

Can Data Accuracy Survive Someone's Death? A post-mortal privacy study

Isabela Maria Rosa^[0000-1111-2222-3333]

¹ Centre for IT & IP Law (CiTiP) at KU Leuven, 3000, Belgium

Abstract: As a general rule, fundamental rights cease with the death of the individual. Following this approach, the General Data Protection Regulation (GDPR) excludes personal data from deceased individuals from its scope of protection, leaving room for national law to extend aspects related to personal data protection beyond someone's life. This paper focuses on a normative question of whether the accuracy principle, central to the fundamental right to personal data protection, should be extended after the data subject's death. Accuracy is directly connected with the data subjects' right to rectification. As a purpose and context-based principle under the GDPR, accuracy imposes an obligation on controllers, who should keep personal data accurate and, when necessary, up-to-date for the purposes of processing. The right to rectification, on the other hand, serves as an instrument for the data subject to complete or correct inaccurate information about themselves. Based on the ideas behind the post-mortal privacy theory, the research concludes that accuracy should be imposed even after someone's death and instruments for rectification should be available for heirs to correct or complete at least factual information about someone who has already died.

Keywords: personal data protection; data accuracy; post-mortem privacy; right to rectification; human rights.

1 Introduction

Data accuracy is one of the guiding principles for personal data protection. [1-2] As an instrument to mitigate risks, accuracy, also known as data quality,¹ is part of the data protection tradition, being present in different data protection norms, [3-4] including the General Data Protection Regulation (GDPR). [5] The principle establishes obligations to controllers to maintain and process accurate and, when relevant, up-to-date personal data. It also serves as the basis for data protection rights, such as the rights to rectification, [2, 6] to objection,[1] and to exclusion. In the GDPR, accuracy is foreseen as a contextual category, [7] meaning that the data should be as accurate as needed for the purposes intended. Any inaccurate data for said purposes should be erased or rectified without delay.

¹ In this paper, data quality will be used as a synonym for data accuracy, since both connect to the argument of the research. However, for more on the possible differences between the two, see: Dimitrova, 2021 [2].

In parallel, as a rule, the fundamental right to personal data protection, in its personality right dimension and in civil law, does not apply to deceased people. [Recital 27, 5] Excluding this category from the scope of protection can be justified by the understanding that the dead cannot suffer direct harm and that personality ceases with someone's death. [8, pp. 3-5, in 9] Nonetheless, other arguments can be used for an opposite conclusion, meaning that at least certain aspects related to the right to personal data protection should be extended even after someone's passing.

Initially, one should have a level of control over their character, image, and story even after death, to protect their character and their own existence. [c.f., see brief conceptualization of autonomy in 8] Passing through the idea of autonomy and human dignity, [10] a person's personality should not be completely disregarded after their death. This is the reason behind certain personality rights being protected even after someone's death. Also, personal data related to living people can be inferred from datasets composed of personal data of deceased individuals. In this case, since inferred personal data from living people would be part of the dataset, data protection rules would apply. [11] In both cases, accuracy could be relevant. In the former, accuracy can be an instrument to guarantee control over one's memory – and personal data – even after their passing. In the latter case, accuracy can be important to confirm or deny the connections with the living and to protect them against discriminatory actions.

Nonetheless, considering the GDPR, accuracy obligations would cease with the data subjects' death, since the norm does not apply to the personal data of deceased persons. However, scholarly developments have defended the need to maintain certain data protection aspects even after someone's death, [8, 12, 13] and national data protection systems have extended the application of this right after one's death (e.g., Italy, or Iceland). [13-14] Withing these approaches, gaps remain in differentiating what aspects of personal data protections would still exist after someone's death. To better understand this, the post-mortal privacy theory becomes essential. As explained by advocates, [8, 15-18] post-mortem privacy entails the survival and protection of the informational body, constituted by personal data, digital remains, and other representations of the self, following sociological research around digital immortality and technological developments and considering aspects of autonomy and informational self-determination.

From this scenario, the study aims to understand if the data accuracy principle should apply, at least to a certain extent, after the death of the data subject, considering the contextual aspect of the accuracy principle. Throughout the paper, two use cases will be used to illustrate the research's relevance.

First, the research will explore how instruments for correcting official documents developed after forced disappearances and deaths in dictatorial regimes in Latin America already showcases the societal and individual importance of personal data accuracy even after someone's death. Second, in the Netherlands, a database regarding the prosecution of individuals who might have been involved with the Nazi regime could be made accessible to everyone, even via the internet. However, in the end, the responsible body decided to keep access restrictions. Two main factors influenced this conclusion. First, the database was deemed incomplete (or inaccurate). While it had files related to the prosecution of individuals, it did not contain information about the outcomes. Second, even though the majority of the data in the records was related to deceased

individuals, there could still be living persons portrayed in the documents or the data of the dead could affect living individuals by inference, which could be inaccurate. [19-20]

Using this example throughout the research, the paper will explore the possible extension of the principle of accuracy even after someone has died in three topics. First, the paper will explore the relevance of personal data protection of deceased persons, evolving from the post-mortem privacy theory. Next, an overview of the accuracy principle will be presented. Finally, the paper will conclude whether the data accuracy principle in the GDPR should apply after the data subject's death. On this, the research will tackle how the extension of the data accuracy principle can serve as a human rights instrument, even after the death of the data subject.

The paper adopts a legal normative perspective rather than a positive one to tackle the new challenges related to personal data protection. The central research question of the research is "Should the enforcement of the accuracy principle be extended after someone's death as a way to respect and preserve human rights? ".

While the research does not intend to be final, it will contribute to other relevant questions as the possibility of using someone's personal data after their death for reconstruction of their image via artificial intelligence (AI) for incompatible purposes to their way of living (e.g., alignment with brands they positioned themselves against, deepfakes), even when there is an approval of the surviving relatives or heirs. And, even though there might be other legal instruments to address the research problem, the article intends to explore the potential of data accuracy as another solution to the situation.

2 Post-mortem personal data protection

Respect for the dead is shared among cultures. Each country or group may have their own rituals and beliefs, but the need for respect for one's dignity even after their death is a shared understanding represented in diverse manners. Even though human and/or fundamental rights are commonly connected with the idea of human dignity, in civil law, as a general rule, fundamental rights only apply to living people. Justifications for this approach rely on the fact that only a living person can suffer harm and, for that, all rights should be terminated with their death. [8, 21]

Nonetheless, in specific circumstances, certain rights are extended even after someone's death, especially to protect the dignity of the individual or of their family. For example, jurisdictions share a notion of needing to investigate unlawful killings and to establish certain rules for the disposal of human remains. [22] In various jurisdictions, economic rights related to digital assets containing personal data may be considered of economic value and can be passed on to heirs, including intellectual property. [23-24] Brazil penalises imputing a false crime to someone, even after their passing, [art. 138, 25] and there are criminal sanctions foreseen for actions against respecting the dead. [arts. 209-212, 25] India's right to live with dignity has also included the dead. [26] In a landmark decision, the German Federal Constitutional Court reaffirmed that the

certain aspects of the right to privacy remain after the death of someone, also to protect it from gross distortions of their life's story. [27]

Also, regardless of the existing limitations, international human rights law has understood the importance of respect and dignity even after someone's death, [22, 26] recognising that the right to privacy also contains obligations to protect dead persons and their remains. [22] However, there is no harmonised approach under human rights law on how to extend or not these rights for the deceased. With this, big discrepancies between jurisdictions and approaches remain, which is accentuated by the digital lives and remains that individuals now possess. [22]

Under EU law, the scenario is similar. As a rule, fundamental rights cease with someone's death. The possibility of extending fundamental rights after the death of an individual is left to the discretion of Member States, which may adopt laws on the matter. However, scholars defend the possibility and need of extending certain personality rights, including privacy, to after someone's death, to preserve their reputation and dignity. [18] This debate gained even more traction with new technologies that facilitate the creation of an immortal digital trace and body. [On the immortal body, see, c.f., 17 and 28] Lack of harmonised regulation at the EU level may leave the power of decisions over these digital assets in the hands of the data controllers. For instance, at the moment, social media accounts legacy and what can be done with them after the death of their owners is mainly defined by the companies responsible for such platforms. [29]

The same logic applies to personal data protection. In general and under EU law, the right does not apply to deceased individuals. Nevertheless, certain scenarios could or should lead to the application of the right even after someone's death. [pp. 22-23, in 11] As already recognised by the old Working Party 29, the right to personal data protection and the GDPR may apply if it is not possible to know if the data subject is alive or not. Also, processing personal data of deceased individuals may affect the rights and interests of living individuals. In other words, using personal data from a deceased person may implicate processing information about a living individual by inferences made from the deceased's information, which requires compliance with data protection rules. [pp. 22-23, in 11] The same logic applies if the personal data contained in a dataset or document is also directly connected to a living person, where personal data protection rules would apply normally. [30] Another scenario of post-mortem personal data protection happens when national law extends the right to personal data protection to after someone's passing. [31]

Discussions remain on whether personal data protection should have effects in other situations not explicitly recognised by the EU legal framework. For instance, there are no legal recognition of a EU personal protection whenever characteristics of the processing itself could affect aspects protected even after someone's death, such as dignity and autonomy. In the next paragraphs, the paper will showcase how research on post-mortem privacy has already showcased that having a level of control over how your personal data is managed, even after your passing, is essential for keeping a fair and dignified maintenance of your memory, while also preserving relevant information for collective memory.

This is a social need, highlighted by the digitalisation of memory and information. As showcased by research conducted in France at the end of 2024, more than half of

the respondents (52%) would like to have their own content erased after their death. Another 26% would like to have it at least partially curated. [32] This illustrates a societal claim for solutions that allow for control of their personal data, even after their passing, especially considering the preservation allowed by digitalisation.

To respond to this legal and social need to understand how and if personal data protection should apply after one's death, different theories about post-mortem personal data protection have been developed in the last two decades. Their main focus related to digital assets management, [33-36] or information privacy literature. [8, 12] These theories are commonly explored under the umbrella of post-mortem privacy rather than personal data protection. However, they tackle discussions about control, autonomy and dignity, showcasing a connection with personal data protection as well. Different studies on post-mortem privacy recognise that a level of protection of someone's personal data protection right, even after someone's death, reflects the human right to dignity and the idea of autonomy. [c.f., 8, 9, 12, 13, 37]

Actually, post-mortem privacy is broader than post-mortem personal data protection, but the former also encompasses the latter. [12] On these lines, it is important to note that post-mortem data protection in this paper will enjoy the developments of post-mortem privacy, following the human rights-based approach proposed by Harbinja. [12] This approach can lead to solutions that preserve dignity and autonomy, which also serve as a remedy for the protection of the right to personal data protection.

Building from her initial studies, Harbinja proposes the idea of a postmortal privacy framework, which is broader than post-mortem privacy. As she explains, "Postmortal privacy is qualitatively different from post-mortem privacy. As seen above, the latter in legal scholarship has relied on the legal conceptions of personality, data protection and privacy, with normative considerations of privacy, autonomy and testamentary freedom. The postmortal privacy framework goes beyond post-mortem privacy and includes protecting the informational body and aspects of digital immortality. [p. 25, in 12] The broader definition aligns with other studies on the matter. Buitelaar, for instance, defines post-mortem privacy as "the right of a person to preserve and control what becomes of his reputation and dignity after death." [18]

From this, one can already take from previous studies on post-mortem privacy that a certain level of control over someone's personal data, protecting their digital bodies, reputation, and dignity, should exist even after their death as a way to preserve human rights. Solutions for control over one's personal data after their death can come in different forms, including technical measures, policies or legal instruments, and even market solutions. [17, 31] Focusing on how the law could be adapted, the next chapters will explore whether post-mortem data accuracy would be a relevant instrument for that.

3 Accuracy in personal data protection

Before evaluating its significance post-mortem, the principle of accuracy in personal data protection law in the EU will be conceptualised. Data accuracy is part of the majority of legal instruments related to personal data protection, from international law to national frameworks. Its conception can be dated back to the 60s, from discussions on

data quality in information systems, or to the FAIR information principles in the 1970s and its content has not changed significantly since then. [1] It connects directly to the ideas of autonomy and control over one's personal data use, connecting with ideas of informational self-determination and human dignity.

The principle was developed to impose obligations on the actors processing personal data, not for the data subjects, serving as a tool to create more equality in the power imbalance between the individuals and controllers. [7] In other words, the accuracy principle imposes an obligation on the data controller to "take every reasonable step to ensure respect" of this principle, without delay. [38] As defined by the GDPR, accuracy entails that personal data shall be "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay." [Article 8 GDPR, 5]

Accuracy imposes an additional requirement on any personal data processing, regardless of any action from the data subject. [1] But, at the same time, the principle serves as a basis for different remedies offered to the data subjects to have more control over their data. Under the GDPR, this relies on the rights to restriction, rectification, [39], and, to a certain extent, erasure.

Rectification is the right most commonly associated with the principle of accuracy. The right to correct incomplete or inaccurate personal data is central to different approaches to personal data protection. Rectification is, alongside the right to access, the only right already foreseen in the European Charter of Fundamental Rights (Charter) as part of the fundamental right to personal data protection. Under the Charter, "[e]veryone has the right of access to data which has been collected concerning him or her, and the right to have it rectified." [Article 8 of the Charter, 40]

Under the GDPR, the right to rectification is defined as the "right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement." [Article 16 GDPR, 5]

It is undeniable that the accuracy principle, then, applies to all data protection processing activities. [1, 41] It serves as a mirror to the rectification rights foreseen in the Charter. Both the principle and the right are reflections of each other. And, it is exactly the scope of the accuracy principle that defines the scope of the right to rectification. [1] However, the scopes are not identical. The principle's definition only mentions the accuracy and up-to-datedness of the data, not highlighting completeness. On the other hand, the right to rectification provides the data subject with the possibility to change incomplete data with additional information.

From this, one can understand that the data controller cannot process additional, unnecessary personal data for the purpose, solely to ensure the completeness of the information. Otherwise, the controller would be going against the principle of data minimisation. Rather, the data controller is obliged to actively ensure that just enough information is being processed for an accurate representation of the data subject for the purpose intended. On the other hand, the data subject, by exercising their right to rectification, can offer additional information to the controller to guarantee the completeness

of the information. This interpretation aligns with the essence of the fundamental right to personal data protection. [42] As mentioned, under the Charter, everyone has the right to rectify the personal data collected concerning him or her. At the same time, data should be processed fairly for specified purposes, which would include alignment with personal data protection principles, including minimisation and accuracy. [Article 8 GDPR, 5]

Until now, however, EU data protection law and case law do not provide sufficient precision when working with concepts related to accuracy, up-to-datedness, and completeness. This can be due to the fact that defining what is accurate and what can or should be rectified is not always easy.

A major challenge addressed in the legal literature and case law is the application of the accuracy principle to opinions. Unlike factual information, opinions cannot be proven. Opinions are normally based on inferences. They can result from different forms of information handling, including human- or algorithm-based inferences, [1, 43, 44] exactly because of the lack of evidential facts, some believe that opinions should not be under the scope of the accuracy principle. According to this line of thought, it would be impossible to prove something non-factual. [41] Divergence about this application still exists. For instance, the EDPS stated that “[T]he right to rectification only applies to object and factual data, not to subjective statements (which, by definition, cannot be factually wrong).” [39] However, others defend exactly the opposite, mentioning how the accuracy principle and connected rights should be extended to opinions. [c.f., 1]

Another challenge is due to the fact that individuals can be in favour of a level of inaccuracy in their data. Inaccurate information can serve as a remedy to protect their fundamental rights and shield disproportionate interference in their personal lives. [7] Or, sometimes, recording the mistake itself is important for accuracy. [45] There are also cases where the data subject is unaware of the processing or has already passed, making it way more challenging for the exercise of the rights connected to the accuracy principle.

Regardless of these discussions, it is mainly accepted that the accuracy principle is a contextual and purpose-based provision. This means that the level of accuracy required depends on the purpose of the collection and processing.[44] When using personal data, controllers must consider the different rights and interests involved, keeping in mind that accuracy is not absolute. [1]

Another less controversial aspect of accuracy and rectification is how they serve as instruments for self-determination, offering control mechanisms on how someone is represented in the digitalised world, serving to preserve their own autonomy and dignity. Personal data protection serves as a control instrument for how one's personal data is used and how their information body is constructed, and accuracy is central to this.

Accordingly, the Court of Justice of the European Union (CJEU) has already confirmed that personal data accuracy should be verified in light of the purpose of the processing. In a case analysed by the Court, it was evaluated whether presenting proof about a gender reassignment surgery would be necessary for the data subject to be able to have a different gender than the one assigned in their birth document in official records. In its evaluation, the Court understood that the purpose of the processing was to

identify someone. Because of that, it was more relevant and accurate to have information about that person's gender identity at the time of registration than the one assigned to them at birth. Proof about a gender reassignment surgery was deemed not necessary for the purposes intended, also because other supporting documents about their current gender were presented. [46]

In another instance, during the Google Spain case, the CJEU analysed whether the data subject would have a right to have information about them delisted from the results of a search engine. In this case, the information about the data subject was accurate. With the passage of time, nonetheless, the personal data was no longer relevant for the purposes intended. Negative effects on the data subject also played a role in the Court's decision to confirm a right to delisting the personal data in question from the results of the search engine. [41]

These examples in EU case law illustrate the close relationship between personal data accuracy, context, and purpose. At the same time, in both cases, the self-determination of the data subject was taken into consideration. How the data subject would like to be perceived also played a role in defining possibilities and limits to the processing. Considering this and applying data accuracy to the post-mortem personal data protection framework, the next chapter will tackle whether data accuracy should be extended after someone's death to serve as a human rights instrument.

4 Post-mortem accuracy as a human rights instrument

Incompleteness or inaccuracy of someone's personal data may lead to serious consequences for how this person is understood. Consequences may be individual, such as not being able to get a job, or societal, such as not being able to identify the suspect of a crime. In similar notes, having information about someone being investigated for a crime but not having the final result may lead to the unfair understanding that they were involved in said criminal activity. Incompleteness, in this case, may lead to unfair inferences or incorrect opinions. Similarly, in case someone is wrongfully identified in a judicial case and this is not corrected, the rest of society can have a wrongful impression of the individual based on inaccurate information. And, preserving this inaccurate portrait of reality may lead to misrepresentations of historical events and societal developments.

A real example of these risks is what happened in Latin America, where several victims who died under the responsibility of the dictatorial regimes between the 50s and the 80s did not have accurate information in their death certificates. Initially, a large part of these deaths were reported as disappearances. Once their deaths were confirmed, the reason for the passing added in official documents was, a lot of times, incorrect or incomplete. To guarantee the historical accuracy of the information, different activists and surviving relatives fought (and still fight) for remedies. [c.f., 47] After the reestablishment of democratic governments, countries like Brazil and Argentina have created mechanisms for the inaccurate information to be updated and corrected. Brazil established obligations to the notaries to correct death certificates of those who were murdered or disappeared under the power of the State, based on the conclusions of the

national truth commission. [48-49] Argentina has already rectified the death certificates of victims of the dictatorial regime and the federal government maintains an unified database with information about the victims. [50-51] Beyond the importance of these actions for the preservation of human rights and history, the accurate information can also be further used for reparation and liability procedures.

In connection with these experiences, with the increase of forced disappearances, the human right to the truth emerged.² Initially developed in scenarios of transnational justice, [52] the scope of the right has expanded. [53] Currently, the right to truth is seen as an instrument for victims and surviving relatives to receive information about gross human rights [54] and the remains of deceased victims, [22] rectify official information to translate the truth better, receive compensation for these illegitimate acts, and other aspects related to human rights violations. [52]

While the research does not focus on detailing the right to truth,³ this human right serves as a living example of the importance of correct information retention for both individual and collective memory keeping, serving aspects of human dignity and access to information, even after the death of the person documented. Actually, it showcases how aspects related to personal data accuracy are already part of the human rights system. In these scenarios, the State had to act to find solutions to correct the official information created and held by them. In parallel, instruments were offered to surviving relatives or other representatives of the deceased data subjects to rectify incomplete or inaccurate data about the victims killed by the regimes. Guaranteeing the accuracy of personal data, even after someone's death, can then serve similar goals as the rights to truth, human dignity, and access to information.

Another example of the importance of post-mortem accuracy can be found in historical documents. A case in the Netherlands can exemplify the challenges related to this scenario. A database controlled by the National Archives containing information about individuals who were investigated for connections with the Nazi regime during World War II was to be made accessible to anyone via an online platform. However, the files only contained information about the beginning of the investigation, without details about the outcomes of the procedures and whether they were really implicated in the dictatorial regime. It was impossible to determine whether all data subjects were already deceased. Additionally, it was assessed that identifying living individuals by inferences based on those files was possible. To protect and mitigate the interference with the right to personal data protection, safeguards were put in place. Instead of general access to the content, these datasets could only be accessed via specific tokens, with more control of the person accessing them and possible re-use. [19-20]

² Historically, the right to truth is also connected to the Additional Protocol I to the Geneva Conventions. It can be connected or differentiated from the right to know and right to memory. See in United Nations, 2006 [53] .

³ Under the EU human rights system, the right to truth is connected to the other human rights like the right to effective remedy, or prohibition to torture or ill-treatments. In the American, United Nations, and in national frameworks, the right to truth has also been connected with the right to freedom of information. [53] While it has been connected with the right to family, the right to truth is not commonly linked to the right to privacy or personal data protection.

Archives are one of the central institutions for memory keeping, both for collective and for individual perspectives. These purposes are, a lot of the times, set via a public mandate to appraise the historical data and make it as accessible as possible to the public. Digitalisation brought new opportunities for accessibility and maintenance of information. Archival institutions handle constantly large amounts of personal data, including of deceased individuals. However, assessing whether someone is dead, based on the information received by the archives, is not a trivial chore. Commonly, archives are solely the recipients of personal data, and do not maintain direct contact with the data subject. Also, various archival databases or documents are incomplete, creating challenges to the direct identification of an individual.

Recognising the complexity task of personal data within archives, the GDPR created a privileged system for these institutions. [55] Flexibilities relating to data subjects' rights, controllers' obligations, and even data protection principles are set to bodies archiving personal data in the public interest. National law can also establish new derogations on different topics for personal data processing for archiving purposes. [Article 89(1) GDPR, 5] However, no privilege or possibility of derogation is set on data accuracy. Meaning, the data accuracy principle applies fully to archiving activities involving personal data.

What this paper proposes is that the post-mortem privacy theory should also be considered by archives and should include data accuracy as a human rights instrument. The Latin American and the Dutch cases illustrate how data quality is of utmost importance for memory keeping and historical purposes. Whenever this cannot be guaranteed, other additional safeguards related to personal data should be put into place. Therefore, to the extent possible, data accuracy should survive even after one's death. Data accuracy, as a purpose-based principle, could serve as a limiting instrument to further re-use of one's personal information. Meaning, even after the death of the individual, their personal data should not be applied in contexts incompatible with their lives.

Post-mortem accuracy would also create space for the correction or completeness of personal data maintained by different actors. Representatives or heirs should have instruments to complete or correct personal data of deceased individuals. For instance, when deceased artists or public figures should be protected from their life and work, the heirs or representatives could rely on their own personality rights [56] or in the protection provided by post-mortem accuracy. In other words, data accuracy should continue to create obligations to data controllers even after the death of the data subject. For this, accuracy should continue to be evaluated withing the purpose of the processing intended. Extending the data protection principle to after someone's death would preserve their autonomy and fundamental right to human dignity.

On these lines, a post-mortem processing activity that goes against proven facts should be considered illegitimate, unless this is done in a manner to complete the context of the factual truth via annotations and changes in the document to demonstrate the bigger picture. Following the perspective of protection of the information body in the theory of postmortal privacy, amplifying the data accuracy principle after someone's death would also serve as a limitation for re-creating someone's image in contexts where they were never in before. In this sense, the fact that accuracy is contextual also helps us to reach the same conclusion. Since personal data should be accurate in relation

to its context, any further use for unrelated or incompatible purposes could be inaccurate, [7] and, thus, illegitimate.

As the principle of data accuracy imposes obligations on the data controllers, they should do everything possible to ensure that their processing activities solely use accurate information for the defined purposes. As a mirror of this obligation, heirs and other legitimate representatives should be able to exercise rights related to the data accuracy principle, i.e. rights to rectification, objection, or erasure. Further research is still needed on how post-mortem accuracy could or should apply to opinions. However, based on human rights experiences and approaches, factual accuracy should be preserved even after someone's death as a personal data protection instrument.

Conclusions

Personal data protection is a fairly recent fundamental right. It creates minimum grounds for a fair processing, establishing principles and creating obligations to data controllers, while also empowers data subjects with rights and instruments to have more control over their data. One of the central components of this right is the principle of data accuracy, which is directly connected to the data subjects' right to rectification. These elements guarantee that solely accurate data should be processed for the purpose intended, at the same time that the data subject is empowered with remedies to complete or correct their personal data being processed.

As a general rule, the scope of personal data protection in a EU level has only encompassed living individuals. However, considering the risks of affecting living persons, the right has already been extended in certain circumstances to datasets containing personal data of deceased people. Also, the EU frameworks allows for Member States to extend this right post-mortem. With new technologies and considering different contexts, the post-mortem privacy theory has developed a framework that sustains that certain aspects of the right to personal data protection should be extended also for the dead, serving as an instrument for autonomy, dignity and human rights.

This paper analyses how the data accuracy principle can serve this purposes, especially when dealing with historical factual data and human rights violations. By responding to a normative question of how the right should be applied, it concludes that the right to personal data protection should be interpreted in light of the post-mortem privacy. With this interpretation, the accuracy principle should have post-mortem effects, imposing obligations to the data controllers and offering instruments of rectification to heirs and representatives, in line with experience in international and national law.

References

- [1] Dara Hallinan and Frederik Zuiderveen Borgesius, 'Opinions Can Be Incorrect (in Our Opinion)! On Data Protection Law's Accuracy Principle', *International Data Privacy Law* 10, no. 1 (2020).

[2] Diana Dimitrova, ‘The Rise of the Personal Data Quality Principle: Is It Legal and Does It Have an Impact on the Right to Rectification?’, *European Journal of Law and Technology* 12, no. 3 (2021).

[3] Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (Privacy Principles) (1980).

[4] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) (1981).

[5] 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) (Text with EEA Relevance) (2016).

[6] Elisabetta Biasin, ‘Why Accuracy Needs Further Exploration in Data Protection’, 2021, 1–7.

[7] Gloria González Fuster, ‘Inaccuracy as a Privacy-Enhancing Tool’, *Ethics Information Technology* 12 (2010): 87–95.

[8] Edina Harbinja, ‘Post-Mortem Privacy 2.0: Theory, Law, and Technology’, *International Review of Law, Computers & Technology* 31, no. 1 (2017): 26–42.

[9] At the opposite end, on the possibility of post-mortem harm, see, c.f.: Marieke A. R. Bak and Dick L. Willems, ‘Contextual Exceptionalism After Death: An Information Ethics Approach to Post-Mortem Privacy in Health Data Research’, sect. 32, *Science and Engineering Ethics* 28 (August 2022), <https://doi.org/10.1007/s11948-022-00387-0>.

[10] Ralf Poscher, *Human Dignity as a Value and a Right*, MPI-CLS Working Papers 2024/01 (Max Planck Institute, 2024).

[11] Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, no. 4/2007 (Article 29 Working Party, 2007), <https://www.pdp.ie/docs/1030.pdf>.

[12] Edina Harbinja, ‘Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be The Potential Alternatives?’, *SCRIPTed: A Journal of Law, Technology & Society* 10, no. 1 (2013), <https://doi.org/10.2966/scrip.100113.19>.

[13] Fabio Queiroz Pereira and Mariana Alves Lara, ‘A legislação de proteção de dados e a tutela dos dados pessoais post mortem: uma análise comparativa entre o direito brasileiro e o direito italiano’, *Revista Brasileira de Direito Civil* 33, no. 4 (2025): 39–55, <https://doi.org/10.33242/rbdc.2024.04.003>.

[14] White & Case, *GDPR Guide to National Implementation: Iceland*, n.d., accessed 1 February 2025, <https://www.whitecase.com/insight-our-thinking/gdpr-guide-national-implementation-iceland>.

[15] Lilian Edwards and Edina Harbinja, ‘Protecting Post-Mortem Privacy: Reconsidering the Privacy Interests of the Deceased in a Digital World’, *SSRN Electronic Journal*, ahead of print, 2013, <https://doi.org/10.2139/ssrn.2267388>.

[16] Edina Harbinja and Henry Pearce, ‘Your Data Will Never Die, but You Will: A Comparative Analysis of US and UK Post-Mortem Data Donation Frameworks’, *Computer Law & Security Review* 36 (April 2020): 1–13, <https://doi.org/10.1016/j.clsr.2020.105403>.

- [17] Edina Harbinja, *Digital Death, Digital Assets and Post-Mortem Privacy* (Edinburgh University Press, 2023).
- [18] J. C. Buitelaar, 'Post-Mortem Privacy and Informational Self-Determination', *Ethics and Information Technology* 19, no. 2 (2017): 129–42, <https://doi.org/10.1007/s10676-017-9421-9>.
- [19] Puck Huitsing and Marianne Loef, *De Oorlog Online: Handreiking Voor Het Online Beschikbaarstellen van Archieven Uit En over de Tweede Wereldoorlog*, ed. Ellen Bouma (Consortium Oorlog voor de Rechter, 2024).
- [20] Anna Berlee, 'Persoonsgegevensbescherming Na Overlijden', *Rode Draad: Digitale Nalatenschap* 8 (2025): 272–85.
- [21] For more on the history of the non-inclusion of deceased individuals under the scope of the right to personal data protection in the EU see, c.f.: David Erdos, *Dead Ringers? Legal Persons and the Deceased in European Data Protection Law*, no. 21/2020, Legal Studies Research Paper Series (University of Cambridge - Faculty of Law, 2020).
- [22] Morris Tidball-Binz, *Protection of the Dead*, Promotion and Protection of All Human Rights, Civil, Political, Economic, Social and Cultural Rights, Including the Right to Development (Human Rights Council, 2024), https://doi.org/10.1163/2210-7975_HRD-9970-2016149.
- [23] 17 U.S.C. §201(d)(1) of the Copyright Act of 1976 in the United States of America.
- [24] European Parliamentary Research Service (EPRS), *Copyright Law in the EU: Salient features of copyright law across the EU Member States*, 06/2018, [https://www.europarl.europa.eu/Reg-Data/etudes/STUD/2018/625126/EPRS_STU\(2018\)625126_EN.pdf](https://www.europarl.europa.eu/Reg-Data/etudes/STUD/2018/625126/EPRS_STU(2018)625126_EN.pdf)
- [25] Decreto-Lei n. 2847, de 7 de Dezembro de 1940 (Código Penal Brasileiro/Brazilian Penal Code), art. 138.
- [26] Anjli Parrin et al., 'The Protection of Dead Persons under International Human Rights Law: Evaluating Gaps and Developing a Principles Framework', *International Review of the Red Cross* 107, no. 929 (2025): 724, <https://doi.org/10.1017/S181638312510074X>.
- [27] BvR 435/68, Vorher: Az. I ZR 44/66 (BVerfG 24 February 1971).
- [28] Stefano Rodotà, *A Vida Na Sociedade Da Vigilância - A Privacidade Hoje* (Renovar, 2008)
- [29] Ondrej Hammulak et al., 'The Contemporary Issues of Post-Mortem Personal Data Protection in the EU after GDPR Entering into Force', *CYIL* 11 (2020): 225–38.
- [30] European Data Protection Board, *Guidelines 01/2022 on Data Subject Rights - Right of Access*, no. 01/2022 (2022), 29, https://www.edpb.europa.eu/system/files/documents/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf.
- [31] For example, in accordance with Article 85 of the French Data Protection Act, any data subject may define guidelines on how their personal data should be managed. This can be done in a specific manner, relating to one defined controller, or in a general form, related to all personal data of the individual. When no guidelines are provided, heirs may access data necessary for specific purposes or that are important to family memories, and have certain management powers. CNIL, *Our Data After Us: From*

Digital Death to Immortality, Uses and Issues of Post Mortem Data, IP Report - Innovation & Foresight 10 (2025), https://www.cnil.fr/sites/default/files/2025-11/cnil_10th_ip_report.pdf.

[32] Marin Biéri, ‘Enquête : Les Français et Les Données Post Mortem’, *Laboratoire d’Innovation Numérique de La CNIL*, 15 October 2025, <https://linc.cnil.fr/enquete-les-francais-et-les-donnees-post-mortem>.

[33] Jamie P. Hopkins, ‘Afterlife in the Cloud: Managing a Digital Estate’, *Hastings Science and Technology Law Journal* 5, no. 2 (2013), https://repository.uchastings.edu/hastings_science_technology_law_journal/vol5/iss2/1.

[34] Jeehyeon Lee, ‘Death and Live Feeds: Privacy Protection in Fiduciary Access to Digital Assets’, *Columbia Business Law Review*, 2015, 654–704.

[35] Laura Schertel Ferreira Mendes and Karina Nunes Fritz, ‘Case Report: Corte Alemã Reconhece a Transmissibilidade da Herança Digital’, *RDU* 15, no. 85 (2019).

[36] M. M. M. van Eechoud et al., *Data Na de Dood - Juridische Aspecten van Digitale Nalatenshappen* (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2021).

[37] Natasha Chu, ‘Protecting Privacy after Death’, *Northwestern Journal of Technology and Intellectual Property* 13, no. 2 (2015): 255–76.

[38] Cécile de Terwangne, ‘Article 5. Principles Relating to Processing of Personal Data’, in *The EU General Data Protection Regulation (GDPR): A Commentary*, Online, ed. Christopher Kuner et al. (Oxford University Press, 2020), 317, <https://doi.org/10.1093/oso/9780198826491.003.0031>.

[39] European Data Protection Supervisor, *Guidelines on the Rights of Individuals with Regard to the Processing of Personal Data* (European Data Protection Supervisor, 2025).

[40] Charter of Fundamental Rights of the European Union, 2000/C 364/01 (2000), https://www.europarl.europa.eu/charter/pdf/text_en.pdf.

[41] *Google Spain v. AEPD and Mario Costeja González* (Case C-131/12) (Court of Justice of the European Union 13 May 2014), <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131>.

[42] Court of Justice of the European Union, ‘Press Release No. 34/25: GDPR and Transgender Identity: The Rectification of Data Relating to Gender Identity Cannot Be Made Conditional upon Proof of Surgery’, Press Release, 13 March 2025.

[43] Stephanie Rossello, ‘The Rectification of Opinions in Dutch Data Protection Law: A Brief Historical Inquiry’, *Journal of Intellectual Property, Information Technology and Electronic Commerce* 16, no. 2 (2025).

[44] *Nowak v. Data Protection Commissioner* (Case C-434-16) (Court of Justice of the European Union 20 December 2017).

[45] Information Commissioner’s Office, ‘Principle (d): Accuracy’, *A Guide to the Data Protection Principles*, n.d., accessed 23 July 2026, <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/accuracy/#mistakes>.

[46] *Case C-247/23 (Deldits), VP v Országos Idegenrendészeti Főigazgatóság* (Court of Justice of the European Union 13 March 2025).

[47] Simone Machado, 'Ditadura: correção de vítimas é reparo histórico', *DW* (09 October 2025), <https://www.dw.com/pt-br/corre%C3%A7%C3%A3o-de-certid%C3%B5es-de-%C3%B3bito-da-ditadura-%C3%A9-repara%C3%A7%C3%A3o-hist%C3%B3rica/a-71928484>

[48] Jornal Nacional, 'Cartórios de todo o país começam a emitir certidões corrigidas de vítimas da ditadura', *GI*, (07 January 2025), <https://g1.globo.com/jornal-nacional/noticia/2025/01/07/cartorios-de-todo-o-pais-comecam-a-emitir-certidoes-corrigidas-de-vitimas-da-ditadura.ghtml>

[49] Brasil, Conselho Nacional de Justiça, *Resolução N° 601, de 13/12/2024, dispõe sobre o dever de reconhecer e retificar os assentos de óbito de todos os mortos e desaparecidos vítimas da ditadura military* (DJem 16 December 2024)

[50] Vitor Nuzzi and Eduardo Reina, 'Justiça Argentina retifica atestado de óbito do pianista brasileiro assassinado durante a ditadura', *Estadão* (08 November 2025), <https://www.estadao.com.br/cultura/musica/justica-argentina-retifica-atestado-de-obito-do-pianista-brasileiro-assassinado-durante-a-ditadura/>

[51] Argentina, 'Registro Unificado de Víctimas del Terrorismo de Estado' (Archivo Nacional de la Memoria, n/d), <https://www.argentina.gob.ar/derechos-humanos/ANM/rutve>

[52] Patricia Naftali, 'The "Right to Truth" in International Law: The "Last Utopia"?', in *Law and Memory. Towards Legal Governance of History* (Cambridge University Press, 2017).

[53] United Nations, *Promotion and Protection of Human Rights. Study on the Right to the Truth. Report of the Office of the United Nations High Commissioner for Human Rights.*, E/CN.4/2006/91 (2006), 5–6.

[54] United Nations, *International Day for the Right to the Truth Concerning Gross Human Rights Violations and for the Dignity of Victims (24 March)*, n.d., accessed 6 December 2024, <https://www.un.org/en/observances/right-to-truth-day#:~:text=The%20right%20to%20the%20truth%20implies%20knowing%20the%20full%20and,as%20the%20reasons%20for%20them.>

[55] Laura Drechsler and Charlotte Somers, 'Article 89. Safeguards and Derogations Relating to Processing for Archiving Purposes in the Public Interest, Scientific or Historical Research Purposes or Statistical Purposes', in *Compilation from The EU General Data Protection Regulation: A Commentary*, 2nd edn, ed. Christopher Kuner et al. (Oxford University Press, 2025).

[56] Yaniv Benhamou, 'Posthumous Replications: Rights and Limitations, Notion of Original and Copies', *Kunst & Recht 2017* (Bern) 16 (June 2017): 149–68.