The Right to be Forgotten in the European Union Public Sector: Balancing Individual Privacy and Public Interest

Avrupa Birliği Kamu Sektöründe Unutulma Hakkı: Bireysel Gizlilik ile Kamu Yararı Arasındaki Dengenin Sağlanması

Ahmet KÜÇÜK*

Abstract

The study addresses the conflict of rights between the right to be forgotten and the public interest in the public sector. The legal foundations and legal status of the right to be forgotten under the GDPR have been examined, focusing on how right to be forgotten is balanced with the important safeguard of public interest in the public sector, whether one of these rights predominates, the balance between them, and the limits of these two rights. Additionally, practical situations have been assessed through case studies in the fields of health and security. The research also discusses the ethical and legal considerations of data retention versus data deletion in the public sector within the context of the European Union, emphasizing the importance of balancing these two approaches. The study highlights significant legal and ethical approaches regarding the implementation of the right to be forgotten in the public sector, both in terms of protecting individual rights and safeguarding the public interest. In this context, an attempt has been made to establish the balance between the right to be forgotten and public interest, along with recommendations on how improvements can be made.

Keywords

Right To Be Forgotten, Public Interest, GDPR, Individual Privacy, Public Sector

Öz

Bu çalışma, kamu sektöründe unutulma hakkı ile kamu yararı arasındaki hak çatışmasını ele almaktadır. GDPR kapsamında unutulma hakkının yasal temelleri ve hukuki statüsü incelenmiş olup, kamu sektöründe kamu yararı gibi önemli bir güvencenin nasıl bir dengeleme sürecinde olduğu, bu iki haktan birinin ağır basıp basmadığı, aralarındaki denge ve bu iki hakkın sınırları değerlendirilmiştir. Ayrıca, sağlık ve güvenlik alanlarında örnek olay incelemeleriyle pratikteki durum da değerlendirilmiştir. Araştırmada, Avrupa Birliği bağlamında kamu sektöründe veri saklama ile veri silme arasındaki etik ve hukuki değerlendirmeler de ele alınarak, bu iki yaklaşımın dengelenmesinin önemi vurgulanmıştır. Araştırma, unutulma hakkının kamu sektöründe uygulanmasının hem

Hakemli Araştırma Makalesi / **Makale Geliş Tarihi:** 02.08.2025 – **Makale Kabul Tarihi:** 22.09.2025.

Atıf: Ahmet KÜÇÜK 'The Right to be Forgotten in the European Union Public Sector: Balancing Individual Privacy and Public Interest' (2025) 3(2) TRÜHFD 321-361.

* MA Candidate, Dublin City University Data Protection and Privacy Law, ahmet.kucuk2@mail.dcu.ie, ORCID: 0009-0004-6246-3446.

bireysel hakların korunması hem de kamu yararının gözetilmesi açısından önemli hukuki ve etik yaklaşımları ele almaktadır. Bu bağlamda, unutulma hakkı ile kamu yararı arasındaki denge ortaya konmaya çalışılmış ve nelerin nasıl geliştirilebileceğine dair önerilerde bulunulmuştur.

Anahtar Kelimeler

Unutulma Hakkı, Kamu Yararı, GDPR, Bireysel Gizlilik, Kamu Sektörü

INTRODUCTION

In the digital age, the amount of personal data collected, stored and used by public institutions is steadily increasing. Public sector bodies are increasingly digitizing their systems and considering that many public services have already transitioned or are in the process of transitioning to digital platforms. Personal data in the public sector is increasingly being digitized. The transformation, the protection, confidentiality and accountability of public institutions have become crucial for ensuring personal data protection.

One of the most significant advancements in data protection law is the right to be forgotten, as established under the General Data Protection Regulation (GDPR). The right to be forgotten grants individuals the capacity to request the erasure of their personal data under certain conditions. The right enhances individuals' control over their digital identities. While it is a right predominantly applied in the private sector, its implementation in the public sector holds considerable importance from legal, practical and ethical perspectives.

The public sector holds important data in areas such as healthcare, education, taxation, security, national security and justice to serve the public interest. These institutions retain data for long periods to fulfil legal obligations, ensure the continuity of services and serve society. In the context of applying the right to be forgotten within the public sector a key question concerns the extent to which right can be effective when balanced against actions undertaken in the public interest.

The research aims to examine the application of the right to be forgotten in the public sector and analyse the relevant legal decisions in this field. It seeks to explore how the right to be forgotten is balanced with the public interest, the priority of each, the extent of potential conflicts and whether one right can take precedence over the other.

The labour defines the legal framework of the right to be forgotten and trace its development from past to present. A detailed analysis of the landmark Google Spain case which

plays a critical role in shaping this right. It will assess the legal definition and scope of public interest.

The study will subsequently concentrate on the conflict between these two rights within the context of EU law, particularly through the lens of the GDPR, the Charter of Fundamental Rights and the case law of the Court of Justice of the European Union (CJEU). The conflict will be further illustrated through two specific case law examples, highlighting how this issue manifests in areas such as the healthcare sector and national security.

Finally, the research will conclude with an overall evaluation of the findings, offering a broader interpretation of the tension between the public sector and individual privacy in relation to the right to be forgotten, and proposing what the appropriate balance should be.

I. THE LEGAL FOUNDATIONS OF THE RIGHT TO BE FORGOTTEN

A. Origins and Development of the Right to be Forgotten

The right to be forgotten originates from an individual's right to control their personal data and is fundamentally based on the right to be left alone. Individuals are granted the autonomy to determine whether and how their personal data is shared or published. The desire to access and control information and the emergence of the right to know, the development of the right to be forgotten has been shaped by the concept of public interest and the rise of data protection rights.

The principle of the right to be forgotten, 'beginning with the first information privacy statute in Wiesbaden, Germany in the 1970s'[1]. The other perspective is 'The European notion of the right to be forgotten draws its origins from droit a` l'oubli, recognized by different decisions in France and in other European countries.'[2]

Data protection laws in several European countries such as Sweden, Austria, Denmark, France and Norway granted individuals the right to request the removal of their personal data from the internet[3]. The right can be referred to as the right to be forgotten: It allows individuals

[1] Jorida Xhafaj, 'The Right to Be Forgotten: A Controversial Topic Under the General Data Protection Regulation' (Legal Science: Functions, Significance and Future in Legal Systems I – ISCF LUL Conference, January 2019) 303.

[2] Tribunale di Roma, 20 November 1996, in Giustizia civile (1997) I, pp 1979 et seq, cited in Alessandro Mantelero, Il costo della privacy tra valore della persona e ragione d'impresa (Milano: Giuffrè, 2007) 229.

[3] Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz – BDSG), cited in Paul M Schwartz, 'The EU–US Privacy Collision: A Turn to Institutions and Procedures' (2013) (126 *Harvard Law Review* 1966), 1969.

to demand the deletion of their personal data from the Internet or from other publicly accessible data sources, with the aim of giving them full authority over their digital past.

Requests to exercise the right to be forgotten typically involving situations where the data has been processed or stored unlawfully or where the continued retention of the data no longer serves the public interest.

The German Constitutional Court traced the foundations of a general 'right to informational self-determination' ('Informationelles selbstbestimmung') and thus of legal data protection regimes and more broadly of the right to privacy to the fundamental right to the 'free development of one's personality[4]protected by Article 2.1. of the German Constitution:

The value and dignity of the person based on free self-determination as a member of a free society is the focal point of the order established by the Basic Law. The general personality right as laid down in Arts 2 (1) i.c.w 1(1) GG serves to protect these values (...)

The right to be forgotten historically emerged as an extension of the right of individuals, particularly those who have been convicted of crimes to have information about their offenses disregarded or erased upon completion of their sentence. [5] The right is founded upon fundamental human values including human dignity, personal reputation, identity and embodies an individual's authority to govern the manner in which their personal history is presented.

Within the European Union, the origin of data protection law is to be related to the adoption of the Data Protection Directive. The directive defines the terms related to the right to be forgotten and contains provisions that all EU Member States are obliged to implement. Article 12 of the Directive; Member States are required to ensure that data subjects have the right to request the rectification, erasure or blocking of their data, particularly when such data

[4] Although the Court acknowledges that the scope and content of that 'personality right' had not been conclusively settled by case law, it nevertheless indicates that that right 'comprises the authority of the individual to decide for himself based on the idea of self-determination– when and within what limits facts about one's personal life shall be disclosed.' Yet, far from the interpretation of privacy as 'property' advanced by law and economics scholars, one understands from reading the decision through that this 'authority' of the individual is not an end in itself: it prevents situations where inhibition of the individual's 'freedom to plan or to decide freely and without being subject to any pressure/influence (i.e., self-determined). The right to self-determination in relation to information precludes a social order and a legal order enabling it, in which the citizens no longer can know who knows what, when, and on what occasion about them. 'cited in Antoinette Rouvroy and Yves Poullet, *The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy* (in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne & Sjaak Nouwt (eds), *Reinventing Data Protection?* (Springer, Dordrecht 2009) 45–76) 49.

[5] Jorida Xhafaj, 'The Right to Be Forgotten: A Controversial Topic Under the General Data Protection Regulation' (2022) 7 *International Scientific Conference of Faculty of Law – University of Latvia* 296, 304.

is incomplete or inaccurate and therefore not processed in accordance with the provisions of the Directive.

The Directive grants data subject's full authority over the accuracy and lawful processing of their personal data. It also stipulates that, in cases where data is found to be incomplete, incorrect or improperly processed, it must be corrected, erased or blocked across all EU Member States.

The General Data Protection Regulation (GDPR), adopted in April 2016, replaced the Data Protection Directive and came into force on 25 May 2018.

The right to be forgotten is ensured under Article 17 of the GDPR. The provision grants data subjects the authority to request the erasure of their personal data without undue delay by the data controller. It imposes a responsibility on the data controller to inform third parties to whom the personal data has been disclosed of the erasure request. Although the data controller has authorized the disclosure of personal data to a third party, the responsibility for ensuring its deletion remains with the controller.

According to Article 17 of the GDPR, the data must be erased without undue delay if:

-the personal data is no longer necessary for the purposes for which it was collected or processed.

-the data subject withdraws consent and there is no other legal basis for processing.

-there is no overriding legitimate ground for processing.

-the personal data has been unlawfully processed.

-erasure is necessary for compliance with a legal obligation under Union or Member State law.

-or the data was collected in relation to the offering of information society services to children under Article 8 of the GDPR.

The regulation (Article 17 of the GDPR) also sets out exceptions where the right to erasure does not apply. Specifically, the right cannot be exercised where data processing is necessary:

-for exercising the right to freedom of expression and information.

-for compliance with a legal obligation under Union or Member State law.

-for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

-for reasons of public interest in public health.

-for archiving purposes in the public interest, or for scientific, historical, or statistical purposes.

-or for the establishment, exercise, or defence of legal claims.

Under certain conditions, the right to be forgotten grants an individual the ability to have personal data promptly erased from online sources and public archives. The right has been developed over time by EU Member States. It is a personal right that may be restricted in cases where more fundamental rights such as public interest, societal benefit or freedom of expression are at stake.

In a number of cases, the implementation of Article 12 of the Directive 95/46/EC in the different national legal frameworks around Europe gave a legal base to the droit a` l'oubli and involved the national data protection authorities in defining the boundaries of this right.[6] In 2011, the CNIL (Commission nationale Informatique et Libertés – National Commission on Informatics and Liberties) in France ruled on a case involving an association called LEXEEK. Although the association had made court documents publicly accessible, it had not removed personal data contained within those documents. The CNIL ordered the association to delete the names and addresses of the parties and witnesses involved in the case. This decision was based on the view that sharing such data constituted a violation of the right to be forgotten.

The landmark case shaping the right to be forgotten is the Google Spain case, which will be discussed in detail below.

B. The Right to be Forgotten within Data Protection Law

Under the EU Directive 95/46/EC and the GDPR; according to Article 6 of Directive 95/46/EC, personal data can only be collected for specified purpose and processing contrary to these purposes is prohibited. The personal data should not be kept longer than necessary for the processing purposes. Accordingly, random or indefinite collection of data is restricted.

[6] Alessandro Mantelero, 'The EU Proposal for a General Data Protection Regulation and the roots of the "right to be forgotten"' (2013) (29 Computer Law & Security Review 229), 232.

Article 12 of Directive 95/46/EC grants the right to request the deletion of data in cases of processing activities that are "not compliant with the provisions of the Directive." The right to erasure covers any data processing carried out without the individual's consent, without sufficient information or outside the framework foreseen by data protection law.

Article 17 of the GDPR defines the conditions of the right to be forgotten in more detail. It establishes the right to request the deletion of personal data from the data controller. Pursuant to Article 17 of the GDPR, the data controller is also under an obligation to notify the data subject when personal data has been made publicly available, taking reasonable measures to ensure that third parties processing such data give effect to the right to erasure. Moreover, the data controller must act without undue delay.

The European Data Protection Supervisor (EDPS) considers this obligation more realistically as a “duty to make efforts” rather than a “strict liability”.[7] Every correction or deletion operation requires notifying the recipients of the disclosed data; if such notification is not feasible or can only be carried out through disproportionate effort, the obligation shall not be enforced. The definitiveness of the right to be forgotten is contingent upon the effort involved; in certain cases, complete erasure of the data may not be achievable.

Regarding its relationship with public interest, under GDPR Article 17, if the processing is carried out for the public interest, the right to erasure may be restricted in favour of public interest.

C. Seminal Case Study: Google Spain v. Agencia Española de Protección de Datos

In May 2014, the Court of Justice of the European Union (CJEU) issued a ruling in the case of Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, upon the preliminary ruling request by the Spanish Supreme Court, Audiencia Nacional. The ruling changed the way data protection legislation is applied and sparked intense academic debates regarding the correct implementation of the Data Protection Directive (DPD). The decision provided a deep and detailed interpretation of the legislation in force concerning the right to be forgotten.

The court made important doctrinal findings, it also paved the way for significant practical outcomes.

[7] EDPS, Opinion of 14 January 2011 on the Communication from the Commission on “A comprehensive approach on personal data protection in the European Union, para. 89.

The judgment pertaining to the case:

The case began with a complaint filed by Mario Costeja González, a Spanish lawyer to the Spanish Data Protection Agency (AEPD). The complaint was against Google and a Spanish newspaper called La Vanguardia. The complaint originated in a Spanish citizen searching his own name on Google. The complainant obtained access to two pages from 1998 in the newspaper related to a property action due to enforcement proceedings concerning social security debts. The AEPD rejected the complaint regarding the newspaper, stating that the publication had been carried out pursuant to a legal obligation. However, the AEPD upheld the complaint against Google.

The rationale for accepting the complaint against Google is based on the principle that search engines bear responsibility for the dissemination of data. If data broadly affect personal rights and human dignity and the data subject does not consent to the disclosure of such data to third parties, search engine operators are obliged to delete the information. The obligation must be discharged irrespective of whether the data have been transmitted via any third-party communication channels.

Google appealed the decision to the Spanish Supreme Court. The court determined, the dispute needed to be evaluated within the scope of EU law. The court suspended the case and referred it to the CJEU for a preliminary ruling.

The legal framework for privacy and personal data protection in the EU:

The Charter of Fundamental Rights of the European Union guarantees privacy and the protection of personal data under Articles 7 and 8.

"Everyone has the right to respect for their private and family life, home, and communications."[8]

"Everyone has the right to the protection of personal data concerning them."[9]

Such data must be processed fairly for specified purposes and based on the consent of the person concerned or another legitimate basis laid down by law. Everyone has the right to access data collected about them and to have it rectified.

[8] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391, art 7.
[9] Charter of Fundamental Rights of the European Union [2012] OJ C 326/391, art 8.

Compliance with such rules shall be subject to oversight by an independent authority. A broad fundamental right obligation is established concerning the protection of personal data. According to the ruling, EU member states must intervene in cases where personal data processing or the manner of processing involves violations, as part of their obligation. Besides data subjects must be authorized to access their data.

The time of the Google Spain ruling, the Directive 95/46/EC (Data Protection Directive) dated 1995 in force. The Directive required Member States to establish legislation ensuring that personal data is processed lawfully and fairly. It stipulated that data controllers must collect data only for specific, explicit and legitimate purposes. The use of the data must be limited to these purposes and the data must be accurate and kept up to date. It also stated that data should be retained only as long as necessary.

Based on the legal framework, the Spanish Court posed three questions to the CJEU:

1. Does an operator of a search engine like Google although established outside the EU, but having branches within the EU, selling services to EU citizens, targeting activities at the EU and cooperating with its parent company fall within the territorial scope of the Directive?[10]
2. Does Google's automatic indexing, temporary storage, and later provision of access to the relevant information constitute "processing of data"? If so, is the search engine operator considered the "controller" of these data?[11]
3. Does the Directive grant individuals the right to directly request search engine operators to delete information about them (i.e., the "right to be forgotten")? The Spanish court defined this as the individual's desire "to be forgotten."[12]

Google stated that its search engine fully complies with the concept of personal data as defined in the Directive. The Court concluded that Google can be classified as a data controller. It found it appropriate to interpret the concept of controller broadly, arguing that data subjects require full and effective protection. The Court also ruled that Google Spain, as a separate legal entity, falls within the territorial scope of the Directive and cannot avoid responsibility. The CJEU decided to interpret the case considering the fundamental rights to respect for private life and protection of personal data as enshrined in Articles 7 and 8 of the Charter of Fundamental

[10] Judgment of the Court (Grand Chamber), Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Case C-131/12) ECLI:EU:C:2014:317.

[11] Ibid.

[12] Ibid.

Rights of the European Union. It acknowledged that search engines like Google could significantly infringe upon these rights.

The CJEU then ruled: "In light of the fundamental rights set out in Articles 7 and 8 of the Charter, the data subject may request that the information not be made available to the general public by appearing in such a results list." Thus, the principle of the "right to be forgotten" emerged in the EU.

The CJEU imposed an obligation on data controllers not simply to delete data directly but to establish a fair balance between the right of access to information and the rights protected under Articles 7 and 8. The Court stated that, as a rule, these rights prevail not only over the economic interests of the search engine operator but also over the public interest in access to information about the data subject via a name-based search.

To rebut the presumption, it has been argued that in cases where special reasons exist, such as the data subject's role in public life, interference with fundamental rights resulting from inclusion in the results list may be justified by an overriding public interest in access to the information.

In conclusion, the Google Spain case effectively established the "right to be forgotten" as a binding principle within the EU, resulting in significant implications.

II. PUBLIC SECTOR DATA MANAGEMENT AND THE CONCEPT OF PUBLIC INTEREST

A. Defining Public Interest in the Public Sector

The notion of public interest does not have a clear or concrete definition in general terms. The debates regarding its precise meaning continue within legal doctrine. According to Felix Frankfurter, it is "vague, impalpable but all-controlling consideration[13]." The concept serves as a fundamental basis of public law and public administration and is a normative principle that underpins the legitimacy of the state and one of the main reasons for its intervention authority. It can be expressed as a set of values concerning the entire society rather than individual or private interests, aiming at common welfare, security and peace.

[13] Felix Frankfurter, Felix Frankfurter Reminiscences: recorded in talks with Harlan B. Phillips, Reynal, New York, 1960, p. 72. See also G. COLM, "The Public Interest: Essential Key to Public Policy" in C.J. FRIEDRICH (ed.), Nomos V: The Public Interest, Atherton Press, New York, 1962, pp. 115 ff.

Public interest also forms both the legal legitimacy and the moral justification of public policies. Based on public interest, societal welfare, justice, equality and collective well-being are pursued with the aim of building a society founded on fundamental rights and freedoms. However, as an abstract concept, its openness to interpretation and variability from case to case may lead it to go beyond its legal context in areas such as transparency and accountability.

The aim to limit the vagueness of public interest and establish boundaries to tame its all-controlling potential, this quest for the concept focuses on three questions: (i) how does the content of public interest form; (ii) how does it manifest itself; and (iii) what role does it play in the legal system?[14] What is valuable for us here, for now, is the first question: how the content of public interest is formed this is what we will seek to answer.

Bentham's explanation here about how the content of public interest is formed; "public interest [as] only an abstract term; [that] only represents the aggregate of individual interests: [which] must all be taken into the account, instead of considering a part as a whole and the rest as nothing."[15]

Bentham's commentary on society is also important in understanding what public interest is related to. He defines society as.; "is a fictitious body, composed of the individual persons who are considered as constituting as it were its members. The interest of the community then is, what? – the sum of the interests of the several members who compose it."[16] Although he defines it in a highly individualistic manner, Bentham expresses public interest as the sum of individual interests, yet he determines a public interest that addresses all individuals in society by adhering to the whole rather than focusing on a part.

Jean-Jacques Rousseau in The Social Contract; "The general will is always right and tends to the public good; but it does not follow that the deliberations of the people have the same rectitude."[17] While Rousseau emphasized the value of the general will, he also pointed out that the people may not always represent the truth correctly. Individuals must continually renew

[14] Christoph Bezemek and Tomas Dumbrovsky, *The Concept of Public Interest*, Graz Law Working Paper Series, Working Paper No 01-2020, 2.

[15] Jeremy Bentham, "Principles of Judicial Procedure" in The Works of Jeremy Bentham, Vol. 2, William Tait, Edinburgh, 1843, p. 252 (Book III).

[16] Jeremy Bentham, An Introduction to the Principles of Morals and Legislation, Batoche Books, Kitchener, Ont., 2000, p. 15.

[17] Patrick Riley, Will and Political Legitimacy, Harvard University Press, Cambridge MA/London, 1982,172.

themselves and strive to align with the collective interest. Consequently, public interest should be approached as an abstract concept that truly expresses what is good for the entire society.

B. Public Services and the Role of Data

Public services refer to the entire range of goods and services provided by the state or public legal entities on behalf of the state continuously, regularly and within the principle of equality to meet the common needs of citizens. These services can be delivered directly by public authorities or by private organizations under public supervision and regulation.

Public services are generally defined as the interaction with the public and the provision of services. In public services, the provision of access, use and sharing of data by governments emerges as an important driving force for innovation in the public sector. Government data include official records and statistics, data generated from administrative procedures carried out through front office services, data arising from public service users such as web content, sensor data, traffic or satellite data essentially, data originating from public services.

The data provided by government departments, institutions, public bodies and local administrations to bring more benefits to society and become an important factor when expanded and virtualized for commercial or non-profit purposes.

Progress is attained incrementally through the actions of each government and compliance with GDPR rules. Ensuring the data collection conditions comply with the GDPR is particularly crucial for the state which holds immense power in any country. Principles such as transparency and accountability become even more important. The comprehensive safeguarding of the existing rights of data subjects appears to be of fundamental importance.

1. Ethical Considerations of Data Deletion in the Public Sector

Ethics, "values have been defined as a set of beliefs and principles that influence or guide people's actions."[18]Ethics is the necessity of having principles based on moral values in the design and implementation of every kind of plan or project that reflects the conscience of society.

Public sector political decisions together with the complexity of hierarchical structures render the perception of ethics more complex and challenging. The concept of ethics is an abstract notion which gives rise to uncertainties in the evidence. Uncertainty generates a range

[18] Mehmet Akif Demircioglu and David B. Audretsch, *Ethics and Public Sector Innovation* (Cambridge University Press 2024) 186.

of diverse political and ethical perspectives and positions, thereby enhancing overall diversity. Uncertainty holds significance for plans and actions aimed at the public good, as it entails substantial responsibility and the necessity to adhere to essential ethical principles.

The ethical framework regarding the deletion of personal data in the public sector, it involves the permanent deletion of personal data collected by any public body once the purpose of use has been fulfilled.

Under the GDPR the fundamental ethical principle in the data deletion process is transparency. The process must be conducted with transparency at every stage. The data subject ought to be informed, by means of a transparent procedure, not only regarding the storage and use of their data but also concerning its erasure. The public authority collecting the data must also be accountable. The public sector must be able to demonstrate accountability in the processes of data handling and deletion. Accountability should be exercised through an independent public authority.

An independent public authority should be tasked with overseeing whether data controllers and data processors involved in the processing of personal data within the scope of digital solutions adhere to the established principles. If necessary, it should also be able to recommend the revocation of their authority to collect or process data.[19]The data deletion process to proceed in accordance with ethical values, the public sector must not evade its responsibilities and is required to act in full compliance with the GDPR.

2. The Impact of the Right to be Forgotten on Public Sector's Efficiency

The innovations brought by the right to be forgotten to the public sector have led to a significant legal impact. The right to be forgotten is expected to contribute significantly to the development of the principles of accountability and transparency in the public sector. The erasure of data under the conditions stipulated by the GDPR constitutes a legal obligation. The obligation requires a public sector to be transparent, trustworthy and accountable, allowing its actions to be trusted and subject to verification.

Although public sector innovations can be highly successful in any dimension (such as increasing the performance of organizations and individuals, reducing costs, and increasing the

[19] WHO, *SMART Trust (v1.2.0) - Ethical Considerations and Data Protection Principles*, HL7® FHIR® Standard v5.0.0 (World Health Organization 2024)

quality of public services), innovations always have a potentially negative side.[20]The right to be forgotten is an important ethical value for the public sector. It is a significant right and freedom for individuals, ensuring that the public sector operates within ethical standards. Although ethics can be primarily associated with innovation failures, some successful innovations can also have negative or unethical aspects.[21] An innovation or principle that enhances the quality of public services or reduces costs, with the aim of improving human life and upholding the rule of law, will be evaluated positively from an ethical standpoint. Certain innovations may change organizational dynamics.

Upon proper implementation of the right to be forgotten in the public sector, data should be deleted once no longer needed.

Data deleted proactively and subsequently required again must be collected anew, resulting in additional workload for the public sector.

The right to be forgotten paves the way for transparency and accountability. In my opinion, developing the public sector along these principles will bring it closer to the private sector's tendency to move quickly.

To elaborate the public sector is generally a closed and slow-moving area, often lost in command-and-control structures. Transparency and accountability are important for achieving efficiency and economic improvements.

With the right to be forgotten, the public sector can overcome this slowness but since it will be continuously subject to accountability and oversight, it will remain within an active planning process, resulting in an increased workload.

III. THE RIGHT TO BE FORGOTTEN AND PRIVACY IN THE PUBLIC SECTOR

A. Balancing Individual Privacy and Public Interests

Balancing the protection of personal data is of critical importance. European courts play a balancing role in disputes arising over data protection rights.

[20] Mehmet Akif Demircioglu and David B. Audretsch, *Ethics and Public Sector Innovation* (Cambridge University Press 2024) 187.

[21] Ibid.

The GDPR recognizes balancing as the primary approach between data protection and other rights, as explained in Recital 4:

The processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, following the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognized in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.[22]

A significant number of the GDPR articles directly indicate the need to establish a proper proportion between the protection of personal data and other values.[23]

The European Union's "EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data," published on December 19, 2019, is an important resource. Progress should be guided by the principles of necessity and proportionality while prioritizing fundamental rights and freedoms. The perspective of the public interest:

The Court of Justice of the European Union has recognised that EU legislation is often required to meet several public interest objectives which may sometimes be contradictory and require a fair balance to be struck between the various public interests and fundamental rights protected by the EU legal order.[24]

---

[22] 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) [2016] OJ L119.

[23] (See: Articles 6(3), 6(4), 9 (2g), 9(2j), 9(2i), 9(2j), 14, 19, 23, 24(2), 34(3c), 35(7b), 83(1), 83(9),84(1),90(1); recitals 4,19, 49, 50, 62, 73, 129, 148, 151, 152, 156, 170). Regulation (Eu) 2016/679, supra note 4.

[24] Case C-275/06, Productores de Música de España (Promusicae) v Telefónica de España SAU, ECLI:EU:C:2008:54, para. 68. In joined cases C-203/15 and C-698/15, Tele2 Sverige AB, Advocate General Saugmandsgaard Øe explained in his Opinion, ECLI:EU:C:2016:572 para. 247, that "[t]his requirement of proportionality within a democratic society - or proportionality stricto sensu- flows both from Article 15(1) of Directive 2002/58 and Article 52(1) of the Charter, as well as from settled case-law: it has been consistently held that a measure which interferes with fundamental rights may be regarded as proportionate only if the disadvantages caused are not disproportionate to the aims pursued" (emphasis supplied). In para. 248 he also pointed out that the requirement of proportionality in this particular case of retention of large amount of data

The decision indicates that, in the name of public interest, certain contradictory measures have been implemented. It can be inferred that the scope of public interest may be interpreted more broadly than necessary, creating the possibility that other rights and freedoms could be overlooked. Particular emphasis should be placed on the necessity of achieving an absolute balance.

Although the EU implements the issue of balance it must be highly effective, transparent and fair, ensuring the proper interrelation among rights. Nevertheless, criticisms of the principle of proportionality also exist:

However, "The principle of proportionality seeks to provide an objective and accurate answer in the conflict between human rights and public interest, similar to that offered in mathematical equations[25]. The EU seeks to find a balance between rights through balancing. It is important to prevent deviation from the purpose of the public interest and to maintain the balance between individual privacy.

B. Legal, Ethical, and Practical Challenges in Data Deletion

Data erasure is regarded as a request arising from an individual's intention to have their data removed from the digital environment due to a change of mind.

While individuals want to delete their data, conflicts of interest may arise between them and the organizations collecting the data. Such circumstances can particularly arise when the retention of data may yield financial benefits for organizations or when the deletion of data incurs significant costs.

The right to be forgotten is guaranteed under Article 7 of the GDPR, which obliges the data-collecting institution or organization to withdraw the data as specified. The concept of deletion can correspond to a deeper and more complex notion than it appears. It is observed that truly deleting data can be a difficult step.

Data collector who complies with the law and adheres to ethical principles, deleting data primarily means leaving no trace behind.

A central idea of our definition is that execution of the deletion request should leave the data collector and the rest of the system in a state that is equivalent (or at least very similar) to

"[o]pens a debate about the values that must prevail in a democratic society and, ultimately, about what kind of society we wish to live in".

[25] Ibid 143.

one it would have been in if the data that is being deleted was never provided to the data-collector in the first place.[26] Leaving no trace means that the data no longer exists in memory and according to one view, that there is no data that can interpret or represent this information anymore. However, according to the GDPR the situation referred to here is the deletion of the data itself, not the deletion of data derived from processing the original data. This issue is debated in doctrine and some argue that within an ethical framework, data derived from deleted data should also be deleted.

Another ethical approach to data deletion is the data collector's obligation to exercise due diligence. Accordingly, the data collector must show necessary care by properly evaluating deletion requests and completing the deletion process fully and timely.

In legal contexts, the data collector must determine whether deletion requests should genuinely be honoured, a decision that can sometimes prove quite challenging. GDPR Article 7 specifies how data deletion should be carried out in which processes. However, when a conflict arises between rights, the issue becomes how to take the appropriate course of action.

A data collector may need to retain certain information due to legal or archival obligations. In such cases, it is a crucial question how they should decide whether to perform the deletion.

The scope of the interpretation of public interest, whether narrow or broad and the extent to which the data serves the public interest is an important criterion that complicates the question of whether the data should be deleted or not.

The GDPR guarantees by law that deletion is not required where the process imposes unnecessary burdens or costs. The difficulty of carrying out the deletion varies from sector to sector and depends on the importance of the data. In situations where legal or practical obstacles exist, the complexity of data deletion may arise.

The deletion process becomes complicated in practice due to the distributed and complex nature of data. Besides access to data outside the EU in jurisdictions not subject to the GDPR is a separate issue concerning data deletion.

In the Google Spain case, data access within EU borders is deleted, yet access from outside the EU has generated debates and contradictions, since the data subject remains aware

[26] Garg, Goldwasser and Vasudevan, 'Formalizing Data Deletion in the Context of the Right to Be Forgotten' (2020) *Lecture Notes in Computer Science* 12106, 373–402, 377.

that their information is still accessible. Data deletion raises many questions legally, practically and ethically.

C. Societal Consequences of Deleting Data for Public Security Purposes

In the subsection, we will examine the deletion of data due to public security reasons and try to elaborate on the issue from a somewhat opposite perspective. Accordingly, the deletion of data for public security reasons appears controversial in terms of its effects on freedom of expression. For example, EU Regulation 2021/784 introduced a rule obliging digital service providers under national authorities to remove certain content within one hour. The regulation concerns the removal of terrorist content. With the new mechanisms established by EU Regulation 2021/784.

The mechanism is novel, not only in view of the direct nature of the removal orders issued (which do not require separate approval by the authorities of the receiving state in order to be valid) and their cross-border execution, but also in view of their almost immediate effect – in most cases consisting in the obligation to block access to the content within a maximum of one hour.[27] This rapid intervention method aims to prevent illegal activities but the lack of a prejudicial review and the very short timeframe for this preventive censorship mechanism raise questions about the extent to which it interferes with freedom of expression.

Under the GDPR, the right to erasure also applies to personal data held by the public sector. Right to erasure can extend to public archives, especially in the case of online archives, courts struggle to balance data protection rights with freedom of expression. The process of balancing rights is challenging, an impediment to the public's right of access to information may arise.

The CJEU's decisions regarding the protection of public interest and individual privacy, The CJEU adopts a more lenient approach towards blanket data retention for the purpose of safeguarding national security, as opposed to its stance on combating serious crime and protecting public safety.[28] To ensure a robust national security regime states employ sophisticated technologies and implement significant measures and the CJEU largely supports this approach. The judgments illustrate that the Court adopts a pragmatic approach when

[27] Marcin Rojszczak, 'Gone in 60 Minutes: Distribution of Terrorist Content and Free Speech in the European Union' (2022) 18(2) *International Journal of Law and Information Technology* 149, 181.

[28] Ketevani Kukava, 'Privacy and Personal Data Protection v. the Protection of National Security and the Fight Against Crime: An Analysis of EU Law and Judicial Practice' (2024) 2 *Journal of Law* 243, 250.

ensuring a fair balance between competing interests.[29] The CJEU's discussion gave rise to criticism for different reasons. Several states deemed the proportionality test on data retention to be excessively stringent and the suggested solutions, such as the targeted data retention, impractical or ineffective.[30] On the other hand, human rights defenders, who advocate for a total ban on mass surveillance instruments, view the CJEU's recent judgments "as a form of legalizing unlimited surveillance methods for national security purposes.[31]

Deleting data for public security purposes involves complex social consequences and covers several areas. Although the aim is to combat crime and ensure national security, attention must be paid to fundamental rights such as privacy, data protection and freedom of expression. In establishing such a balance, the European Court of Justice has also emphasized the significance of the principles of proportionality, judicial oversight and transparency.

IV. PRACTICAL IMPLICATIONS OF THE RIGHT TO BE FORGOTTEN

The main practical consequences of the right to be forgotten in the public sector appear as privacy, transparency and accountability. These are specific responsibilities that public sector institutions must fulfil because of the necessity of the right to be forgotten. Public institutions must establish processes to respond to RTBF requests and ensure compliance with the GDPR. The process also includes GDPR related aspects such as determining the necessity of the data and ensuring its prompt deletion accordingly.

Considering the volume of data, the diversity of data types and the public burden associated with the data held by public institutions, the process is genuinely complex. It is evident that the process must be resolved through a balanced approach.

'In other words, we witness with respect to the well-known EU Court of Justice ruling of 13.05.2014, 131/12 on Google Spain and Google v. Agencia Española de Protección de Datos and Mario Costeja González, characterized by the total openness to the right to be forgotten, seen almost as an absolute right with no limits to the construction, again with a view to a balancing operation between fundamental rights, of a series of barriers that define the boundaries of the right to be forgotten and, in some way, limit its full operation.'[32]

---

[29] Ibid.

[30] Edoardo Celeste, Giulia Formici, Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia, German Law Journal, 2024, 18.

[31] Ibid.

[32] Giulio Ramaccioni, *Cases and Issues of the Right to Erasure (Right to Be Forgotten) Under the Article 17 of Regulation (EU) 2016/679* (2024) 47.

It can be observed that such circumstances foster the public sector's compliance with the GDPR and contribute to the development of a more legally robust public system.

Public institutions are obliged to maintain their transparency while also protecting the individual privacy of their citizens. The recent legal provision of the right to erase should not conflict with archiving, statistical, scientific, and historical research purposes in order to balance privacy with the public interest.[33]

An attitude that directs public institutions toward careful oversight and sound decision-making also serves as evidence that public institutions bear a significant workload and must adhere to prudent policies. Addressing this issue requires public institutions to enhance their use of digital technologies and to be proactive and effective in data deletion processes.

A. Case Study 1: Healthcare Data and Public Health Benefits in the Netherlands

In 2020, the Netherlands established Health Innovation Netherlands (hi-nl) to promote health innovation. The initiative engages all important stakeholders involved in innovations process, ensures a development process via customization and 'fit-for-innovation' guidance, and manage the implementation and termination of promising and non-promising innovations respectively[34]

The Dutch GDPR Implementation Act is the Uitvoeringswet Algemene ver ordening gegevensbescherming (UAVG)[35] In accordance with Article 9 of the GDPR, Sub section 3(1) of UAVG covers special categories of data. Section 22(1) of this subsection provides, in alignment with Article 9(1) of the GDPR, processing of special categories of data, including health data is prohibited. But the subsection also introduces few exclusions to the overall ban. When it comes to the health data reuse by innovators, data subject shall consent to the re-use, [36] and in the absent of consent, four cumulative conditions outlined under Article 24[37] which provide an alternative to consent, shall be met by the applicant: (a) the project has a research

[33] Melanie Dulong de Rosnay and Andres Guadamuz, 'Memory Hole or Right to Delist? Implications of the Right to be Forgotten for Web Archiving' (2017) *RESET* 6, 2.

[34] See https://www.healthinnovation.nl/about (accessed 25 June 2025).

[35] Dutch GDPR Implementation Act (UAVG), available at https://vertaalbureaufiducia.nl/wp-content/uploads/2022/06/Vertaling-UAVG-EN.pdf accessed 18 July 2025, s 22(2)(a).

[36] Ibid.

[37] 'Exception for Scientific or Historical Research or Statistical Purposes.' Worth noting, Article 28 on 'exception for processing genetic data', is another consent alternative, covering the genetic type of health data. However, since Article 28 is complementary and quite similar to Article 24, this provision is not investigated separately in this study.

purpose; (b) the project serves the public interest; (c) obtaining consent is extremely difficult or impossible; and (d) appropriate safeguards are in place. The data subject also has the right to object, and he must be able to do so with ease. This approach is referred to as 'opt-out-plus.'[38]In sections c and d appear to be concrete parts that are easier to prove; However, the same cannot be asserted for sections A and B. The situation arising in the public sector is considered as "research compatible with the public interest" within the public sector. Therefore, it has been assessed that the reuse of health data without consent could be allowed under Article 24.

Regarding private companies the situation is more complex; nevertheless, given that the focus of this study is on the public sector, it will not be addressed in this context.

The Netherlands has regarded the use of data in the public sector as falling within the scope of public interest. Nonetheless, the definition of "public interest" within the Dutch context remains ambiguous.

Public interest refers to the welfare or well-being of the society. According to Dutch law, the concept of public interest is not explicitly defined. Although it is referenced around 70 times in the GDPR, the term "public interest" itself is not directly mentioned. The Dutch health research ethics guideline defines the concept of public interest as follows: "in describing the concept of public interest, the letter of Dutch Ministry of Health, Welfare and Sport on the secondary use of health data to parliament shall be taken into account."[39]

The memorandum determines whether the research serves the public interest based on the following explanation:

[38] Irith Kist, 'Assessment of the Dutch Rules on Health Data in the Light of the GDPR' (2023) 30 *European Journal of Health Law* 322, 334.Cited in S. Rebers, T. van der Valk, G.A. Meijer, F.E. van Leeuwen en M.K. Schmidt, 'Zeggenschap over nader gebruik van lichaamsmateriaal: patiënt is het best gediend met 'geen bez waar'-procedure', Nederlands Tijdschrift voor Geneeskunde 156 (2012) a4485; S. Rebers, E. Vermeulen, A.P. Brandenburg, T.J. Stoof, B. Zupan-Kajcovski, W.J.W. Bos, M.J. Jonker, C.J. Bax, W.J. van Driel, V.J. Verwaal, M.W. van den Brekel, J.C. Grutters, R.A. Tupker, L. Plusjé, R. de Bree, J.H. Schagen van Leeuwen, E.G.J. Vermeulen, R.A. de Leeuw, R.M. Brohet, N.K. Aaronson, F.E. Van Leeuwen and M.K. Schmidt, 'A Randomised Controlled Trial of Consent Procedures for the Use of Residual Tissues for Medical Research: Preferences of and Implications for Patients, Research and Clinical Practice', PLoS ONE 11(3) (2016).

[39] Maryam Afra, *'An Assessment on Innovator's Ability for Consent-Free Health Data Reuse, In the Context of the GDPR and EHDS: The Netherlands Case Study'* (2024) Maastricht University Faculty of Law, 486. Cited in Letter of the minister to the 2nd chamber on secondary use of health care data under the gdpr | Reactie Artikel fd over secundair gebruik data (4 October 2019), available online at https://open.overheid.nl/documenten/ronl-91c5cafa-2a9e-40c8-ae76-75a20f9ca043 /pdf (accessed 25 June 2025).

It must be reasonably plausible that the results of the research (a) Generate new scientific insights that apply to a population larger than the direct research population. (b) The researchers will have to make an effort to make their results transparent to a wider public than just the circle of involved researchers and involved patients. And (c) the research and results must be published, even if the results are negative.[40]

Since dishonest actors usually operate behind closed doors, with little to no tendency to share research findings with the public, the aim of the provision is to prevent data misuse by individuals who are not sincere about their research intentions.[41]The memorandum also states that research must have as its 'essential objective' the promotion and protection of public health. This means that this exception cannot be applied if the research is conducted in an 'exclusively commercial or industrial context.[42]

Given the absence of financial objectives within the public sector, the concept of public interest is entirely grounded in the provision of public services, thereby justifying the protection and reuse of data. Promoting and safeguarding public health is a valid objective in the public sector but it has different implications for the private sector which operates in a commercial or industrial context. In the public sector, public interest is of primary importance with the use of health data regarded as a legitimate justification. Health data can be stored and reused without consent in the public sector. Under the right to be forgotten; Patients appear to have the right to exclude their health information if the data are no longer required for reference by the purpose for which it was collected or processed or even if consent is withdrawn.[43] The right exists when the data subject opposes processing and there are no legitimate grounds for rejecting this request; also the data has been processed unlawfully all the reasons following Article 17 of the GDPR (78).[44] The law has no limits regarding genetic and health data. In this context, any data that can unveil a "self" that the holder does not want to project to society could be subject to the right to be forgotten.[45] Although individuals' health information is highly personal and sensitive, it must be balanced against interests such as public health, scientific research, and freedom of expression. Therefore, when a document refers to the public interest, there is no

[40] Ibid.
[41] Ibid.
[42] Ibid.
[43] Mónica Correia, Guilhermina Rêgo and Rui Nunes, 'Gender Transition: Is There a Right to Be Forgotten?' (2021) 27(3) *Health and Technology* 285, 291.
[44] Ibid.
[45] Ibid.

absolute guarantee that personal data will be deleted. In such cases, a balancing policy must be established one that weighs public interest against individual privacy.

However, the concept of public interest holds significant weight in this balance and tends to take precedence in the name of protecting public health. The reuse and potential deletion of health data in the public sector must be approached from a perspective where public interest is prioritized and balanced with the right to be forgotten.

Such data are not subject to deletion within the context of public welfare and public health. The data are preserved for potential future reuse and are employed when deemed necessary.

B. Case Study 2: Security Data and National Security

According to Article 23 of the GDPR, Member States are permitted to impose restrictions on data protection on the grounds of national security. National security is against individual privacy, the GDPR dictates that national security shall prevail. The article also requires that the essence of fundamental rights and freedoms must be respected. While the restrictions of the term "national security" are hard to determine, the European Convention on Human Rights case-law has made it possible to give some more substance to the notion of national security which involves the protection of state security from terrorism, separatism, etc.[46]

From the perspective of the European Union legal framework, the case law of the European Court of Human Rights (ECtHR) is particularly important in illustrating how fundamental rights, particularly the right to privacy, are balanced against national security concerns. National security is facing numerous challenges, particularly regarding whether individual rights should be violated or guaranteed. Security and stability of every state institution are the major guarantees for the safety of citizens, human security and respecting individual rights of the relative citizens.[47] The concept of national security (while expressing the protection of state security) covers a broad and relatively open area. When considering how

[46] Gergana Georgieva, Yavor Simov and Reneta Nikolova, *Some National Security Issues under the European Convention on Human Rights Case-Law* (Ministry of Interior 2021) 157. Cited in Marin, N. Nationalisms Versus Solidarity in Case of EU Law and Security, in International conference KNOWLEDGE-BASED ORGANIZATION 24(2):221-224, June 2018, DOI: 10.1515/kbo-2018-0093. See also Mihov, S. Some Problems of the European Information Exchange Model in the Field of the Law Enforcement Cooperation, International conference KNOWLEDGE-BASED ORGANIZATION, Volume 24: Issue 2, DOI: https://doi.org/10.1515/kbo-2018-0094, published online: 26 Jul 2018.

[47] Ibid 158, cited in Trobbiani, R, *How Should National Security and Human Security Relate to Each Other?*, APR 26 2013, available at https://www.e-ir.info/2013/04/26/how-should-national-security-and-human-security-relate-to-each-other/.

far national security can override individual privacy and personal rights, the case of Rotaru v. Romania[48] an important example. The Romanian Intelligence Service presented a letter in court concerning Rotaru's past political activities. Rotaru has been characterized as an extremist right-wing figure and a member of the Legionary movement. He contended that the information was false and defamatory and sought its removal from the records. Nevertheless, the court held that it lacked the authority to order the deletion of the document.

The European Court of Human Rights did not consider the Romanian Intelligence Service's retention and use of this information to be lawful. It found violations of both Article 8, the right to respect for private life and Article 6 the right to a fair trial. The reason for the position lies in the national security legislation being drafted in very general terms and lacking adequate safeguards to protect individuals' privacy.

The Court ruled RIS's ownership and usage of information about the applicant's privacy (though admissible in cases for example in the interest of national security) was not "in accordance with the law" because the law was formulated in very general terms and did not provide any guarantees for individuals to protect their privacy.[49] Mr. Rotaru's right to privacy was therefore infringed. Thus, the Court has the view that the law itself needs to be particularized.[50] The Court stated that the systematic filing and retention of personal data such as political activities, education, and criminal records by state officials constitute an interference with private life under Article 8. As seen, the ECtHR considered the retention and non-deletion of old intelligence data as a violation. Although the decision predates the entry into force of the GDPR, the ECtHR regarded the storage of data from a document dating back to 1937 as a breach of the right to privacy. The Court determined the national security definition to be insufficient and overly broad, failing to protect individual rights.

The ECtHR prioritized individual rights over national security. The reason for prioritizing individual rights is that the information dated back to 1937 and a considerable amount of time had passed, indicating a genuine violation. The intelligence service had unlawfully retained this information for an extended period. The Court rejected the State's broad interpretation of national security protection, demonstrating that, even prior to the GDPR era, the significance of data deletion was recognized and any violations were clearly apparent. The individual right to data erasure outweighed national security. Moreover, under current GDPR conditions, the

[48] Rotaru v. Romania, Application No. 28341/95, Judgment of 4 May 2000.
[49] Ibid.
[50] Ibid.

need for a balancing policy between public interest and the right to erasure is constantly emphasized. The ECtHR decision demonstrates that when the balance shifts excessively in favour of the public interest, a violation arises.

V. LEGAL DISPUTES BETWEEN PUBLIC INTEREST AND INDIVIDUAL RIGHTS

A. Examining Conflicts Between Public Interest and Individual Privacy

The balance between public interest and individual privacy in the EU has increasingly become a source of legal disputes, particularly considering technological advancements and the growing significance of data. Disagreements arise primarily from the existence, storage, transfer and use of data, which often conflict with personal privacy.

1. Surveillance and Predictive Policing:

The relationship between public interest and the right to be forgotten as a broader discussion between security and privacy. The balance between these two is particularly significant in the context of mass data surveillance and predictive policing practices. The EU's goal is to anticipate and prevent crimes before they occur. Data Retention Directive grant law enforcement authorities' access to such predictive tools. This involves large scale processing of personal data, raising concerns about the proportionality of such measures and the extent to which personal data is protected.

The EU has introduced various legal instruments, including the e-Privacy Directive, the Passenger Name Record (PNR) Directive, and the Anti-Money Laundering Directive. The regulations also intersect with the stages of predictive and preventive policing, leading to increasing overlap between the public and private sectors within the EU. This raises the risk of infringing individual rights and freedoms based on speculative threats or crimes that have not yet occurred.

The Court of Justice of CJEU has made critical rulings on this matter. on 8th April 2014, the CJEU, sitting in Grand Chamber, declared Directive 2006/24/EC invalid since it violates the right to privacy (Article 7 of the Charter) and the right to protection of personal data (Article 8 of the Charter), read in light of Article 52 of the Charter of Fundamental Rights of the

European Union (the Charter). In adopting Directive 2006/24, the EU legislature exceeded the limits imposed by the principle of proportionality.[51]

In particular, the ECJ underlined that the Data Retention Directive set up a regime that failed to limit interference with privacy rights "to what is strictly necessary,"[52] suggesting emphatically that, on the contrary, the Data Retention Directive "entail[ed] an interference with the fundamental rights of practically the entire European population."[53] In the ECJ's view, five major faults doomed the legality of Directive 2006/24.[54] First, the Directive did not set any limit on the personal scope of application: the Directive "affects, in a comprehensive manner, all persons using electronic communications services . . . . It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime."[55]

Second, the Directive did not set any limits on the possibility of national authorities accessing the data retained by private companies, and failed to specify conditions that justify the use of these data for law enforce meant purposes: "[o]n the contrary, Directive 2006/24 simply refer[red], in Article 1(1), in a general manner to serious crime, as defined by each Member State in its national law"[56] and did not make access dependent "on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities . . . ."[57]

Third, the Directive did not set a sufficiently restrictive timeframe for the retention of data: "Article 6 of Directive 2006/24 requires that . . . data be retained for a period of at least six months, without any distinction . . . between the categories of data set out in Article 5 . . . on the basis of their possible usefulness for the purposes of the objective pursued or according

[51] Joined Cases C-293/12 and 594/12 Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung et al (cjeu, 8 April 2014). See also Joined Cases C-293/12 and 594/12 Digital Rights Ireland Ltd v. Minister for Communication et al and Kärtner Landesregierung et al (cjeu, 8 April 2014), Opinion of ag Villalón; F Fabbrini, 'Human Rights in the Digital Age, The European Court of Justice Ruling in the Data Retention Case and its Lessons for Privacy and Surveillance in the us' (2015) 28(1) Harvard Human Rights Journal (forthcoming).

[52] Joined Cases C-293/12 & C-594/12, Digital Rights Ireland, §56.

[53] Joined Cases C-293/12 & C-594/12, Digital Rights Ireland, §56.

[54] Federico Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States' (2015) 28 *Harvard Human Rights Journal* 65, 80.

[55] Ibid 60.

[56] Ibid 60.

[57] Ibid 62.

to the persons concerned."[58] Fourth, the Directive did not provide for sufficient safeguards relating to the security and protection of the data retained by private providers of electronic communications.[59] Finally, the Directive did "not require the data . . . to be retained within the European Union, with the result that it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security . . . is fully ensured.[60] In light of these serious flaws in the Data Retention Directive, the ECJ ruled that "the EU legislature ha[d] exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter"[61] and struck down the Directive, making it immediately inapplicable in the EU legal order.[62] The CJEU's annulment of the Data Retention Directive due to its violation of the Charter of Fundamental Rights highlights both the value of personal data and the importance of maintaining a balance between public interest and fundamental rights. A careful balancing policy is necessary in the area, and giving priority to public interest in a way that overrides fundamental rights constitutes an unacceptable approach.

2. Financial Information and Tax Purposes

On November 22, 2022, in Press Release 188/22, the CJEU gives a preliminary ruling on the judgment of the Court of Justice in Joined Cases C-37/20 Luxemburg Business Registers and C-601/20 Sovim concerning Directive (UE) 2015/849 of the European Parliament and of the Council.[63] Later on, the recent case of the European Court of Justice that was made public concerned WM and Sovim SA vs. Luxembourg Business Registers.[64] The issue concerns companies being able to access beneficial ownership information without providing justification. The accessible information includes surname, first name, nationality, date of birth, month of birth, year of birth, place of birth, country of residence, full private or professional address, national identification number for individuals registered in the national population register, foreign identification number for unregistered foreigners, the nature of the beneficial interest held and the percentage of that interest.

---

58 Ibid 63.
59 Ibid 66.
60 Ibid 68.
61 Ibid 69.
62 Ibid 71.
63 Glória Teixeira, Maria Filipa Pinho and Hugo Teixeira, 'Access to Financial Information for Tax Purposes and Proportionality – Balancing Public Interest with the Protection of Privacy' in Monica Rosini and Gloria González Fuster (eds), *Data Protection and Tax Information Exchange* (Springer 2023) 9.
64 Joined cases C-37/20 and C-601/20 of 22 November 2022.

Access to such information enables the straightforward identification of the beneficial owner, and this has been regarded as a violation of the fundamental right to privacy.

The CJEU emphasized three key principles. While the principles of transparency and legality were not deemed to have been violated, the Court ruled that a breach had occurred regarding proportionality. "The difficulties in precisely defining the circumstances and conditions under which the public may access beneficial ownership information cannot justify the EU legislator providing for general public access to such data. “The situation is considered an interference with fundamental rights protected under the EU Charter of Fundamental Rights.

In an era, where information often becomes available through illegal access to personal and most importantly private data, a recent decision, dated of November 11, 2022, when the Finnish Data Ombudsman (Tietosuojavaltuutettu), which is the national authority supervising compliance with data protection legislation, gave her ruling in the case Dnro 3681/186/21, giving a proper insight when it comes to the performance required by the competent entities, when such cases occur.[65]

The data protection authority first emphasized the need to assess whether the processing complies with the GDPR and relevant legislation. While the collection of such data is justified as an effective approach to combating tax evasion, money laundering and the financing of terrorism, the data protection authority underlined that each specific case must proceed in a lawful, fair, and proportionate manner.

Reference is provided to Article 5 of the GDPR, emphasizing that processing must be relevant and limited to what is necessary in relation to the purposes for which the data is collected. Additionally, Article 25(2) of the GDPR was cited, which obliges data controllers to implement appropriate technical and organizational measures to ensure that only personal data necessary for the purpose is processed.

This decision may serve as a precedent for other EU Member States. The limits of access to personal data are yet to be fully defined and must also align with public interest criteria. In the European Union, a series of rulings exists, ranging from local courts to the CJEU. Compliance with the GDPR whether in data processing, retention or erasure must align with

[65] Glória Teixeira, Maria Filipa Pinho and Hugo Teixeira, ‘Access to Financial Information for Tax Purposes and Proportionality – Balancing Public Interest with the Protection of Privacy’ in Monica Rosini and Gloria González Fuster (eds), *Data Protection and Tax Information Exchange* (Springer 2023) 11.

the principle of proportionality, which seeks to balance public interest with individual privacy and the protection of fundamental rights and freedoms.

B. Ethical and Legal Considerations of Data Retention vs. Deletion in the Public Sector in the EU

Ethical considerations regarding data deletion in the public sector are multifaceted. Legal regulations, court rulings, and especially technological advancements and processes increasingly shape this area. "Data retention is the collection of bulk metadata. Everyone's data is collected without the requirement of any suspicion or the intercession of a judge. It is the job of individuals and organizations in the private sector to retain the metadata (tapping into a whole new industry of data warehousing)".[66] While the preamble to the Data Retention Directive refers to law enforcement authorities in three places (twice in Preamble 9 and once in Preamble 14) and declares itself compliant with the European Convention of Human Rights (ECHR), in the text Article 4 permits member states to allow access to data retained by whatever competent law enforcement agency it chooses.[67] Thus there is no necessary monopoly of criminal justice authorities over access to the data. Member states could allow their intelligence services to have access to the data (as the US authorities have done in respect of PRISM).[68] These are among the aspects of data retention which have caused the most concern, as it is hard to escape the conclusion that retention of the data is arbitrary and access to it is unlimited.[69]

Data retention raises significant ethical concerns related to principles and practices. The storage of personal data, especially for individuals who have been wrongly accused or unfairly linked to a crime, can lead to continued stigmatization and discrimination. For instance, regarding DNA data, a forensic DNA database typically contains two kinds of DNA profiles. The first category consists of profiles which are derived from unidentified crime scene stains.[70]

These are bodily samples such as skin cells, hair, blood or saliva which possibly belong to an individual who has been involved in a criminal offence.[71] The other category, which in

[66] IBM and Oracle quotations, cited in Elspeth Guild and Sergio Carrera, The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive (CEPS Paper in Liberty and Security in Europe No 65, May 2014) 2.

[67] Ibid 3.

[68] Ibid 11.

[69] Elspeth Guild and Sergio Carrera, *The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive* (CEPS Paper in Liberty and Security in Europe No 65, May 2014) 3.

[70] N Van Camp and Kris Dierickx, 'The retention of forensic DNA samples: a socio-ethical evaluation of current practices in the EU' (2008) 34 *Journal of Medical Ethics* 606.

[71] Ibid.

most countries makes up the largest part of the database, consists of the DNA profiles of individuals who have been convicted of a criminal offence or who are a suspect of a crime that is still under investigation.[72]

In recent years, the steady expansion of these forensic DNA databases has provoked a number of critical questions on issues related to this practice, such as the entry and removal criteria of these databases,[73] the intrusiveness of coercive sampling,[74] the possible creation of databases covering the entire population.[75] The issue of DNA retention is an area where governments are increasingly collecting data but are reluctant to address it openly, especially due to security concerns related to terrorism and other necessary reasons. Governments argue that they are protecting the public interest through these security measures. However, European institutions and EU member states have not addressed this issue sufficiently or adequately in either political discourse or legal regulations. Although we should not exaggerate the possibility that forensic DNA samples are used for ends such as those described above, the ongoing expansion of forensic DNA databases and police sampling powers do give rise to justifiable concerns regarding the consequences of these evolutions for genetic privacy.[76] Probably the major shortcoming of European regulations regarding the processing of personal information is that they do not apply to justice and security issues.[77] This can clearly be observed in the Data Protection Convention of the Council of Europe (Article 3, Section 2) which explicitly mentions that it does not apply to measures taken in the interests of ‘‘protecting state security, public safety, the monetary interest of the state or the suppression of criminal offences’’(Article 9, Section 2).[78] As the provisions of this Directive would make it otherwise well-nigh impossible for the Member States to use DNA profiling techniques and operate DNA databases, Article 3 clearly states that this Directive does not apply to ‘‘[…] activities of the State in areas

[72] Ibid.

[73] Ibid, 606, cited in See for example: Guillén M, Lareu MV, Pestoni C, et al, *Ethical-Legal Problems of DNA Databases in Criminal Investigation* (2000) 26 *J Med Ethics* 266–71.

[74] Ibid, 606, cited in See for example: Kaye DH, *Who Needs Special Needs? On the Constitutionality of Collecting DNA and Other Biometric Data from Arrestees* (2006) 34 *J Law Med Ethics* 188–98.

[75] Ibid, 606, cited in See for example: Cronan JP, *The Next Frontier of Law Enforcement: A Proposal for Complete DNA Databanks* (2000) 28 *Am J Crim Law* 119–56.

[76] Ibid, 607.

[77] Ibid.

[78] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) art 9(2) http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm accessed 04 July 2025.

of criminal law''.[79] In the directives and decision-making mechanisms, the authority regarding DNA data appears to be largely left to the discretion of individual states.

The only official document on the European level which has brought forward clear benchmarks regarding this issue is the Recommendation No. (92) 1 of the Council of Europe. In contrast with the Data Protection Convention and Directive 95/46/EC, it does not make an exception for the processing of data in the field of justice and security and thereby explicitly forbids any secondary use except those for the purpose of the investigation and prosecution of criminal offences. However, the Recommendation does also allow for an exception when the samples are used for ''research and statistical purposes'' (Section 3).[80] The directive encourages the destruction of biological material collected for DNA profiling once a final decision has been made in the relevant case. However, the encouragement varies in practice: while some EU countries destroy the material immediately, others follow different procedures. Additionally, the DNA data of convicted individuals may be retained for a long period.

As observed, the definition of public interest regarding the retention and deletion of data is generally interpreted broadly by governments. Therefore, both ethically and legally, personal data and individual rights tend to be considered secondary to public interest. Past terrorist attacks in Europe are cited as a significant reason for this approach. The context in which the principle of proportionality is applied is the aspect that holds importance.

C. Balancing Conflicting Interests: How Can a Fair Solution Be Achieved?

Through various examples from different public sectors, it has been observed how data retention and deletion practices are linked to the concept of public interest. A balancing policy is essential and evident. According to the policy, a balance must be established between the public interest and the individual rights and freedoms involved in the data deletion process and actions should be taken accordingly.

[79] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, art 3 http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett accessed 6 July 2025

[80] Council of Europe, Recommendation No R (92) 1 of the Committee of Ministers on the use of analysis of DNA within the framework of the criminal justice system, section 3 accessed July 2025.

1. What should be done to achieve this balance?

a. Regulatory clarity and compliance

For balanced solutions regarding data deletion and the interpretation of the GDPR, the CJEU judgment in C-507/17, Google v. Commission nationale de l'informatique et des libertés (CNIL) highlights how the right to be forgotten must be balanced against other rights in cases of conflict. Even within Member States, the Court admits that the results of weighing up the competing rights will not necessarily be the same, posing a challenge to harmonisation if cooperation mechanisms among Member States is not properly implemented.[81]

Under the GDPR, the balance between the right to be forgotten and the public interest must be carefully assessed on a case-by-case basis, and appropriate precedent-setting decisions should be made. The boundaries of public interest remain unclear. Defining the boundaries at least within a certain framework would clearly help determine priorities and support the application of the principle of proportionality.

b. Technological solution in Machine Learning

In the contemporary technological era, where data can be rapidly stored using AI, specific procedures have been established for its deletion. 'Although there are different data handling methods, as the techniques exist currently, there is no evidence that these have been applied to industry.'[82] The majority of the paper's proposals do use example data sets as part of its evaluation, but the effectiveness for industry is not yet clear.[83] In these and similar technological fields, issues related to data deletion need to be addressed. In areas already marked by conflict, the deletion process can be particularly difficult, making it essential to properly enforce this right. Therefore, appropriate technological measures must be taken.

c. Public Engagement and Education

Building trust through public participation and education in the data deletion process is essential for ensuring that data deletion decisions in the public sector progress in a balanced

---

[81] Mary Samonte, *'Google v CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law'* (Insight, *European Papers* vol 4, no 3, 2019) 839–851, 850.

[82] Katie Hawkins, Nora Alhuwaish, Sana Belguith, Asma Vranaki and Andrew Charlesworth, *"A Decision-Making Process to Implement the 'Right to Be Forgotten' in Machine Learning"* (eds Kai Rannenberg, Prokopios Drogkaris and Cédric Lauradoux; *Privacy Technologies and Policy – 11th Annual Privacy Forum, APF 2023, Proceedings* (Springer, Lecture Notes in Computer Science vol 13888, 2024) 20–38, 32.

[83] Ibid.

and appropriate manner. For example, in the healthcare sector with systems like EDHS the effect of the data sharing arrangement therefore needs to be monitored carefully to ensure that suitable techniques are used in the relevant data sharing contexts, so that the data minimisation principle is respected.[84] Such processes require careful steps to be taken and it is crucial to have a clear understanding of the differences between data minimization, data anonymization and data deletion. Citizens should also be informed and made aware of these issues.

d. Ethical-Legal Oversight and Accountability

As defined in the GDPR; fairness, transparency and accountability are crucial aspects of data auditing. Effective data auditing requires independent bodies in the public sector to conduct oversight that balances public interest while ensuring transparency and accountability to data subjects. Effecting data auditing also facilitate the balance between data deletion processes and the public sector, leading to more accurate and appropriate practices in this area.

CONCLUSION

In the European Union framework, the balance between the right to be forgotten as an individual right and the public interest in the public sector has become increasingly complex and delicate, particularly due to technological advancements and the growing digitization of data usage by public institutions.

For the balancing policy between the right to be forgotten and the public interest, the importance of the terminological definition and conceptual integrity of both public interest and the right to be forgotten has emerged. The case of Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González (C-131/12, 13 May 2014) represents a significant turning point.

The broad interpretation of public interest in certain areas, and situations where the right to privacy may be overridden by the right to be forgotten. These include mass data surveillance for public security purposes, financial information sharing, the expansion of DNA databases, and the storage and use of health sector data to ensure national security, highlighting conflicts and tensions between public interest and the right to be forgotten.

[84] Zhicheng He, *'From Privacy-Enhancing to Health Data Utilisation: The Traces of Anonymisation and Pseudonymisation in EU Data Protection Law'* (2023) *Digital Society* vol 2, no 2, art 17, accessed (22 July 2025), 17.

The important rulings of the CJEU, especially the annulment of the Data Retention Directive, have established that the principle of proportionality and the protection of individual rights are indispensable. In this context, the significance of the right to be forgotten also emerges. These rulings clearly demonstrate that the public interest cannot override individual rights and the right to be forgotten.

The principle of proportionality and the protection of fundamental individual rights are core principles in balancing these rights, and transparency and accountability will facilitate public institutions' compliance with these principles. It is evident that the right to be forgotten has gained significant importance, especially following the Google Spain case, and that this right has emerged as a crucial individual right in the public sector as well, particularly in ensuring that the concept of public interest is properly evaluated.

For a fair and effective resolution of the balancing policy between public interest and the right to be forgotten, it appears essential that the boundaries of public interest are not interpreted too broadly. Regulatory clarity must be ensured in this regard. As stated under the GDPR, the principle that data may be retained in the name of public interest should be interpreted correctly rather than expansively, particularly in relation to the principle of proportionality with the right to be forgotten.

Between the right to be forgotten and the public interest a balancing policy must be applied with great sensitivity. Technological developments, especially in the field of machine learning, should be integrated into the data deletion process to support this balance. Public participation and awareness raising efforts are crucial for increasing individuals' understanding of their rights. There should be initiatives aimed at ensuring that public sector employees develop a deeper awareness of their duties and the limits of public interest.

Independent oversight mechanisms should be implemented to ensure that public institutions uphold the principles of transparency and accountability. The delicate nature of the balancing policy between public interest and the right to be forgotten can be improved, leading to a more ethical approach.

REFERENCES

Afra M, 'An Assessment on Innovator's Ability for Consent-Free Health Data Reuse, In the Context of the GDPR and EHDS: The Netherlands Case Study' (2024) (Maastricht University Faculty of Law, 486).

Arjamand M, Cholistani MS, Shakoor S, Farhan M, Ashraf B, Naqqi M, Iqbal Q, Luqman M, Fatima SEEM, Kareem K and Khan HU, 'Forensic DNA Profiling: Its Role and Advancements in Criminal Investigations' (15 November 2024) 7(5) (*International Journal of Multidisciplinary Research and Publications* 42–46).

Ayday E and Hubaux JP, 'Threats and Solutions for Genomic Data Privacy' (2015) in Gkoulalas-Divanis A and Loukides G (eds), *Medical Data Privacy Handbook* (Springer International Publishing 2015) 463–92.

Bartolini C and Siry L., 'The Right to Be Forgotten in the Light of the Consent of the Data Subject' (2016) (32 Computer Law & Security Review 218).

Christoph Bezemek ve Tomáš Dumbrovský, 'The Concept of Public Interest' (2020) *SSRN Electronic Journal*

Bougiakiotis E, 'The Enforcement of the Google Spain Ruling' (2016) (24 International Journal of Law and Information Technology 311).

Bugarski T, Tubić B and Pisarić M, 'Legal Regulation of Air Pollution in Urban Environments at the Level of the European Union' (2020) 54 (*Zbornik radova Pravnog fakulteta Novi Sad* 71–91).

Case C-131/12 Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECLI:EU:C: 2014:317.

Case C-293/12 and Case C-594/12, Digital Rights Ireland, EU:C:2014:238.

Celeste E, Formici G, Constitutionalizing Mass Surveillance in the EU: Civil Society Demands, Judicial Activism, and Legislative Inertia, German Law Journal, 2024.

Charter of Fundamental Rights of the European Union [2012] OJ C 326/391.

Chenou JM and Radu R, 'The "Right to Be Forgotten": Negotiating Public and Private Ordering in the European Union' (2019) 58(1) (*Business & Society* 74–102).

Correia M, Rêgo G and Nunes R, 'Gender Transition: Is There a Right to Be Forgotten?' (2021) 29(3) (*Health Care Analysis* 283).

Correia M, Rêgo M and Nunes R, 'Gender Transition: Is There a Right to Be Forgotten?' (2021) 27(3) (Health and Technology 285).

Court of Justice of the European Union PRESS RELEASE No 70/14 Luxembourg, 13 May 2014 Press and Information Judgment in Case C-131/12 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González.

Court of Justice of the European Union, Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others (Joined Cases C-293/12 and C-594/12) ECLI:EU:C:2014:238.

Demircioglu MA and Audretsch DB, Ethics and Public Sector Innovation (Cambridge University Press 2024).

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

Dulong de Rosnay M and Guadamuz A, 'Memory Hole or Right to Delist? Implications of the Right to Be Forgotten for Web Archiving' (2017) 6.

Engin Z and Treleaven P, 'Algorithmic Government: Automating Public Services and Supporting Civil Servants in Using Data Science Technologies' (2019) 62 The Computer Journal 448.

European Court of Human Rights and European Union Agency for Fundamental Rights, Right to be Forgotten: ECtHR and CJEU Case-Law – Joint Factsheet.

European Data Protection Supervisor (EDPS), *Opinion of 14 January 2011 on the Communication from the Commission on "A comprehensive approach on personal data protection in the European Union"* (EDPS 2011).

European Data Protection Supervisor, EDPS Guidelines on Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data (19 December 2019).

Fabbrini F. 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States' (2015) (28 Harvard Human Rights Journal 65).

Frankfurter F., Felix Frankfurter Reminiscences: recorded in talks with Harlan B. Phillips, Reynal, New York, 1960, p. 72. See also G. COLM, "The Public Interest: Essential Key to

Public Policy" in C.J. FRIEDRICH (ed.), (Nomos V: The Public Interest, Atherton Press, New York, 1962, pp.).

Frantziou E, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos' (2014) (14 Human Rights Law Review 761).

Galea M, The Right to be Forgotten; a Balance Between Privacy and Public Rights? (LL.D. Thesis, University of Malta, 2015)

Garg S, Goldwasser S and Vasudevan PN, 'Formalizing Data Deletion in the Context of the Right to Be Forgotten' (2020) (Lecture Notes in Computer Science 12106, 373–402).

Georgieva G, Simov Y and Nikolova R, Some National Security Issues under the European Convention on Human Rights Case-Law (Ministry of Interior 2021).

Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz – BDSG), cited in Paul M Schwartz, 'The EU–US Privacy Collision: A Turn to Institutions and Procedures' (2013) (126 Harvard Law Review 1966).

Guild E and Carrera S, The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive (CEPS Paper in Liberty and Security in Europe No 65, May 2014).

Guillén M, Lareu MV, Pestoni C, Salas A and Carracedo Á, 'Ethical-legal problems of DNA databases in criminal investigation' (2000) 26(4) (*Journal of Medical Ethics* 266–71).

Hawkins K, Alhuwaish N, Belguith S, Vranaki A and Charlesworth A, "A Decision-Making Process to Implement the 'Right to Be Forgotten' in Machine Learning" (eds Rannenberg K, Drogkaris P and Lauradoux P; Privacy Technologies and Policy – 11th Annual Privacy Forum, APF 2023, Proceedings (Springer, Lecture Notes in Computer Science vol 13888, 2024) 20–38.

Hawkins K, Alhuwaish N, Belguith S, Vranaki A and Charlesworth A, 'A Decision-Making Process to Implement the 'Right to Be Forgotten' in Machine Learning' (2024) LNCS 13888, (*Privacy Technologies and Policy - 11th Annual Privacy Forum* 20).

He Z, 'From privacy-enhancing to health data utilisation: the traces of anonymisation and pseudonymisation in EU data protection law' (2023) 2(2) (Digital Society 17).

Heylliard C, 'Le droit à l'oubli sur Internet' (Master 2 recherche thesis, Université Paris-Sud – Faculté Jean Monnet, 2012).

J. Bentham, "Principles of Judicial Procedure" in The Works of Jeremy Bentham, Vol. 2, William Tait, Edinburgh, 1843, p. 252 (Book III).

J. Bentham, An Introduction to the Principles of Morals and Legislation, Batoche Books, Kitchener, Ont., 2000.

Judgment of the Court (Grand Chamber), Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (Case C-131/12) ECLI:EU:C:2014:317.

Justickis V, 'Balancing Personal Data Protection with Other Human Rights and Public Interest: Between Theory and Practice' (2020) 13(1) (Baltic Journal of Law & Politics 140).

Katsirea I, Press Freedom and Regulation in a Digital Era: A Comparative Study (Oxford University Press 2024).

Kist I, 'Assessment of the Dutch Rules on Health Data in the Light of the GDPR' (2023) (30 *European Journal of Health Law* 322).

Kohl U, 'The Right to Be Forgotten in Data Protection Law and Two Western Cultures of Privacy' (2023) 72(3) *International & Comparative Law Quarterly* 737–769

Krošlák D, 'Practical Implementation of the Right to Be Forgotten in the Context of Google Spain Decision' (2015) 6 Communication Today 1 (Vol 6, No 1).

Kukava K, 'Privacy and Personal Data Protection v. the Protection of National Security and the Fight Against Crime: An Analysis of EU Law and Judicial Practice' (2024) (2 Journal of Law 243).

Maceratini A, 'Subjective Identity and the Right to be Forgotten: A Multifaceted Claim in the Legal System' (2024) 29(3) (*Białostockie Studia Prawnicze* 271–86).

Mantelero A, 'The EU Proposal for a General Data Protection Regulation and the roots of the "right to be forgotten"' (2013) 29(3) (Computer Law & Security Review 229).

Mantelero A, 'The protection of the right to be forgotten: lessons and perspectives from open data' (2015) Jurisdiction & Dispute Resolution in the Internet Era: Governance and Good Practices, Geneva, Switzerland.

Mantelero, Alessandro, *Il costo della privacy tra valore della persona e ragione d'impresa* (Giuffrè Editore 2007).

Mitrou L and Karyda M, 'EU's Data Protection Reform and the Right to be Forgotten: A Legal Response to a Technological Challenge?' (2012) (*5th International Conference of Information Law and Ethics*, Corfu, 29–30 June 2012).

Nandy D, 'Human Rights in the Era of Surveillance: Balancing Security and Privacy Concerns' (2023) (*Journal of Current Social and Political Issues* 11, 13–17).

P. Riley, Will and Political Legitimacy, (Harvard University Press, Cambridge MA/London, 1982).

Panneerchelvam S and Norazmi MN, 'DNA profiling in human identification: from past to present' (2023) 30(6) (*Malaysian Journal of Medical Sciences* 5–21).

Pina E, Ramos J, Jorge H, Váz P, Silva J, Wanzeller C, Abbasi M and Martins P, 'Data Privacy and Ethical Considerations in Database Management' (2024) 4(3) (*Journal of Cybersecurity and Privacy* 494–517).

Post RC, 'Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere' (2018) 67(5) (Duke Law Journal 981).

Giulio Ramaccioni, 'Cases and Issues of the Right to Erasure (Right to Be Forgotten) under Article 17 of Regulation (EU) 2016/679' (2024) 14 *Computer Science & Information Technology* 35–48

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) [2016] OJ L119.

Rojszczak M, 'Gone in 60 Minutes: Distribution of Terrorist Content and Free Speech in the European Union' (2022) 18(2) (International Journal of Law and Information Technology 149).

Rotaru v Romania (Application No 28341/95) (ECtHR, 4 May 2000)

Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in S Gutwirth, Y

Poullet, P De Hert, C De Terwangne and S Nouwt (eds), *Reinventing Data Protection?* (Springer 2009) 45–76.

Samonte M, 'Google v CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law' (Insight, European Papers vol 4, no 3, 2019) 839–851.

Sever T, 'Public Benefit and Public Interest in the Slovenian Legal System – Two Sides of the Same Coin?' (unpublished manuscript, University of Ljubljana, Faculty of Public Administration, 20 June 2025).

Staunton C, Slokenberga S and Mascalzoni D, 'The GDPR and the Research Exemption: Considerations on the Necessary Safeguards for Research Biobanks' (2019) (27 *European Journal of Human Genetics* 1159).

Teixeira G, Pinho MF and Teixeira H, 'Access to Financial Information for Tax Purposes and Proportionality – Balancing Public Interest with the Protection of Privacy' in Monica Rosini and Gloria González Fuster (eds), Data Protection and Tax Information Exchange (Springer 2023).

Tichý L, 'Public Interest and its Importance in Law' in L Tichý and M Potacs (eds), Public Interest in Law (Intersentia 2021) 25.

Van Camp N Dierickx K and, 'The retention of forensic DNA samples: a socio-ethical evaluation of current practices in the EU' (2008) (34 Journal of Medical Ethics 606).

Vedaschi A and Lubello V., 'Data Retention and its Implications for the Fundamental Right to Privacy: A European Perspective' (2015) 20(1) (*Tilburg Law Review* 14–34).

Vogiatzoglou P, *Mass Data Surveillance and Predictive Policing: Contested Foundations and Human Rights Impact* (Routledge 2025).

Waind E, 'Trust, Security and Public Interest: Striking the Balance – A Narrative Review of Previous Literature on Public Attitudes towards the Sharing, Linking and Use of Administrative Data for Research' (2020) (5 International Journal of Population Data Science 3).

World Health Organization, *SMART Trust (v1.2.0) – Ethical Considerations and Data Protection Principles, HL7® FHIR® Standard v5.0.0* (WHO 2024).

Jorida Xhafaj, 'The Right to Be Forgotten: A Controversial Topic Under the General Data Protection Regulation' (2019) 7 *International Scientific Conference of Faculty of Law – University of Latvia* 26

Zhou J and others, 'A unified method to revoke the private data of patients in intelligent healthcare with audit to forget' (2023) 14(1) (*Nature Communications* 6255).

Yazar Beyanı	
Yazarların Katkıları	Bu çalışma tek yazarlıdır.
Mali Destek	Yazar, bu çalışmanın araştırılması, yazarlığı veya yayınlanması için herhangi bir finansal destek almamıştır.
Çıkar Çatışması/Ortak Çıkar Beyanı	Yazar tarafından herhangi bir çıkar çatışması veya ortak çıkar beyan edilmemiştir.
Etik Kurul Onayı Beyanı	Çalışmanın herhangi bir etik kurul onayı veya özel bir izne ihtiyacı yoktur.
Araştırma ve Yayın Etiği Bildirgesi	Yazar, makalenin tüm süreçlerinde TRÜHFD'nin bilimsel, etik ve alıntı kurallarına uyulduğunu ve verilerde herhangi bir tahrifat yapılmadığını, karşılaşılacak tüm etik ihlallerde TRÜHFD'nin, yayın ve editör kurullarının hiçbir sorumluluğunun olmadığını beyan etmektedir.