European Review of Private Law 5-2021 [785–806] © 2021 Kluwer Law International BV, The Netherlands.

What Can We Do with the Data of Deceased People? A Normative Proposal

Iñigo de Miguel Beriain[*], Aliuska Duardo Sánchez[**] & José Castillo Parrilla[***]

Abstract: The health and genetic data of deceased people are a particularly important asset in the field of biomedical research. However, in practice, using them is complicated, as the legal framework that should regulate their use has not been fully developed yet. The General Data Protection Regulation (GDPR) is not applicable to such data and the Member States have not been able to agree on an alternative regulation. Recently, normative models have been proposed in an attempt to face this issue. The most well-known of these is posthumous medical data donation (PMDD). This proposal supports an opt-in donation system of health data for research purposes. In this article, we argue that PMDD is not a useful model for addressing the issue at hand, as it does not consider that some of these data (the genetic data) may be the personal data of the living relatives of the deceased. Furthermore, we find the reasons supporting an opt-in model less convincing than those that vouch for alternative systems. Indeed, we propose a normative framework that is based on the opt-out system for non-personal data combined with the application of the GDPR to the relatives' personal data.

Résumé: Les données sanitaires et génétiques des personnes décédées constituent un atout particulièrement important dans le domaine de la recherche biomédicale. Cependant, dans la pratique, leur utilization est compliquée, car le cadre juridique qui devrait réglementer leur utilization n'est pas encore totalement développé. Le règlement général sur la protection des données (RGPD) n'est pas applicable à ces données et les États membres ne sont pas parvenus à s'accorder sur une réglementation alternative. Récemment, des modèles normatifs ont été proposés pour tenter de faire face à cette problématique. Le plus connu d'entre eux est le don de données médicales à titre posthume. Cette proposition soutient un système de don opt-in de données de santé à des fins de recherche. Dans cet article, nous soutenons que le données médicales à titre posthume n'est pas un modèle utile pour aborder le problème en question, car il ne tient pas compte du fait que certaines de ces données (les données génétiques) peuvent être des données personnelles des parents vivants du défunt. En outre, nous trouvons les raisons qui soutiennent un modèle opt-in moins convaincantes que celles qui se portent garantes de systèmes alternatifs. En effet, nous proposons un cadre

* (Corresponding author) has the Chair in Law and the Human Genome Research Group, Department of Public Law, University of the Basque Country UPV/EHU, Bizkaia, Spain, and at IKERBASQUE, Basque Foundation for Science, Bilbao, Spain. Email: inigo.demiguelb@ehu.eus.

** Researcher at the same Chair in Law and the Human Genome Research Group. Email: aliuska.duardo@ehu.eus.

*** postdoc at the same Chair in Law and the Human Genome Research Group. This work was supported by H2020 Science with and for Society Programme (grant number 788039 – PANELFIT). The final version of this article was submitted on 28 July 2021. Email: castillop@ugr.es.

normatif qui repose sur le système d'opt-out pour les données non personnelles combiné à l'application du RGPD aux données personnelles des proches.

Zusammenfassung: Die gesundheitlichen und genetischen Daten von Verstorbenen sind ein besonders wichtiges Gut im Bereich der biomedizinischen Forschung. In der Praxis ist ihre Verwendung jedoch kompliziert, da der rechtliche Rahmen, der ihre Verwendung regeln sollte, noch nicht vollständig entwickelt ist. Die europäische Datenschutz-Grundverordnung (DSGVO) ist auf solche Daten nicht anwendbar und die EU-Mitgliedsstaaten konnten sich nicht auf eine alternative Regelung einigen. In letzter Zeit wurden normative Modelle vorgeschlagen um diesem Problem zu begegnen. Das bekannteste davon ist die posthume medizinische Datenspende (PMDD). Dieser Vorschlag unterstützt ein Opt-in-Spendesystem von Gesundheitsdaten zu Forschungszwecken. In diesem Beitrag argumentieren wir, dass PMDD kein brauchbares Modell ist, um das vorliegende Problem anzugehen, da es nicht berücksichtigt, dass einige dieser Daten (die genetischen Daten) die persönlichen Daten der lebenden Verwandten des Verstorbenen sein könnten. Zudem finden wir die Gründe, die für ein Opt-in-Modell sprechen, weniger überzeugend als diejenigen, die für alternative Systeme eintreten. Überdies schlagen wir einen normativen Rahmen vor, der auf dem Opt-out-System für nicht-personenbezogene Daten basiert, kombiniert mit der Anwendung der DSGVO auf die personenbezogenen Daten der Angehörigen.

1. Introduction

1. The health and genetic data of deceased people are particularly important assets in the field of biomedical research. Today, thousands of stored medical records from people who have passed away could be used to improve our knowledge of many pathologies or to develop mechanisms such as artificial intelligence algorithms. However, using them would be complicated in practice, as the legal framework that should regulate their use has not been fully developed.[1] This increases legal uncertainty, which consequently discourages investment in research in this sector.

2. This situation has created a regulatory loophole regarding the data of deceased persons, which is especially worrying if we take into account several particularly important factors: 1) This type of data is an enormously valuable source of information for not only biomedical research but also research of all kinds (e.g., for epidemiological studies after a pandemic such as the one we are experiencing); 2) These are data that will gradually accumulate, as, if one thing is certain, it is that people will continue to die so that in the coming years there will be more data on deceased people than data on living people; 3) Drawing up a very different regulatory framework for data on living people and deceased people may even make ongoing research more difficult. Consider, for example, a biomedical researcher using the data of living persons, which are processed on a legal basis according to

1 J. Krutzinna & L. Floridi, 'Ethical Medical Data Donation: A Pressing Issue', in J. Krutzinna, L. Floridi (eds), *The Ethics of Medical Data Donation* (Cham (CH): Springer 2019), pp 1-8.

the General Data Protection Regulation (GDPR). If these people die during the course of the research, could data that would no longer be personal continue to be processed? Under what legal basis?

3. Recently, some regulatory models have been proposed that attempt to address this issue through new tools. The most well-known of these is posthumous medical data donation (PMDD), developed by the Digital Ethics Lab at the Oxford Internet Institute, University of Oxford, and funded by Microsoft.[2] This proposal supports the donation of medical data once the data subjects pass away, on the basis of the need to profit from people's altruism and the similitude with organ donation. In this article, however, we argue that PMDD is not a useful model for addressing the issue at hand, as it does not consider that some of these data (i.e., the genetic data) may be the personal data of the living relatives of the deceased. Furthermore, we cannot find the reasons supporting an opt-in system convincing. Therefore, we propose an alternative model that appears much more feasible to us: a model based on the opt-out system that regulates data donation in several European Union (EU) countries. Before reaching this point, however, we shall begin by setting out the legal framework relating to the data of the deceased, both at the EU level and in the Member States. This is the main objective of the next following sections.

2. Data of Deceased People: A Preliminary Analysis of Its Legal Framework according to the GDPR

4. What is the legal framework that rules over the data of deceased people? Unfortunately, this question has no easy answer. First, it should be noted that, in principle (and we will come back to this affirmation in further sections), the data of deceased persons cannot be considered their personal data for the simple reason that dead people are no longer persons. If there is one thing that is common to all legal systems we know of, it is that personality is extinguished with death. This does not mean that there are no regulations to protect posthumous interests (criminal regulations usually consider outrages to their bodies as crimes, and civil regulations protect the defence of their moral rights), but this defence does not include recognition of a legal personality in any way. Therefore, it is logical and consistent that their data are not considered personal data (or, rather, *their* personal data).

5. This position has been adopted by 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 (GDPR), which states that the data of deceased persons are not their personal data. Its Recital 27 explicitly states that

2 J. Krutzinna, M. Taddeo & L. Floridi, 'Enabling Posthumous Medical Data Donation: A Plea for the Ethical Utilisation of Personal Health Data', in *The Ethics of Medical Data Donation* pp 163–180.

'This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons. Thus, the data of the deceased are not their personal data according to the GDPR and therefore its clauses do not apply to them. As a consequence, the regulation of this issue remains in the hands of the Member States. In recent years, some of them have made an effort to establish explicit regulations on this kind of data. These will be explored in the next section.

3. Data of Deceased People: An Analysis of Their Legal Framework at the EU Member State Level

6. The legal framework for data corresponding to deceased people differs between the different EU Member States. However, there are some common roots that are generally shared by most (if not all) of them. This includes rules of common law protecting dead people's honour and dignity. On this basis, a person can be sued if, for instance, they reveal information that might damage deceased people's public image or create an offence against their respectability. Obviously, this means that you cannot process their data in a way that is not strictly respectful of the deceased people's fundamental rights without the risk of being sued and condemned to compensate their heirs for the harm done. Furthermore, some countries protect professional secrecy even after the data subject is dead. For instance, health care workers are obliged to keep secrecy about health care records even after the death of the patients, otherwise, they could be sued and/or suffer from a sanction that might cause them to lose their license to practise. Some countries may even sanction with fines and/or prison sentences °those who gain access to a deceased's records without a legal basis or break the secrecy of the information.

7. However, if we talk strictly about data protection regulation as such then we should state that the Member States' regulation of the data of deceased people shows great variety. To begin with, there are countries such as Austria, the Czech Republic, Finland, Greece, Latvia, Lithuania, the Netherlands or Ireland, whose data protection laws do not contain specific clauses on this matter. On the other side, the Danish Data Protection Act rules that the GDPR is applicable to the data of deceased persons for a period of 10 years following the death of the data subject.[3] Quite similarly, the Portuguese regulation, on the other hand, extends the GDPR scope of application to deceased persons. The particularity of this legislation is that it does not protect all of the deceased's personal data, but only those that fall under the special categories of personal of GDPR Article 9 (1), or that involve intimacy, privacy, image or data relating to communications. The corresponding rights may be exercised by those who have been designated by the

3 *Databeskyttelses-loven* (Danish Data Protection Act), https://www.datatilsynet.dk/media/6894/danish-data-protection-act.pdf (accessed 29 Sept. 2021) (Unofficial English translation).

data subject, or in their absence, by the heirs of the deceased. However, the data subject may also prevent the exercise of such rights after their death, under the applicable legal terms.[4]

8. Somewhere in between, countries such as France, Hungary, Italy, Slovenia or Spain have developed specific previsions about these data, but not a general framework entirely. In France, national data protection stipulates a digital will regarding the use of the data subject's personal information after death.[5] In this sense, the data subject can establish general guidelines for the storage of all of their personal data to a third person certified by the French data protection authority. The data subject may also issue particular guidelines to the specific responsible person regarding the processing of their personal data after their death, by giving specific consent. Where there are no guidelines, the heirs may exercise the data subject's rights where necessary for the organization and settlement of inheritance rights for the controller to take into account the death of the data subject. The heirs may close the data subject's user accounts, object to further processing or request an update of the accounts. The French regulations also establish that the information regarding the deceased, including the cause of death, may be processed for reasons of research, studies and evaluation, in the area of Health, except if the data subject opposed it during their life.[6]

9. According to Hungary's Privacy Act, deceased data rights may be enforced, within 5 years of the data subject's death, by a person authorized through an administrative disposal or a declaration made to the controller and incorporated in a public deed or a private deed of full probative value. If the data subject has made more than one declaration to the same controller, the most recent one will be taken into account.[7]

10. In Italy, the Data Protection Act states that data subjects' rights can be exercised by those who have a personal interest, or who behave to protect the deceased data subject on their behalf or for family reasons that shall be protected, unless the data subject has expressly forbidden it. Nonetheless, this prohibition shall not affect third parties' economic interests as well as the right to defence.[8]

---

4 Article 7, Law 58/2019, from 8 August https://dre.pt/web/en/home/-/contents/123815982/details/normal (accessed 29 September 2021).

5 Article 8, Loi n°78-17 du 6 janvier 1978 (Law no. 78–17 of 6 January 1978 on information technology, files and freedoms).

6 *Ibid.*, Art. 86.

7 Section 25, Act CXII of 2011 on the right to informational self-determination and on the freedom of information (Privacy Act), http://njt.hu/translated/doc/J2011T0112P_20190426_FIN.pdf (accessed 29 September 2021).

8 Article 2 *terdecies*, Legislative Decree 196/2003, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9042678 (accessed 29 September 2021).

11. The personal data of deceased persons are protected by Slovenian law. Such data may be shared with the first – or second-order legal heir of the deceased, if the latter demonstrates a legitimate interest in the use of the personal data and the deceased did not prohibit the provision of such personal data in writing. In addition, data processing may be permitted by law, or if necessary, for research/statistical purposes. In particular, persons who, under the law governing inheritance, are the first – or second-order legal heirs of the deceased, may prohibit in writing the provision of the data of the deceased, unless otherwise provided for by law.[9]

12. Finally, the Spanish Data Protection Act establishes that persons linked to the deceased for family or de facto reasons or their heirs may request access to these data, as well as their rectification or deletion. However, the regulation allows the deceased to impose a veto on the access to these previous subjects, with some exceptions related to patrimonial inquiries.[10] If dealing with health data, several EU countries allow persons linked to the deceased to access, rectify or delete data if not excluded by the deceased. Regarding health data, the explicit veto will not apply if the access requirement is motivated by a health risk.

4. Bridging the Gap: The PMDD Proposal

13. According to Sections 2 and 3 of this article, we must conclude that the legal framework regarding the data of deceased people is not clear at all, at least if we concentrate on data protection regulation at the Member States level. Of course, one might argue that there are some regulations regarding the data of deceased people at the Member State level. However, none of them seem able to guarantee the adequate use of such impressive wealth that might be underutilized if no reasonable measures are taken to remedy it. Under these conditions, some voices have already emerged, suggesting that reasonable alternatives should be adopted to ensure that these data are used in a way that is satisfactory to our common interests. The most remarkable of these initiatives is the so-called PMDD, a proposal developed by Krutzinna, Taddeo and Floridi, researchers working at the Digital Ethics Lab at the Oxford Internet Institute, University of Oxford, funded by Microsoft,[11] which is meant to serve as an efficient tool to conciliate the use of data gathered from deceased people with the exigencies of the GDPR.

---

9 Article 23, Data Protection Act (Official Gazette of the Republic of Slovenia, No. 94/07 – Official Consolidated Text and 177/20) (*Zakon o varstvu osebnih podatkov, ZVOP-1*), https://www.ip-rs.si/en/legislation/personal-data-protection-act (accessed 29 September 2021).

10 Article 3.1. Organic Law 3/2018, of 5 December on the protection of personal data and guarantee of digital rights.

11 J. Krutzinna, M. Taddeo & L. Floridi, in *The Ethics of Medical Data Donation*, pp 163–180.

14. Indeed, the PMDD is an initiative that encourages enabling the act of donating one's personal medical data after death. Its proponents base their proposal on the idea that the management of genetic data should resemble that of human organs or bodies: an opt-in system based on a person's explicit consent. Just as we all have the ability to decide to donate the organs for transplants or to encourage research or learning by future doctors, we should also have the possibility of disposing of our personal data after our death.

15. According to its proponents, the consent that enables donation shall be gained through a detailed process that allows people to introduce numerous details regarding the concrete use that can be made of their data:

> Prior to giving informed consent, the person concerned shall be offered appropriate information about the nature and purpose of PMDD, including examples of the type of research for which it will be used, the financial interests of the data-collecting entity, and the management of access to and use of the data, including the kinds of safeguards that will be maintained (...) Donors shall be free to place restrictions on the use of their data and to exclude subsets of data from their donations (...) Donors shall be informed of their right to make changes to their preferences or to withdraw consent at any point prior to their death. Donors shall be encouraged to discuss their decision with their relatives, especially those with close genetic links. Donors shall be informed that the use of their PMDD is not guaranteed and that in some rare instances a particular PMDD may be rejected if it poses a significant risk of harm to an individual or a group. Information shall be provided on possible reasons for exclusion. Consent shall be appropriately documented.

5. PMDD: A Critical Analysis

16. Thus, PMDD constitutes a carefully elaborated normative proposal meant to resolve the issues related to the data of deceased persons in the framework of the GDPR. However, is it convincing? It appears so at first sight. Both the expertise of its supporters and the strength of their arguments give the proposal large amounts of consistency. Indeed, they provide up to 10 apparently convincing reasons to support their proposal:

1. It is unethical to frustrate the 'will-to-do-it' without proper justification (...) The ability to contribute to the advancement of medicine and act as a moral agent can provide a significant benefit during one's lifetime.
2. The concept of altruism is well-established and should include data donation for the common good. There is evidence that most individuals already desire to act morally.

3. If one receives healthcare, it is only fair that one gives back (...) there is moral obligation to participate in scientific research.
4. PMDD is an appeal to inter-generational solidarity.
5. PMDD would foster a human right to science (...) This includes a human right to participate in the scientific process in its entirety.
6. There is an economic argument (...) the more data are donated, the more value the old data have.
7. It is crucial to facilitate PMDD immediately, as the trend towards commercialization of personal health data is growing.
8. PMDD is also a matter of logical coherence. Considering that (most) people can already donate their organs and blood, and that it is possible to extract substantial data from those donations, it is logically incoherent not to allow PMDD. Furthermore, implicitly, individuals are already allowed and often enabled to give away freely their personal data to private corporations, often for uncertain purposes, as the terms and conditions of many commercial platforms make clear.
9. Two key risks are diminished in PMDD, as both consent and privacy are less troublesome where the data relate to a deceased as opposed to a living person.
10. Given that most of the reasons for scientific data sharing also apply to PMDD, a decision to promote one but not the other is logically and ethically inconsistent.

17. Are these points provided by the proponents of PMDD as consistent as they seem at first sight? In our opinion, they are not, for different reasons. Some are quite obvious, as they are due to clear inaccuracies in the assumptions of some of the reasons given. We will begin by providing arguments to answer each one of the '10 reasons in favour of PMDD' and finally, other arguments not directly related to one of these '10 reasons'.

1. Of course, it is not ethical to frustrate the 'will-to-do-it' of people without proper justification. Nonetheless, there are proper justifications such as the improvement of medical diagnosis, the provision of health care or treatment, contributing to ensure high standards of quality and safety of health care, medical products or medical devices. All those reasons can be summed up as an example of public interest in the health field. The first reason also states that contributing to the advancement of medicine is to act as a 'moral agent', and it «can provide a significant benefit during one's lifetime». This argument appears weak compared to public interest in the health field.

2. The idea of social altruism could reinforce either PMDD or the PMDC (post-mortem data conscription)[12] model. If most individuals desire to act morally,

12 That is, legal prevision of using post-mortem data for specified health or scientific reasons.

and donating health data for public interest is 'moral', there should not be obstacles to developing legal previsions for post-mortem data use related to public interest in the health field.

3. If giving back health profit is a reason in favour of PMDD, it is also a reason in favour of PMDC. The voluntary model described in this point could be a good model for developing the legal previsions of PMDC.

4. Inter-generational solidarity can emerge either spontaneously or by legal prevision; hence, it does not necessarily lead to a voluntary model (PMDD). Rules that restrict people's will after death (e.g., limitations to the will to test), or that take a part of people's wealth after death without their consent (e.g., inheritance tax) are also expressions of social awareness and inter-generational solidarity.

5. Legal previsions on using post-mortem data for health or scientific reasons would not hinder the possibility of letting people participate in the scientific process if the PMDC model is only developed for justified and specific situations where using these data is crucial for health or scientific advances. Other situations could still use the voluntary model (PMDD), combining both depending on the situations as described by the law.

6. The 'scale argument' of reason 6 is unquestionable: the more data can be used, the more valuable each of those data are. This is also related to the so-called 'network effect'. Again, if achieving this 'network effect' is desirable, a voluntary model would require more time to achieve than a model based on legal provisions for specific situations. A PMDC model would obtain more data in less time.

7. If we want to stop data commercialization in the field of health data, the most effective way would be to consider health data as res extra commercium (as it happens with organs or the human body), but this measure has nothing to do with PMDD or PMDC, as both systems would not reject this consideration of health data. Besides, if our purpose is to stop the growth of health data markets, what better than declaring post-mortem health data both as res extra commercium and of public interest value so that public power can make use of them whenever proper justifications are given (regardless of the deceased person's consent) and only under the conditions specified by the law? Consent as legal basis would leave more space for the growth of health data markets than legal provisions of use, as the last would be unique (for each State or, e.g., for the EU).

8. It would not be incoherent to deny data donation even though organ donation is allowed. Organs and health data can be similar from certain points of view (e.g., both should be considered res extra commercium), but it does not mean that their legal regulation should be identical. Even when people donate their organs, this fact does not allow data to be extracted and processed when those data are personal data.

This point also outlines a concerning situation on data processing: people already grant 'cheerful consent' to data processing, and this is troubling because it indicates a paucity of consent as the basis of legitimacy to data processing. If this is

true, PMDD (based on consent) may not be the most advisable way to regulate post-mortem data processing.

It is untrue that 'individuals are already allowed and often enabled to freely give away their personal data to private corporations' (point 8). Even though people can consent to data processing, they cannot renounce the rights provided by the GDPR. Thus, these data are not commercialized in any way, therefore banning data donation would not be incoherent at all. For similar reasons, point 7 is not truthful: put simply, the commercialization of personal data is clearly illegal in the EU arena. Therefore, it can hardly grow.

9. This point could speak in favour of a voluntary model (PMDD) and a legal-provided model (PMDC).

10. Sharing the data of living people and post-mortem data sharing are not comparable, as the latter are not accurately personal data.

18. There is a strong argument in favour of PMDD: a voluntarist model for collecting data is less likely to cause social alarm than, for example, a legal prevision of using these data for scientific or health reasons regardless of the opinion of the deceased. Nonetheless, consent as legal basis would provide less legal certainty than a detailed legal prevision of using post-mortem data if specific scientific or health reasons are met. Both legal bases are possible according to the GDPR, but the most recent (legal prevision of using post-mortem data for scientific or health reasons) has not been explored or debated yet.

19. Some other reasons are more convincing, but not so much as to overcome some particularly complex obstacles. For example, the case of genetic data that reveal information about genetically related people is not adequately addressed by the PMDD. Its proponents are aware of the issues that this type of data involves. Indeed, they state that in those cases 'it may be preferable to exclude such data from the donation where a comprehensive risk assessment reveals an unacceptably high risk to living people. This may apply especially where the relatives are vulnerable people and/or the condition is a hereditary disease, which may lead to stigma and/or discrimination'. There is, however, a fundamental juridical issue that is not addressed by the proponents of the initiative: if these data provide information about natural persons, then these data could entirely be considered the personal data of those people. But, in that case, the concept of data donation would be entirely inaccurate. On the other hand, we consider that the PMDD model proposed by Krutzinna, Taddeo and Floridi does not provide us with solid reasons that make it preferable to the conscription model or to an opt-out donation model. In the next sections, we will attempt to elaborate on these objections.

6. Data of Deceased People Might Be Personal Data

6.1. Understanding the Issue: Genetic Data as Biological Group Data

20. We have merely stated that data that might reveal information about the relatives of deceased people can absolutely be considered personal data. This might appear contradictory to the statements made in the earlier sections of this article. Indeed, we have previously considered that the data of the deceased are not their personal data, according to the GDPR. However, this does not mean that they are not personal data at all. Indeed, in the case of data concerning health (that is, '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', GDPR Article 4(15)), and more particularly, in the case of genetic data (that is, 'personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question', GDPR Article 4(13)), these might entirely be considered as such. Indeed, they are the personal data of the people these data relate to, namely those persons who are genetically related to the deceased person who provided the genetic data.

21. The fact that Article 4(13) includes at the end the tag 'in particular, from an analysis of a biological sample from the natural person in question' where defining genetic data does not deny the statement we have just made, but on the contrary, confirms it. It must be deduced from its formulation that the legislator considered that the data extracted from a 'biological sample from the natural person in question' constituted a particular case of genetic data, but there may be other data that do not come from this source but from other sources. Genetic data extracted from a third party genetically related to the natural person about whom it discloses information falls perfectly into this category.

22. Of course, this means that, in general, we should talk about data subjects in plural instead of a data subject when we consider genetic data, as the information this type of data discloses refers to different people. This might appear unusual, but it is not at all a revolutionary notion, as the Article 29 Working Party stated in 2004 that:

> It is worth noting that a new, legally relevant social group is coming into existence – namely, the biological group, the group of kindred as opposed, technically speaking, to one's family. Indeed, such a group does not only include family members such as one's spouse or foster children, but it can also consist of

> entities outside this family circle – whether in law or factually (e.g.: gamete donors).[13]

Similarly, the European Data Protection Supervisor (EDPS) has recently stated that 'Genetic research in particular has implications not only for the subject of the DNA tests but others in his or her family or with shared characteristics in this and future generations'.[14] Thus, considering that personal data can be shared by a group of people is not at all inconceivable under the GDPR.

23. Moreover, this statement is perfectly consistent with the wording of GDPR Article 4(1), which states that personal data means:

> any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

According to this definition, data revealing information about a relative of the deceased person is personal data of that relative whenever this relative exists and is known (or can be known) by those who process the data.

24. Furthermore, the statement made is also well-aligned with the extensive interpretation of the concept of personal data given by the Court of Justice of the EU in cases such as *College van Burgemeester en Wethouders van Rotterdam* v *M. E. E. Rijkeboer*,[15] which has been reinforced in recent years.[16] Namely, in the *Peter Nowak* v *Data Protection Commissioner* case, where the Court stated that:

> The use of the expression "any information" in the definition of the concept of "personal data", within Article 2(a) of Directive 95/46, reflects the aim of the EU legislature to assign a wide scope to that concept, which is not restricted to

---

13 A29WP, Working Document on Genetic Data, WP 91, Adopted on 17 Mar. 2004, p 14, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf (accessed 29 September 2021).

14 European Data Protection Supervisor, A Preliminary Opinion on data protection and scientific research, 6 January 2020, p 26, https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf (accessed 29 September 2021).

15 ECJ 7 May 2009, *College van Burgemeester en Wethouders van Rotterdam* v. *M. E. E. Rijkeboer*, ECLI:EU:C:2009:293, curia.europa.eu/juris/documents.jsf?num=C-553-07.

16 D. Jove, 'Peter Nowak v. Data Protection Commissioner: Potential Aftermaths Regarding Subjective Annotations in Clinical Records', 5. *European Data Protection Law Review* 2019, pp 175–183.

information that is sensitive or private, but potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments, provided that it "relates" to the data subject.[17]

Therefore, all types of information that might be linked to a natural person, by reason of its content, purpose or effect, must be considered personal data. Thus, it is crystal clear to us that genetic data that provides information about a person is their personal data, wherever it comes from and whether it also provides information about someone else.

25. Finally, such an approach would work particularly well with some relevant regulations about human rights at the international level. For example, Article 10 of the UNESCO Universal Declaration on the Human Genome and Human Rights states that: 'No research or research applications concerning the human genome ... should prevail over respect for the human rights, fundamental freedoms and human dignity of individuals or, where applicable, of groups of people'. Similarly, Article 4 of the Council of Europe Additional Protocol to the Convention on Human Rights and Biomedicine, concerning Genetic Testing for Health Purposes reads: 'Any form of discrimination against a person, either as an individual or as a member of a group on grounds of his or her genetic heritage is prohibited'. Thus, both documents recognize the importance of the biological linkages between people and somehow introduce the notion of common interests and rights of those groups, a notion that works perfectly well with the idea we support: that genetic data are the personal data of a group of people (the biological group).

6.2. Objections to the Argument

26. If genetic data obtained from deceased people can be considered the personal data of their relatives, then they cannot be owned, and thus, they cannot be donated, according to the GDPR. Indeed, processing would only be lawful if researchers find an applicable legal basis for it independent of the source of the data. But if this is all true, then the approach adopted by Krutzinna and colleagues would clearly be inconsistent, at least in the case of genetic data, as consent provided by a person who has passed away can hardly erode the rights, interests and freedoms of their living relatives: if any of them opposes processing, the

17 ECJ 20 December 2017, *Peter Nowak* v. *Data Protection Commissioner*, ECLI:EU:C:2017:994, curia.europa.eu/juris/documents.jsf?num=C-434/16. See also ECJ 29 Jan. 2009, *Productores de Música de España (Promusicae)* v. *Telefónica de España SAU*, curia.europa.eu/juris/documents.jsf?num=C-275/06, ECLI:EU:C:2008:54; ECJ 24 November 2011, *Scarlet Extended SA* v. *Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, curia.europa.eu/juris/documents.jsf?num=C-70/10, ECLI:EU:C:2011:771; ECJ 19 Oct. 2016, *Patrick Breyer* v. *Bundersrepublik Deutschland*, ECLI:EU:C:2016:779, curia.europa.eu/juris/documents.jsf?num=C-582/14.

deceased donor's consent would serve no purpose (and safeguards created by Article 89 would of course apply to the living relatives). Finally, we should always bear in mind that, under such circumstances, GDPR Article 14 would oblige researchers to inform the living relatives about the processing within a reasonable period of obtaining the data and no later than one month.

27. There are, however, objections that can be made to our alternative approach, all consistent with the PMDD model. First, one could argue that these data are not personal data, as it is not possible to link them with the relatives if a fundamental data is not included in the record: the existence of such relatives. However, this does not seem to be a major objection, as civil registries are public in most countries. Therefore, it would be easy for a person to know with whom these data are related. Consequently, they should be considered 'identifiable' natural persons. Furthermore, relatives would surely know that the deceased person is genetically related to them. Therefore, they are usually aware that a record that might contain information related to them exists.

28. Second, it could be argued that if we were correct, processing the data of deceased persons would be extremely complex. In principle, genetic data reveal information about many people, so all of them would have to agree to the processing of the data. Therefore, it does not seem very reasonable to trust the future of our research on this basis. The problem with this rebuttal is that it should lead to the substitution of consent for another legal basis for the processing of such data, such as vital or public interest, but it would not serve to refute our argument as such.

29. A third objection comes from a practical side of the debate. Even though one might agree on the theoretical approach built on the biological group concept, in practice this would bring us nowhere, as all human beings are somehow linked to each other. Somehow, we all constitute a biological group. Therefore, this approach would make it necessary to concede that we would all be data subjects in any data processing. However, this would render the whole data protection framework feeble. This is a more consistent objection, but it can also be negated if we consider that it is not so different to all the rebuttals that are built on the idea of 'fuzzy concepts'. For example, in the gene editing debate, a major argument against using these techniques stems from the fact that it is difficult in practice to find a border between therapy and enhancement. However, it is often stated that this should not be a definitive criterion for banning gene editing, as it would always be possible to trace these borders through regulation and jurisprudence.[18] In the case of biological groups, this could absolutely happen in the same way: we should

18 I. De Miguel Beriain, 'Should Human Germ Line Editing be Allowed? Some Suggestions on the Basis of the Existing Regulatory Framework', 33. *Bioethics* 2019, pp 105–111.

have to determine who is to be considered a data subject through regulation, and the consequences of this recognition should be clearly described. Of course, this would make things difficult, but not impossible: it would be sufficient to balance the interest of the different people involved in each data processing. Furthermore, if we were to take the alternative position, then the concept of 'biological group' would remain an empty box, but this does not work well with the opinion of the Article 29 Working Party and the abovementioned international regulatory tools.

30. A further, weightier objection is that, if genetic data are the personal data of a group, then clearly this should be true of both the deceased and the living persons. In other words, if the fact that genetic data are information associated with several identifiable persons means that they should all be considered data subjects, then all those with genetic links should be considered to share the same personal data. This objection is more convincing than those previously addressed and is not easy to address. Indeed, it would be difficult to deny that the GDPR was built based on individual subjects' rights. As Hallinan and De Hert stated:

> the idea of genetic groups as a focus of data protection law is novel. The Regulation – as with its predecessor the Directive – was drafted on the presumption that the individual, and individual rights, were the primary target of protection. Although data protection may seem like a – if not the – logical legal area of law through which to protect genetic groups' interests in the processing of genetic data, this is no guarantee that the Regulation will be a suitable instrument for this purpose.[19]

31. Indeed, the idea of personal data pertaining to a genetic group does not work well with the concept of the data subject, which is key in the GDPR. According to Article 4(1), a data subject is 'an identified or identifiable natural person'. However, this should not even be considered a definitive reason to omit biological groups in terms of data protection. Indeed, it is quite common that an only data refers to several data subjects, but nobody considers that this creates a terrible obstacle for the application of the GDPR. Imagine, for example, the case of a group photograph taken at a convention of practicing nudists. This photograph would clearly constitute the personal data of each and every one of those who are portrayed in it. We are all aware of this and we have learned how to deal with these situations. The same could be said about genetic data: we need to develop a framework that rules over them in accordance with the GDPR. This could be

19 A. Hallinan & P. De Hert, 'Genetic Classes and Genetic Categories: Protecting Genetic Groups Through Data Protection Law', in L. Taylor L. et al. eds, *Group Privacy.* Philosophical Studies Series, p 126.

difficult in practice, but this fact should not serve as an excuse to deny that genetic data are the personal data of different people.

7. Conscription as an Alternative to PMDD

7.1. Exposition

32. We have merely demonstrated that genetic data are the personal data of the deceased persons' relatives and thus cannot be donated by a person who is not and cannot be its (only) owner. But what about the non-personal data gathered in their medical records? This is not a weak question, as most of these data are not genetic data. Therefore, most of them do not reveal information about a living person, and thus they can be donated, as with other types of non-personal data. Thus, the PMDD model appears applicable to this category of data, at least at first glance.

33. However, we do not think that this would be the best option. First, we cannot understand why PMDD is preferable to a conscription model. It is difficult to see why, if these data are so important for scientific research and therefore for public interest, their use should be left to the individual's will instead of legal previsions. Krutzinna, Taddeo and Floridi provide some reasons for justifying this approach, but they are not so consistent. Think, for example, about point 3: if there is moral obligation to participate in scientific research, we can see no reason to let people refuse the use of their data for scientific purposes, provided that adequate safeguards to their posthumous interests are put in place. Furthermore, the economic argument (point 6) is certainly unquestionable. However, if we are to gather as many data as possible, leaving the requirement of consent aside would greatly facilitate the process. Moreover, if data commercialization is the upshot, conscription is an impressive tool at hand.

34. Indeed, in our opinion, a data conscription system is much more consistent with the reasons provided by Krutzinna, Taddeo and Floridi for sustaining the PMDD initiative than the model suggested itself. In a conscription system, data can be used without any prerequisites. As soon as a person dies, the State becomes the owner of that data, regardless of the will of the decedent, and all issues regarding informed consent disappear. As Mann, Savulescu and Sahakian[20] have argued:

> the requirement of informed consent is not appropriate for all kinds of records-based research by distinguishing studies involving minimal risk from those that

20 S.P. Mann, J. Savulescu & B.J. Sahakian, 'Facilitating the Ethical Use of Health Data for the Benefit of Society: Electronic Health Records, Consent and the Duty of Easy Rescue', *Philos Trans A Math Phys Eng Sci.* 2016, p 374(2083):20160130. doi:10.1098/rsta.2016.0130.

> feature moderate or greater risks (...) the duty of easy rescue – the principle that persons should benefit others when this can be done at no or minimal risk to themselves – grounds the removal of consent requirements for minimally risky records-based research.[21]

Furthermore, all arguments that uphold after-death organ conscription appear applicable to posthumous data.[22] In fact, these might be even stronger, as there are no religious beliefs, or fears, involved in data conscription, to our knowledge. Therefore, why should we prefer PMDD to a conscription system?

7.2. Criticism

35. Unfortunately, conscription can be the object of important criticism. Indeed, it has been criticized because by making the donation of data compulsory, people could feel that their autonomy has been violated, as it happens in the case of organ conscription.[23] As for the avoidance or alleviation of social alarm that a legal model (PMDC) could generate compared to the PMDD model, this can be controlled if: (1) proper measures are developed to guarantee post-mortem data processing only based on health public interest, and (2) the system is properly explained to the population. Moreover, the conscription of data involves depriving us of the possibility of behaving altruistically. As Krutzinna, Taddeo and Floridi argued, 'it is unethical to frustrate the '*will-to-do-it*' without proper justification. Although no individual donor will receive a benefit at the point of donation, the ability to contribute to the advancement of medicine and act as a moral agent can provide a significant benefit during one's lifetime (...) The concept of *altruism* is well-established and should include data donation for the common good. There is evidence that most individuals already desire to act morally, and may do so without the need for further encouragement when provided with the right information, a straightforward procedure, and appropriate safeguards'.[24] Indeed, there are scientific reasons to hold that altruistic behaviour

---

21 S.P. Mann, J. Savulescu & B.J. Sahakian, in *Philos Trans A Math Phys Eng Sci.* 2016, doi:10.1098/rsta.2016.0130.

22 F.M. Kamm, Morality, Mortality (vol. 1) (New York: Oxford University Press 1993); J. Harris 'Law and Regulation of Retained Organs: The Ethical Issues', 22. *Legal Studies.* 2002, pp 527–549, doi:10.1111/j.1748–121X.2002.tb00667.x; J. Harris, 'Organ Procurement: Dead interests, living needs', 29. *Journal of Medical Ethics.* 2003, pp 130–134, doi:10.1136/jme.29 March 0130.

23 E-HW Kluge, 'Improving Organ Retrieval Rates: Various proposals and Their Ethical Validity', 8. Health Care Analysis 2000, pp 279–295. doi:10.1023/A:1009496002775; R. Veatch, L. Ross, Transplantation Ethics (2d ed., Washington, DC: Georgetown University Press 2015).

24 J. Krutzinna, M. Taddeo & L. Floridi, in *The Ethics of Medical Data Donation*, pp 163–180.

and happiness are reciprocal in nature.[25] In fact, neuroscientists have found neural bases for altruism.[26] Therefore, if we deprive people of the possibility of behaving altruistically, they would lose a source of happiness, and this could be considered unethical. Nonetheless, as we have stated earlier, this argument in favour of protecting individual happiness based on altruism appears weaker than the improvement of research and public interest in the health field.

8. Non-personal Data and Data Donation: The Opt-out Model

8.1. Exposition

36. An alternative to a conscription system would be an opt-out system, like those that already exist in organ donation. Different from conscription, opt-out systems respect individual autonomy and people's choice, as they would be allowed to ban data processing once they die, except in situations where the access and use of certain data of the deceased would be crucial for addressing an important risk to the health of a third person. Therefore, an opt-out model would allow people to enjoy the psychological benefits, i.e., happiness, that altruism provides without risking the loss of huge amounts of data. Although this model makes it possible to refuse to share information in theory, it would be difficult for this to really happen. In practice, it is hard to foresee that a considerable number of people would actually opt-out from donation, provided that they are ensured the adequate safeguards about the use of their data. If we are wrong and people request for data deletion massively, this would probably mean that the main assumption of the PMDD – that most people are looking forward to donating their data for altruistic reasons – is absolutely weak. Under such circumstances, however, the best solution if we hold that we should not waste this valuable resource at all, should be opting for conscription. Therefore, there are no good reasons to hold that the opt-in system could work better that the opt-out in any way.

37. As opt-out models do not ask of people extra effort that involves thinking about their own death, for example, they could do well to avoid the circumstances that provoked the failure of initiatives such as care.data, which were mainly the lack of awareness and understanding.[27] A well-designed information campaign that ensures that the population can be informed about the system and tools that enable opting out easily should be more than appropriate, from an ethical point of view, to

25 A.R. Dalal, 'Philosophy of Organ Donation: Review of Ethical Facets', 5. *World J Transplant.* 2015, pp 44–51, doi:10.5500/wjt.v5.i2.44.

26 J. Moll, F. Krueger, R. Zahn, M. Pardini, R. de Oliveira-Souza & J. Grafman, 'Human Fronto-Mesolimbic Networks Guide Decisions About Charitable Donation', *Proc Natl Acad Sci USA.* 2006, 103(42) pp 15623–15628.

27 P. Carter, G. Laurie & M. Dixon-Woods 'The Social Licence for Research: Why Care.Data Ran Into Trouble', *J Med Ethics.* 2015(41) pp 404–409.

justify the implementation of such a system. We intuitively thought that such a model would be more peacefully accepted in countries where the organ donation system already operates on the basis of an opt-out system. However, it is likely that the lower intensity of the interests at stake means that even those who have resisted adopting this model in organ donation would be able to implement it in the case of data.

8.2. Criticism

38. The main issue of an opt-out model on non-personal health data mainly relates to the limitations of consent as the legitimate basis for data processing. Sorbie has argued that there are a number of ethical issues in data donation due to the timing: 'the consent of live data donors to the posthumous collection and user of their data is held in stasis at the point they die (...) Given that consent to donation may come at any time prior to death, there is a considerable temporal disjuncture between the giving of consent and the use of the data; this even includes the act of collecting the data (to say nothing of its subsequent use in research) because these events will likely take place many years later'.[28] Furthermore, there are also issues related to the extent of the consent:

> it is probable that, both due to the passage of time and the breadth of the information contained within a donor's PMR [personal medical records], the data collected will subsequently be used in ways that simply cannot be anticipated at the point of consent (...) The disjuncture in timing between obtaining consent and the realization of value in data far beyond what could be anticipated at the time of consent should lead us to question seriously what informed consent could look like in these circumstances.[29]

39. However, although these objections are reasonable, they seem to be too closely linked to the idea of the need for consent to the processing of personal data, or more precisely, to special categories of personal data. As commonly known, in such circumstances, 'broad consent' is not easily applicable. The Article 29 Working Party has stated that 'when special categories of data are processed on the basis of explicit consent, applying the flexible approach of Recital 33 will be subject to a stricter interpretation and requires a high degree of scrutiny'.[30] Moreover, as Albena Kuyumdzhieva points out:

---

28 A. Sorbie, 'Medical Data Donation, Consent and the Public Interest After Death: A Gateway to Posthumous Data Use' in *The Ethics of Medical Data Donation*, pp 115-129.

29 *Ibid.*, p 120.

30 Article 29 Working Party Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017, As Last Revised and Adopted on 10 Apr. 2018, WP259 rev.01, p 29.

> the notion of broad consent should not be mistaken with the notion of blanket or open consent. The Guidelines on transparency, prepared by the Article 29 Data Protection Working Party 6 (2018: 9), explicitly note that statements such as "We may use your personal data for research purposes" are not compliant with GDPR as they do not provide sufficient information as to the type of the research that is to be carried out.[31]

40. Thus, extensive consent regarding personal data is clearly suspicious as a legal basis for data processing. However, in the case of non-personal data, our range of requirements regarding the legal basis for processing decreases considerably. Indeed, the Regulation on the free flow of non-personal data, which applies from 28 May 2019, is meant to stimulate data processing. To reach this aim, the EU legislature provides incentives for industry, with the support of the Commission, to develop self-regulatory codes of conduct on the switching of service providers and the porting of data.

41. Thus, one might absolutely conclude that the requirements for non-personal data processing are not at all as demanding as those imposed by the GDPR on personal data. It is therefore clear that the extent of consent should not be restricted in the same way for one type of data and another. In fact, appealing to the data subject's consent in the case of non-personal data would not make any sense because, by definition, they are data that cannot be linked to a data subject. The data of deceased people somehow constitute an anomaly in the system, because, being data that can be linked to a person, they are no longer personal data, as that person no longer exists (with the aforementioned exception of data that transmit information on living relatives).

42. It will of course be difficult to determine precisely which data are personal (from third parties) and which are not. Most medical records may contain both types of data. In such cases, it would be appropriate to follow the provisions of the Guidance on the Regulation on a framework for the free flow of non-personal data in the EU,[32] a Communication from the Commission to the European Parliament and the Council devoted to providing support on this issue. Mainly, it states that the data should be split into two different categories, personal and non-personal, and then follow the corresponding regulation. If this is not possible, we should

---

31 A. Kuyumdzhieva, 'Ethical Challenges in the Digital Era: Focus on Medical Research', in Z. Koporc (ed.), *Ethics and Integrity in Health and Life Sciences Research* (Emerald: Bingley 2018) pp 45–62.

32 Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union, Communication from the Commission to the European Parliament and The Council, Brussels, 29 May 2019, COM (2019) 250 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN (accessed 29 September 2021).

consider that the GDPR rules. In practice, this means, in our opinion, that medical records should be carefully examined to differentiate one data from another. Then, we should act accordingly, i.e., following the provisions of the deceased if the data only provide information about them, or according to the rules of personal data processing of the GDPR, if they are data concerning living relatives.

9. Conclusion

43. The legal regime for the data of deceased people presents multiple issues that hinder their use for biomedical research. The issue, as we have shown, is particularly complex because most medical records mix data that provide exclusive information on the deceased with data that also refer to their genetically related relatives. If the former are non-personal data according to the GDPR, the latter should instead be considered personal data, according to the same rule. Therefore, to be able to use these data in a reasonable manner, it is necessary to differentiate between both kinds of data, which follow very different legal frameworks. In the case of personal data, it would be necessary to follow the rules of the GDPR. In the case of non-personal data, it seems reasonable to opt for another alternative.

44. The PMDD initiative developed by Oxford is an attractive proposal that, however, suffers from shortcomings that make it less reasonable than other alternatives, such as a conscription model. The difficulties involved in obtaining the consent of people might provoke the loss of essential assets. Furthermore, it does not trace distinctions between personal and non-personal data, a perspective we find unacceptable. As an alternative, we propose a combination of an opt-out system for non-personal data and strict application of the GDPR if the personal data of living relatives are at stake. We are aware, however, that none of these proposals might substitute what would constitute an excellent solution: a regulation exclusively devoted to these data. In our opinion, this would be the optimal tool to give the final word on such a relevant issue.

Reprinted from European Review of Private Law (5), 2021, p. 785–806, with permission of Kluwer Law International. No commercial use of the publication should be involved.

.

This work was supported by PANELFIT, which has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.

This article reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.