36] and Law no. 2018-493 of 20 June 2018 on the protection of personal data[37], which adapted the national regulation to the GDPR[38].

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

[37] Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

[38] On the French implementation of the GDPR *see* O. Tambou, 'GDPR Implementation Series - France: The French Approach to the GDPR Implementation' (2018) 4 Eur. Data Prot. L. Rev. 1, pp. 88-94.

This framework defines detailed rules for data processing with scientific purposes: it requires the processing to be subject to baseline and standard rules laid down by the French Data Protection Authority, the Commission nationale de l'informatique et des libertés (hereinafter: CNIL)[39].

First of all, Article 4 of the LIL mentions the research exception to the purpose limitation principle, and specifies that a research purpose is not incompatible with the primary purpose as long as the processing is carried out in compliance with the GDPR, and is not used to make decisions with regards to data subjects. So, the compatibility of research is confirmed at the national level following Art. 5, par. 1, letter b) GDPR.

Secondly, Article 8, par. 1, point 2(c) of the LIL specifically refers to Article 9, par. 4, GDPR. Article 8 regulates the tasks and powers of the CNIL. Point 2(c) of this Article establishes that this authority provides and publishes baseline rules and methodologies (recognised as "référentiels" and "méthodologies de référence") to ensure the security of personal data and to govern the processing of biometric, genetic and health data. According to this provision, the CNIL can define additional technical and organisational measures to be applied to the processing of biometric, genetic and health data, unless the processing is carried out by a controller on behalf of the State and acting in the exercise of official public tasks. The CNIL's guidance is therefore highly influential.

As regards derogations to data subjects' rights in light of Article 89, par. 2 GDPR, Articles 49, par. 3, 78 and 79 of the LIL refer to Articles 15, 16, 18 and 21 GDPR: derogations to these rights are possible insofar as such rights are likely to render impossible or seriously impair the achievement of the research purpose. This requirement explicitly follows the GDPR. The data controller should however implement specific safeguards, including restriction of access to personal data and anonymisation before disseminating the data or making them available.

Furthermore, specific rules are dedicated to personal health data in Title II, Chapter III, Section 3. Articles from 64 to 77 of the LIL in fact regard the processing of personal data in the medical field and include requirements on scientific research purposes (Sub-section 2 "special provisions concerning processing for the purposes of research, study or evaluation in the health field"). In more detail, Article 66 states that these provisions apply

[39] On the French approach to clinical research and the protection of personal data *see* e.g. F. Lesaulnier, 'Recherche en santé et protection des données personnelles à l'heure du Règlement général relatif à la protection des données' (2019) 158 Médecine & Droit, pp. 103-111; E. Toulouse, et al. 'French legal approach to clinical research' (2018) 37 Anaesthesia Critical Care & Pain Medicine 6, pp. 607-614.

to processing operations that are carried out in the public interest, such as ensuring high standards of quality and safety of healthcare, medical products and medical devices[40]. Article 66, par. 2, directly mentions the CNIL's "référentiels" by specifying that processing in the medical field can be carried out only if it complies with the reference guidelines of the authority. After the necessary adjustment, the data controller should send a declaration of compliance to the CNIL. Alternatively, the data controller shall obtain a prior authorisation from the same authority (Art. 66, par. 3)[41]. This authorisation may refer to many processing operations having the same purposes, relating to identical categories of personal data and identical recipients (Art. 66, par. 4). Where the CNIL has not given its opinion within two months of the extension time, the application for authorisation shall be deemed to have been accepted, but this requirement does not apply to research purposes (Art. 66, par. 5). Either way, the data controller should involve the CNIL in the data processing. As an example, this provision applies to the "healthcare exception" or to clinical trials.

As regards research purposes in the medical field, Article 73 of the LIL establishes that when the processing complies with a "méthodologie de référence" of the CNIL, it may be carried out without the prior authorisation mentioned in Article 66; however, the data controller shall send a declaration of compliance to the CNIL. The authorisation is instead necessary for data processing that does not comply with any reference methodologies. This binding authorisation is issued by the CNIL within two months (and can be postponed for the same amount of time), after a consultation with one of the two ethical committees: the "Comité éthique et scientifique pour les recherches, les études et les évaluations dans le domaine de la santé" when the research does not involve a human being, or the "Comité compétent de protection des personnes mentionné à l'article L. 1123-6 du Code de la santé publique"[42] when the research involves a human (Article 76). Without authorisation, the processing is unlawful. This framework applies to both data processing carried out for primary research purposes and data processing that has secondary research purposes.

[40] This specification seems to evoke Art. 9, par. 2, lett. i), GDPR.

[41] The procedure is available at *https://declarations.cnil.fr/declarations/declaration/accueil.action;jsessionid=EDD5F30C677D70781F9F4CD2DBF8B0C2*.

[42] The Public Health Code unifies the applicable rules in the healthcare field, including the code of medical ethics.

Thus, in the "référentiels"[43], meaning reference documents on processing activities[44], the CNIL lists the conditions under which processing of health data can be carried out, including a DPIA. In the six "méthodologies de référence" the authority defines reference methodologies, including measures and baseline technical standards, on particular processing situations carried out for research purposes in the medical field. These "méthodologies de référence" are domain-limited, often refer to categories of research projects and give great importance to the DPIA. When a processing falls under the conditions of one of the "méthodologies de référence", the data controller must comply with the baseline rules defined by the CNIL and submit a declaration of compliance[45]. Where applicable, the controller should apply online for prior authorisation ("demande d'autorisation de recherche") on the CNIL website by describing the processing operations and uploading documents[46]. "Méthodologies de référence" address research studies that are aimed at a public interest encompassing both private and publicly funded research[47].

In brief, "Méthodologie de référence" MR-001 is the reference document for data processing that uses health data, has a public interest, involves a human being, and requires the informed consent of a human participant in a scientific research study[48], while MR-003 for data processing has the same initial conditions, but does not require the informed consent of a human participant in a scientific research study and instead concerns non-interventional research and clusters of clinical trials of medicinal products[49]. MR-002 refers

[43] The information is summarised in the article at *https://www.cnil.fr/fr/quelles-formalites-pour-les-traitements-de-donnees-de-sante-caractere-personnel.*

[44] See e.g. CNIL, "Référentiel relatif aux traitements de données à caractère personnel destinés à la gestion des cabinets médicaux et paramédicaux", available at *https://www.cnil.fr/sites/default/files/atoms/files/referentiel_-_cabinet.pdf.*

[45] The procedure is available at *https://declarations.cnil.fr/declarations/declaration/accueil.action.*

[46] The procedure is available at *ibidem.*

[47] Examples of reasons of public interest in the area of public health are included in Art. 9, par. 2, lett. i) GDPR: "*protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products*". The specification on public interest excludes commercial purposes.

[48] Délibération n° 2018-153 du 3 mai 2018 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé avec recueil du consentement de la personne concernée (MR-001) et abrogeant la délibération n° 2016-262 du 21 juillet 2016. MR-001 is available at *https://www.cnil.fr/fr/declaration/mr-001-recherches-dans-le-domaine-de-la-sante-avec-recueil-du-consentement.*

[49] Délibération n° 2018-154 du 3 mai 2018 portant homologation de la méthodologie de référence relative au traitement des données à caractère personnel mis en œuvre dans le cadre des recherches dans le domaine de la santé ne nécessitant pas le recueil du consentement de la personne concernée (MR-003) et abrogeant

Online First ISSN 2281-5147

to non-interventional performance studies conducted on in vitro medical devices (IVDs)[50]. When the research does not involve human beings and refers to studies that re-use personal health data in light of a public interest, MR-004 applies[51]. Finally, MR-005[52] and MR-006[53] concern specific processing situations related to national programs for healthcare institutions, hospital federations and the healthcare industry.

Beyond the involvement and guidance of the CNIL, Article 77 of the LIL introduces an audit committee for the national health data system ("comité d'audit du système national des données de santé"), which defines strategies for making available personal data that are collected in the "système national des données de santé" (SNDS) for research purposes[54]. The SNDS covers almost the entire French population[55]. Thus, personal data are first

---

la délibération n° 2016-263 du 21 juillet 2016. MR-003 is available at *https://www.cnil.fr/fr/declaration/mr-003-recherches-dans-le-domaine-de-la-sante-sans-recueil-du-consentement*.

[50] Délibération n° 2015-256 du 16 juillet 2015 portant homologation d'une méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des études non interventionnelles de performances en matière de dispositifs médicaux de diagnostic in vitro (MR-002). MR-002 is available at *https://www.cnil.fr/fr/declaration/mr-002-etudes-non-interventionnelles-de-performances-concernant-les-dispositifs-medicaux*. As regards medical devices see Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC. OJ L 117, 5.5.2017, and Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU. OJ L 117, 5.5.2017.

[51] Délibération n° 2018-155 du 3 mai 2018 portant homologation de la méthodologie de référence relative aux traitements de données à caractère personnel mis en œuvre dans le cadre des recherches n'impliquant pas la personne humaine, des études et évaluations dans le domaine de la santé (MR-004). MR-004 is available at *https://www.cnil.fr/fr/declaration/mr-004-recherches-nimpliquant-pas-la-personne-humaine-etudes-et-evaluations-dans-le*.

[52] Délibération n° 2018-256 du 7 juin 2018 portant homologation d'une méthodologie de référence relative aux traitements de données nécessitant l'accès par des établissements de santé et des fédérations aux données du PMSI et des résumés de passage aux urgences (RPU) centralisées et mises à disposition sur la plateforme sécurisée de l'ATIH (MR 005). MR-005 is available at *https://www.cnil.fr/fr/declaration/mr-005-etudes-necessitant-lacces-aux-donnees-du-pmsi-etou-des-rpu-par-les-etablissements*.

[53] Délibération n° 2018-257 du 7 juin 2018 portant homologation d'une méthodologie de référence relative aux traitements de données nécessitant l'accès pour le compte des personnes produisant ou commercialisant des produits mentionnés au II de l'article L. 5311-1 du code de la santé publique aux données du PMSI centralisées et mises à disposition par l'ATIH par l'intermédiaire d'une solution sécurisée (MR 006). MR-006 is available at *https://www.cnil.fr/fr/declaration/mr-006-etudes-necessitant-lacces-aux-donnees-du-pmsi-par-les-industriels-de-sante*.

[54] The rules on the SNDS are provided by Articles L. 1461-1 to Article L. 1461-7 of the *Code de la santé publique*.

[55] F. Lesaulnier, 'Recherche en santé et protection des données personnelles à l'heure du Règlement général relatif à la protection des données'.

collected for healthcare purposes in the national ecosystem and then may be accessed for research purposes by internal or external researchers. Law no. 2019-774 of 24 July 2019 on the organisation and transformation of the health system[56], which modified the *Code de la santé publique*, changed the rules on the protection of personal health data by expanding the lawful research purposes by the use of the SNDS.

So, the French Government created the Health Data Hub (Plateforme des données de santé, hereinafter: HDH)[57], which is a public initiative and entity affiliated with the Ministry of Solidarity and Health and with the Ministry of Research[58]. The HDH is also a platform and single-entry point for health data access in the national health data system for research, studies, evaluation and innovation in the medical field[59]. The governance of this platform is composed of 56 entities of health data stakeholders, including the government, public bodies, patients' associations, and health research organisations. All the purposes of the HDH can be summarised as follows[60]:

1. collecting, organising and making available the data of the national health data system and promoting innovation in the use of health data;

2. informing patients, promoting and facilitating their rights, in particular with regard to the right to object, meaning the right to opt-out to the secondary use of their health data according to the framework of Article L. 1461-3 of the *Code de la santé publique*;

3. collaborating with the Scientific and Ethics Committee, which evaluates the research studies and with the CNIL, which develops methodologies for safeguarding data protection and security of health data;

4. carrying out the operations necessary for allowing access to the national health data system when a subject has obtained authorisation;

5. contributing to the dissemination of standards for data exchange, taking into account European and international standards;

---

[56] Loi n° 2019-774 du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé.

[57] Arrêté du 29 novembre 2019 portant approbation d'un avenant à la convention constitutive du groupement d'intérêt public «Institut national des données de santé» portant création du groupement d'intérêt public «Plateforme des données de santé». The CNIL released a preliminary opinion that is available at *https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038142154/*.

[58] *https://www.health-data-hub.fr/*.

[59] Art. L. 1461-1 Code de la santé publique.

[60] Art. L. 1462-1 Code de la santé publique.

6. supporting, even financially, the project leaders and their stakeholders selected in the context of calls for projects.

Researchers, named "data users", can access datasets of health data for research purposes, but these data remain in the original repositories. In the HDH personal data are processed solely in a pseudonymised form. Only researchers carrying out public interest research with a specific and detailed project can access health data. Therefore, the researcher, as a public or private entity, should prove that the study is of public interest[61]. Other prerequisites to this access are the approval of the Scientific and Ethics Committee of the HDH (CESREES) and the authorisation of the CNIL. The details of the data processing and the research project are available on the HDH website in a concise, transparent, intelligible and easily accessible form that uses clear and plain language. This disclosure of information is compliant with the transparency and accountability principles of the GDPR (Article 5, par. 1, lett. a) and par. 2, Article 12. This mode of communication of information is particularly interesting since it combines information on the retrospective or prospective study with information required by Articles 13 and 14 of the GDPR, but it addresses society and not specific data subjects.

Taking into account the combination of all the requirements provided for scientific research activity in the medical field, it is worth pointing out that a legal or regulatory provision at the national level represents the basic ground for data processing in France. Hence, the data controller should provide adequate information to the data subjects and does not need to seek the consent of those involved in the scientific projects. The default basis is the legal provision at the national level in the LIL and the *Code de la santé publique* insofar as the research is aimed at a public interest, and the condition of the request of the consent is the exception. In fact, Article 75 of the LIL requires the informed and explicit consent of the data subject when the research involves genetic information, unless Article L. 1131-1-1 of the *Code de la santé publique* applies[62]. The data controller carrying out data processing with a public research purpose must comply with the CNIL's guidelines. When the research does not have a public interest, the applicable legal ground seems to be Article

[61] The website of the HDH specifies that the public interest of each project is assessed by an independent ethical and scientific committee that includes ethical and legal experts and representatives from patients' associations. *See* the information on this entity at *https://www.health-data-hub.fr/cesrees*.

[62] Art. L1131-1-1 concerns the examination of genetic characteristics of a person. It allows examination when the person has been informed and has not expressed her opposition. This is an "opt-out" approach, which is different from the "opt-in" approach of the LIL.

9, par. 2, lett. j) GDPR and the consent of the data subject is required as a condition for starting the research lawfully.

Both French and Italian legal systems define specific rules for processing personal health data with medical research purposes. Looking at the processing situation where personal health data are first collected and processed under the "healthcare exception" provision, and the data controller seeks to use these data for a secondary medical research purpose, without anonymising them, meaning carrying out a prospective or retrospective study, it can be argued that in France the basic ground is law and it can operate through the central HDH platform; whereas in Italy the typical ground is Article 9, par. 2, j) and the consent of the data subjects is required as an additional safeguard, unless one of the exceptions mentioned above is applicable. In Italy the limitation to research that has a public interest is not included. Therefore, this legal framework does not distinguish between data processing activities that pursue scientific purposes, but involve different interests.

On the one hand, the additional condition of consent required by the two national frameworks is not conceived by the GDPR[63]. It may raise the "traditional problems" of unwitting consent, coerced consent, and incapacitated consent[64], and it may result in complex planning of research projects that involve several centres of different countries and cross-borders transfers of personal health data[65]. The revocability of consent may limit research studies creating uncertainty on what data can be lawfully used in the project phases. Thus, forms of broad consent are promoted by the authorities[66]. On the other hand, the GDPR leaves spaces to Member States to define the safeguards necessary to process personal data for research under Articles 9, par. 2, j) and 89 and the limitations with regard to the processing of data concerning health[67] (health research is, indeed, driven by the Member States national competences on public health).

---

[63] *See* section 2.

[64] *See* G. Schneider and G. Comandé, 'Differential Data Protection Regimes in Data-Driven Research: Why the GDPR Is More Research-Friendly Than You Think', cit., pp 12-15; D. Peloquin *et al.*, 'Disruptive and avoidable: GDPR challenges to secondary research uses of data" '(2020) 28 Eur J Hum Genet 28, pp. 697–705.

[65] A typical example is a research project funded by the Horizon Programmes. *See* at *https://ec.europa.eu/programmes/horizon2020/en/h2020-sections-projects*.

[66] *See* the EDPB, "Preliminary Opinion on data protection and scientific research", cit., and the Proposal for a Regulation of the European Parliament of the Council on European data governance, *supra* note no. 5.

[67] *See* section 2 and also Article 9, par. 4 GDPR.

Online First ISSN 2281-5147

France and Italy adopted different approaches on the conditions for secondary processing of personal health data. The French approach to research in the medical field is centralised since a national public entity (i.e. the HDH) allows the use of personal health data already collected for healthcare purposes. Conversely, in Italy the approach is decentralised. Therefore, research stakeholders should identify the suitable path.

Despite this difference, as in the Italian framework, in France it is highly likely that a DPIA will be required as an *ex ante* instrument of compliance. In addition, both legal frameworks often require data processing to be subject to prior consultation or authorisation from the DPAs. In this sense, the CNIL has a defined online procedure and several reference documents to guide the request for authorisation. This framework also includes the declaration of compliance as a starting condition for the data processing.

Finally, the CNIL and Italian DPA lay down specifications on data concerning health and provide guidance on research purposes in the medical field since both national laws (LIL and IDPC) define specific powers and tasks in this particular domain. French specifications are more detailed and complex, and include ethical bodies that are external to the research organisations, but coordinated at the national level. Instead, where applicable, Italian researchers should obtain the opinion of the ethical committee internal to the organisation they are part of[68].

The next section proposes a proactive approach that is focused on the Italian framework, but can be applied to other frameworks with appropriate adjustments since it follows the requirements of the GDPR and the data protection by design principle. So, it takes into account the rules described in sections 2 and 3. It also uses the transparency approach of the HDH mentioned in section 4: it represents an advanced example of how information on the research study can be provided online to data subjects and citizens by combining characteristics on data processing with details of the scientific project. The proposed legal-technical solution clarifies the legal ground of the data processing, and uses the explicit consent as additional safeguard laid down in Italian framework, trying to avoid the above-mentioned possible criticalities. It involves a mobile application as intermediary that is already used by citizens for healthcare purposes and that fosters an interdisciplinary and privacy by design implementation. The solution is integrated with a virtual coaching system that interacts with the user by sending messages on active research projects to be joined and on all the information related to the data processing activities. By means of this

[68] In fact, Art. 110 IDPC does not institute a central ethical committee like the French CESREES, but it refers to "*the competent ethics committee at the territorial level*".

approach, the secondary use of personal health data may be boosted. The management of the data processing, including its legal grounds and conditions, will be carried out in a way that considers both healthcare providers' and researchers' perspectives.

5. A proactive legal-technical solution: a data protection by design approach

Healthcare provision, medical scientific research and data processing of health data have been deeply affected and revolutionised in the digital age [69]. In the medical field, digitalisation is more than a technical process: on the one hand, it involves Information and Communication Technologies (ICTs) and algorithms, including Artificial Intelligence, and, on the other hand, it leads to a considerable impact on healthcare-related processes, practices, and services at the organisational level[70]. The use of ICTs in health products, services and processes is identified by the concept of *e-health*[71]. E-health solutions refer to

[69] *See ex multis* J. Madir, *Healthtech. Law and Regulation* (Elgar Commercial Law and Practice, 2020); S. Melchionna and F. Cecamore, 'Le nuove frontiere della sanità e della ricerca scientifica', in Panetta (ed.), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato D.lgs. n. 196/2003 (Codice Privacy)* (Giuffrè Francis Lefebvre, 2019), pp. 579-620; D. Sigulem *et. al*, 'The New Medicine: From the Paper Medical Record to the Digitized Human Being', in de Fátima Marin (ed.), *Global Health Informatics* (Elsevier, 2017), pp. 152-167; W. W. Lowrance, *Privacy, confidentiality, and health research*, Vol. 20 (Cambridge University Press. 2012).

[70] *See* further EXPH, Expert Panel on effective ways of investing in Health, "Assessing the impact of digital transformation of health services", Publications Office of the European Union, 2019.

[71] *See* the definition of e-health in the European Commission, "eHealth Action Plan 2012–2020. Innovative healthcare for the 21st century", 2012, p. 3: "*The use of ICT in health products, services and processes combined with organisational change in healthcare systems and new skills, in order to improve health of citizens, efficiency and productivity in healthcare delivery, and the economic and social value of health*".

multiple technologies, such as clinical information systems, electronic health records, personal health records[72], telemedicine systems[73], and mobile applications[74].

The digital processing of health data creates both enormous opportunities and critical challenges. E-health can theoretically improve the efficiency and quality of healthcare provision[75] and can also facilitate scientific research, which can potentially access and share a greater amount of personal health data than before (i.e. Big Data)[76]. At the same time,

---

[72] On these systems *see ex multis* G. Bincoletto, 'Data Protection Issues in Cross-Border Interoperability of Electronic Health Record Systems within the European Union' (2020) 2 Data & Policy 3, pp. 1-11; G. Bincoletto, 'A Data Protection by Design Model for Privacy Management in Electronic Health Records', in: *Privacy Technologies and Policy, 7th Annual Privacy Forum*, Lecture Notes in Computer Science, (Springer International Publishing, 2019), pp. 161-181; G. Comandé, L. Nocco, and V. Peigné, 'An empirical study of healthcare providers and patients' perceptions of electronic health records' (2015) 59 Computers in Biology and Medicine, pp. 194-201; C. George, D. Whitehouse, and P. Duquenoy, *eHealth: legal, ethical and governance challenges* (Springer Science & Business Media, 2012); P. Guarda, *Fascicolo sanitario elettronico e protezione dei dati personali*, Vol. 94 (Quaderni del Dipartimento di Scienze Giuridiche, 2011); C. P. Hartley and E. Douglass Jones, *EHR implementation: A step-by-step guide for the medical practice* (American Medical Association, 2012); N. P. Terry and L. P. Francis, "Ensuring the privacy and confidentiality of electronic health records" (2007) U. Ill. L. Rev., pp. 681-736; E. J. Bieber, F. M. Richards and James M. Walker, *Implementing an electronic health record system* (Springer, 2005).

[73] On telemedicine *see ex multis* C. Botrugno, 'Telemedicine in daily practice: Addressing legal challenges while waiting for an EU regulatory framework' (2018) 7 Health Policy and Technology 2, pp. 131-136; C.L. Wen, 'Telemedicine, eHealth and Remote Care Systems', in de Fátima Marin (ed.), *Global Health Informatics* (Elsevier, 2017), pp. 168-194; P. Guarda, 'Telemedicine and Application Scenarios: Common Privacy and Security Requirements in the European Union Context' (2015) *Trento Law and Technology Research Group Research Paper n. 23*; C. Ionescu-Dima, 'Legal challenges regarding telemedicine services in the European Union', in Carlisle et al. (ed.), *eHealth: Legal, Ethical and Governance Challenges* (Springer, 2013), pp. 107–133.

[74] On mobile health *see ex multis* T. Mulder, 'Health apps, their privacy policies and the GDPR' (2019) 10 European Journal of Law and Technology 1; E. Mantovani *et al.*, 'Towards a Code of Conduct on Privacy for mHealth to Foster Trust Amongst Users of Mobile Health Applications', in Leenes (ed.), *Data Protection and Privacy: (In)visibilities and Infrastructures* (Springer, 2017), pp. 81–106; European Commission, "Green paper on mobile Health", COM(2014) 219 final, 2014.

[75] *See* e.g. W. Ricciardi, 'Assessing the impact of digital transformation of health services: Opinion by the Expert Panel on Effective Ways of Investing in Health (EXPH)' (2019) 29 European Journal of Public Health Supplement 4, ckz185–769; European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society", COM (2018), 233 final, 2018.

[76] On Big Data and the use of artificial intelligence (AI) in the medical field and data protection issues *see ex multis* P. Guarda and L. Petrucci, 'Quando l'intelligenza artificiale parla: assistenti vocali e sanità digitale alla luce del nuovo regolamento generale in materia di protezione dei dati' (2020) 2 BioLaw Journal-Rivista di BioDiritto, pp. 425-446; P. Guarda, '"Ok Google, am I sick?": artificial intelligence, e-health, and data protection regulation' (2019) 15 BioLaw Journal-Rivista di BioDiritto 1, pp. 359–375; R: Pierce, 'Machine learning for diagnosis and treatment: Gymnastics for the GDPR' (2018) 4 Eur. Data Prot. L. Rev., pp. 333-343; A. Ferretti, M. Schneider, and A. Blasimme, 'Machine Learning in Medicine: Opening the New Data

Online First ISSN 2281-5147

security, privacy and data protection represent challenging issues to consider. As mentioned, data processing operations must guarantee the right to data protection of data subjects and then comply with the requirements laid down by the GDPR and by national data protection regulations[77]. It has been shown that the GDPR lays down specific rules on the processing of personal health data and on the processing carried out for scientific research purposes, and that national laws develop the requirements.

Moreover, the GDPR incorporates an ambitious provision and binding obligation for data protection by design (DPbD), which should play a central role when projecting any data processing within an e-health system, especially in the case of secondary processing of health data for medical scientific research. Article 25, par. 1, GDPR states that the data controller shall implement appropriate technical and organisational measures that are designed to achieve data protection principles in an effective manner and to integrate the necessary safeguards into the processing at the time of the determination of the means for processing and at the time of the processing itself[78]. To this end, the data controller can take into account various criteria, namely: the state of the art, the cost of implementation and the nature, scope, context and purposes of processing, and the risks of varying likelihood and severity for rights and freedoms of natural persons posed by every processing operation. The evaluation and assessment of the risks must be preliminary and done very carefully.

Protection Black Box' (2018) 4 Eur. Data Prot. L. Rev., pp. 320-332; A. Stylianou and M. A. Talias, 'Big data in healthcare: a discussion on the big challenges' (2017) 7 Health and Technology 1, pp. 97-107.

[77] Only after the anonymisation of personal data, the activities fall outside the scope of the GDPR. An implicit premise is that the data processing falls under the material and territorial scope of the GDPR (Art. 2 and 3).

[78] On data protection by design *see* L. A. Bygrave, 'Chapter IV Controller and Processor (Articles 24-43). Article 25. Data protection by design and by default', in Kuner et. al (ed.), *The EU General Data Protection Regulation (GDPR): A Commentary*, cit., pp. 571-581; A. E. Waldmam, 'Data Protection by Design? A Critique of Article 25 of the GDPR' (2020) 53 Cornell Int'l L.J., pp. 147-167; I. S. Rubinstein and N. Good, 'The trouble with Article 25 (and how to fix it): the future of data protection by design and default' (2019) International Data Privacy Law, pp. 1–20; European Data Protection Board, 'Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, 2019 available at *https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en*; G. Bincoletto, *La privacy by design* (Aracne Editrice, 2019); European Data Protection Supervisor, 'Opinion 5/2018, Preliminary Opinion on privacy by design', 2018 available at *https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en*; L. Jasmontaite *et al.*, 'Data protection by design and by default: Framing guiding principles into legal obligations in the GDPR' (2018) 4 Eur. Data Prot. L. Rev., pp. 168-189, p. 177; A. Tamó-Larrieux, *Designing for privacy and its legal framework: data protection by design and default for the internet of things*, Law, Governance and Technology Series (Springer, 2018); L. A Bygrave, 'Data protection by design and by default: deciphering the EU's legislative requirements' (2017) 4 Oslo Law Review 2, pp. 105-120.

Online First ISSN 2281-5147

Data controllers should apply DPbD on a case-by-case basis since Article 25 GDPR does not provide a "one-size-fits-all" approach, and instead requires proper management of every aspect and characteristic of data processing activities. However, beyond the complexity and the vagueness of the text of the provision, a concrete implementation of DPbD can be achieved through an interdisciplinary approach. Interdisciplinarity is indeed necessary to simultaneously take into account the state of the art of the technology adopted for the data processing and the related engineering methodologies and approaches, the management of processing activities at the organisational level, and the applicable legal requirements in the data protection framework[79]. Solutions should then combine legal and technical perspectives.

By trying to embrace legal and technical perspectives, as well as research needs, in a unique solution, we have tried to assess the aspects of the national contexts mentioned above. The proactive solution that will be proposed below has been elaborated through an interdisciplinary investigation[80]. The legal-technical solution is applicable in multiple

[79] On the interdisciplinary method *see* G. Pascuzzi, *La creatività del giurista. Tecniche e strategie dell'innovazione giuridica* (Zanichelli, 2013).

[80] The solution was developed in collaboration with the "eHealth" Research Units of the Italian Fondazione Bruno Kessler (FBK), and in particular during the activities carried out within the Competence Center on Digital Health "TrentinoSalute4.0". In 2017 the local government of the Autonomous Province of Trento (Provincia Autonoma di Trento - PAT), the local healthcare provider Azienda Provinciale per i Servizi Sanitari (APSS) and the research institute Fondazione Bruno Kessler established the Competence Center on Digital Health "TrentinoSalute4.0" to identify new organisational models and technological solutions in the e-health domain, to study the legal aspects and evaluate their impact, and to transform technical-organisational solutions into innovative services for the healthcare sector. These objectives of "TrentinoSalute4.0" are reported at *https://trentinosalutedigitale.com/en/*. The solution was tested on the platform TreC+, which is based on the concept of personal health record. On the concept of personal health record *see* R. Saripalle, C. Runyan and M. Russell, 'Using HL7 FHIR to achieve interoperability in patient health record' (2019) 94 Journal of biomedical informatics, 103188. The solution is the advanced version of the Personal Health Record (PHR) TreC developed in 2008. The previous version of the application, TreC, is described in C. Eccher *et al.*, 'TreC platform. An integrated and evolving care model for patients' empowerment and data repository' (2020) 102 *Journal of biomedical informatics*, p. 103359. *See* also the website of TreC at *https://trec.trentinosalute.net/fast-trec*. TreC+ is currently in a release phase, and the following proposed solution is not yet fully implemented. For further details on PHR in the Italian legal system, *see* also P. Guarda and R. Ducato, 'From Electronic Health Records to Personal Health Records: emerging Legal Issues in the Italian Regulation of eHealth' (2016) International Review of Law, Computers & Technology, pp. 271-285. For the sake of clarity, the data controller of TreC+ platform is the local healthcare provider (Azienda Provinciale per i Servizi Sanitari - APSS). This local healthcare provider conceived the platform with the local government Autonomous Province of Trento and FBK. APSS stores clinical documents of citizens resident in the Province in the hospital information system (SIO, Sistema Informativo Ospedaliero). The aim of the TreC+ platform is to improve patients' empowerment by allowing access to and management of personal data (e.g. referrals, laboratory tests, drug prescriptions) and of services provided by APSS (e.g. prescriptions, telemonitoring, payments, access to parameters measured by medical devices). The digital ecosystem encompasses a web-based platform with a dashboard that is

contexts and may be a model for enhancing interoperability between different solutions adopted at the local level. In fact, it is an example of application of the data protection by design concept during the development of an e-health system that processes personal health data for the primary healthcare purpose, but whose data might be secondarily used for research purposes in the medical field.

The core pillar of this solution is the use of an e-health mobile application as a technological intermediary to enrol citizens in research projects (retrospective or prospective). A mobile application is a well-known tool for most people and healthcare providers are using it for healthcare purposes ever more frequently. Deploying this tool improves acceptability and ease of access. If we assume this tool as an intermediary component, we enable the processing of personal health data by the local healthcare provider for secondary research purposes, citizens are involved in modern "citizen science"[81], and the local government creates an "alliance with the citizens" for the proactive use of personal health data in scientific research. In this way, public entities lead the process and support scientific innovation.

It should be noted that the solution does not apply Article 110 IDPC since it refers to scientific research purposes in the medical, biomedical and epidemiological fields that are

controlled by the medical doctor/healthcare staff, a mobile e-health application (hereinafter: TreC+) and a web-based platform for patients. In TreC+ the user plays an active role: she can access and manage personal data, but can also generate data and store information. TreC+ actually allows access to the data collected in the Italian EHR, to the data provided by the patient in the PHR (e.g. weight, blood pressure, symptoms, allergies), and to APSS's services, including telemedicine services (e.g. teleconsultation, telemonitoring). On "Fascicolo Sanitario Elettronico" *see* Articles 12, 13, and 13-bis of Decreto-legge 18 ottobre 2012, n. 179 e legge di conversione 17 dicembre 2012, n. 221 recante "Ulteriori misure urgenti per la crescita del Paese". G.U. Serie Generale n. 294 del 18-12-2012 - Suppl. Ordinario n. 208; Decreto del Presidente del Consiglio dei Ministri 29 settembre 2015, n. 178 Regolamento in materia di fascicolo sanitario elettronico. G.U. Serie Generale n. 263 del 11-11-2015; and Garante per la protezione dei dati personali, Linee guida in tema di fascicolo sanitario elettronico e di dossier sanitario del 16 luglio 2009, G.U. n. 178 del 3 agosto 2009, Registro delle deliberazioni n. 25 del 16 luglio 2009. *See* also G. Vergottini and C. Bottari, *La sanità elettronica* (Bononia University Press, 2018); G. Carro, S. Masato, and M. D. Parla, *La privacy nella sanità* (Giuffrè, 2018); L. Califano, 'The Electronic Health Record (EHR): Legal framework and issues about personal data protection' (2017) 19 Pharmaceuticals Policy and Law 3-4, pp. 141–159; C. Faralli, R. Brighi, M. Martoni *et al.*, *Strumenti, diritti, regole e nuove relazioni di cura: Il Paziente europeo protagonista nell'e-Health* (G. Giappichelli Editore. 2015); M.G. Virone, *Il Fascicolo Sanitario Elettronico. Sfide e bilanciamenti tra Semantic Web e diritto alla protezione dei dati personali* (Aracne Editrice, 2015); G. Comandé, L. Nocco, and V. Peigné, 'Il fascicolo sanitario elettronico: uno studio interdisciplinare' (2012) 1 Rivista Italiana di Medicina Legale (e del Diritto in campo sanitario), pp. 106–121.

[81] On this concept at the European level *see https://ec.europa.eu/digital-single-market/en/citizen-science.* At the theoretical level *see* S. Hoffman, 'Citizen science: the law and ethics of public access to medical big data' (2015) 30 Berkeley Tech. LJ 3, pp. 1741-1805.

not carried out on the basis of a legal or regulatory provision at the national or European Union level. In addition, through the use of a mobile application downloaded by the majority of citizens of a local area to access healthcare services, it is difficult to prove a "disproportionate effort" in informing the data subjects. The solution does not even refer to Article 110-bis IDPC since a typical local healthcare provider is a public institution of hospitalisation and care. However, it takes into account all the research studies involving personal health data and even studies using anonymised data since it provides an information layer and a dedicated website that make all the relevant information available in a transparent manner.

More specifically, when a user downloads an e-health application that gives access to and manages personal data and health-related services of a local healthcare provider, she logs in with her credentials[82] and receives various notices, including information on the use of the app (e.g. as a PHR, FSE, and tool to manage services) and the modular and user-friendly privacy policy. The information on the app will state that it is a tool requesting participation in research projects. The privacy policy will link to the complete policy in a dedicated website, and will specify that the application may profile the user through the data entered and processed in order to propose research projects for which the user is eligible. After viewing the privacy policy, the user must give consent for using the app and may agree to processing related to the FSE (feeding and levels of consultation of the data) and to automatic profiling. The denial of this consent does not affect the proposed solution since, in the case of denial, the research proposal will be sent in another way, which will be described soon.

While using the application, the user will be able to generate different information about her health and medical history. A virtual coaching system integrated in the app will interact with the user by sending messages. A chatbot will invite and guide the user to fill information in the profiling form, which will be a questionnaire on medical history, pathologies, habits and lifestyle, etc. In addition, the user will receive messages from the chatbot about information related to active research projects that do not need the data subjects' consent (e.g. research based on a regulatory provision, research on anonymised data). So, push notifications will be used to send messages relating to the existing research studies that are also described in a website following the French approach of Health Data Hub. The details of the data processing and the research projects will be combined on the

[82] The user must be a citizen enrolled in the health registry. The citizen must have the credentials to use the application. Moreover, the explanation of the solution presumes that the user is not a minor.

Online First ISSN 2281-5147

website as specific sheets using concise, transparent, intelligible and easily accessible forms in clear and plain language that highlight characteristics of the studies and of the processing operations. As a result, citizens can be informed about research activities in the local environment.

When a physician/researcher from the local healthcare provider defines a structured research project that requires the use of health data of patients, after obtaining the approval of the competent ethics committee within the local territory, which may be a preliminary step, the number of people to be enrolled (sample size) and the inclusion criteria necessary for research will be specified. A special dashboard linked to the app checks the eligible users that have accepted to be profiled. If the number of eligible users is sufficient, the research proposal will be sent through the chatbot only to these profiles. If the number of eligible users is not sufficient, the chatbot notification will be activated for all the active subscribers regardless of profiling. The chatbot should then have the function of creating a questionnaire based on the eligibility requirements of the specific study for non-profiled members in order to assess actual eligibility.

If the user has consented to the profiling and is among the eligible persons, the chatbot will send a message inviting her to participate in the research project. If the user has not given consent to profiling, the chatbot will send messages asking about general interest in participating in the specific research project and further messages for filling in the specific questionnaire to verify eligibility.

Anyway, if eligible, the user, guided by the chatbot, will view the information on the research project and the related detailed privacy policy with a reference to the full policy and information sheet on the website. Then, the user will be able to give explicit consent to participate as a data subject and consent as a human participant in a scientific research study, directly in the app. The user must give privacy consent to the specific project and to participate in the project. The denial affects the lawfulness of processing and prevents any research activity.

Afterwards, the user will receive messages about scheduled project events through the chatbot. By entering the website, the user will be able to withdraw her participation in the project by sending an email to the project manager and data protection officer indicated there. It will be specified that the personal data that have been processed for research purposes up to that moment will remain in the project until its end, but that new data will not be sent to the project.

Online First ISSN 2281-5147

At the end of the research project, the user will receive a message to access the project sheet on the website where she will be able to view information about the results, publications, reports and impact of the study. The user may also receive an invitation to respond to an evaluation survey about participation in the research.

The solution described complies with the requirements of the GDPR and with the data protection by design obligation since principles of Article 5 GDPR are fulfilled. The data processing is lawful on the basis of Article 9, par. 2, lett. j) and explicit consent is collected as an additional safeguard that respects the essence of the right to data protection and protects fundamental rights and interests of the data subjects while fostering scientific research. Interpreting Article 110 IDPC *a contrario*, in Italy for the activities carried out under Article 9, par. 2, lett. j) GDPR, the request for consent is binding unless one of the exceptions apply. In the "Scientific research requirements" the *Garante* confirms that consent is required unless the research is carried out on the basis of a legal provision or when it is not possible to obtain it for particular and exceptional reasons.

Moreover, the solution is fair and transparent since detailed information is provided to the data subject by push notifications in the app, even when consent is not required, and the research study is grounded on a regulatory basis by exception. The purpose limitation principle is guaranteed since the purpose of the research study is specified and explicit in the privacy policy and sheet provided to the user when requesting participation and it is always available on the website. Only personal data that are relevant to the research study will be processed (data minimisation); then, the other personal data collected and processed in the application are kept aside and not made available to the researcher. This also complies with the data protection by default requirement (Art. 25, par. 2, GDPR). In addition, the security and storage limitation principles are protected by the measures implemented in the application, but also at the platform level since the activities are carried out in a more complex scenario that does not use only an app but is connected to a digital e-health ecosystem of a local healthcare provider. For the sake of completeness, it should be noted that the other requirements of the GDPR will be implemented at the organisational level, including the DPIA, the creation of the record of the processing activities, the agreements between controllers and any processors, the management of data subjects' rights, and the designation of the DPO. Personal data is not transferred either to third countries or to international organisations.

In sum, an e-health application used by a local healthcare provider in a digital health context can be implemented as the technological intermediary that can be used to enrol citizens in scientific projects in the medical field, provide information and, where

applicable, collect their consent as data subjects and human participants, and manage several aspects of the data processing. Through this tool, the data subject will be able not only to express consent, but also to withdraw it in the future, and to access information on projects involving their data and on other projects that may indirectly impact their health, also receiving push messages on new projects. The controller, a local healthcare provider, can set up many prospective and retrospective research studies, and find participants by using an e-health application. Consent is obtained by the use of a chatbot in the same app. According to this solution, the imbalance of power between the controller and the data subjects seems to be avoided and the data protection by design obligation fulfilled.

6. Conclusive remarks

The issues related to fostering medical scientific research as a secondary use of personal health data are intrinsically characterized by interdisciplinarity. It is challenging to strike an appropriate balance between the promotion of research and the protection of a particular category of personal data. Several and complex rules and conditions are established by the legal frameworks at EU and Member States levels. Facing the analysis of concrete application scenarios and being able to envisage reliable solutions of a technical-legal nature require an innovative and holistic approach that creates a synergy of the various types of knowledge involved.

Data protection by design, therefore, plays a fundamental role. The correct definition of the data protection risks and the adoption, from the beginning, of technical and organisational measures aimed at implementing principles and rights relating to the protection of personal data in an appropriate and effective manner are essential in anticipating and minimising the possible risk of unlawful processing. However, this implementation is very complex, especially in the new e-health context.

A holistic approach but also and above all a proactive one: in order to overcome the complexity and legal nebulosity that governs the possible use of health data for secondary purposes in the medical field, it is more advisable to focus on proactive solutions that emphasise the importance of patients' empowerment, placing them truly at the centre of the flows and the decisions relating to the processing of data concerning them.

In this paper we have tried to analyse the reference regulatory framework in a comparative way by taking into account both the EU level and two Member State's laws. The compatibility of the research purpose does not leave out the need to identify the applicable legal ground for processing and to consider all the binding conditions that apply to the special category of personal data and to the particular activities of research studies.

Online First ISSN 2281-5147

A data protection framework should provide rules to enhance scientific research and not be an obstacle to it.

We also attempted to envisage a proactive legal-technical solution, which applies data protection by design in the development of an e-health system that processes personal health data for the primary healthcare purpose and can be used as a technological intermediary to enrol citizens in research projects. This solution may concretely support researchers and professionals involved in medical research projects since: it defines a clear basis for processing personal data for secondary research purposes; it uses the additional safeguards of the explicit consent (as provided by the Italian framework); it gives high importance to providing complete and transparent information (i.e. as planned by the French national initiative). Such an approach is in line with the GDPR *favour* on fostering secondary uses of personal data and enhances scientific research by involving as many subjects as possible in a safe and compliant environment.

However, the success of this type of initiative relies on the direct involvement of the patient/citizen who must be made aware of the benefits in general terms of scientific research and of the fact that her direct participation in this type of activities is the key to their success. Communication campaigns at the European, national and local levels should attract the interest of citizens regarding categories of research studies and the use of e-health solutions.