The PoSeID-on Blockchain-based platform meets the "right to be forgotten"*

Giovanni Maria Riccio - Adriana Peduto - Fabiola Iraci Gambazza - Luigi Briguglio - Elena Sartini - Carmela Occhipinti - Iván Gutiérrez - Domenico Natale

Abstract

Adoption of disruptive technologies, such as blockchain and artificial intelligence, is more and more raising citizens' suspiciousness based on (i) lack of trusted information, (ii) perception of intrusiveness on privacy and human rights, (iii) disrespect of legal obligations (including GDPR), and (iv) misalignment and lack of cross-fertilization between technology and legal experts. This paper aims at demonstrating how the technology is not a per se issue, as it can be used to create an ecosystem which can deliver a significant and measurable value to citizens and customers and the whole community. In this perspective, this paper describes the legal framework, the method and the results that are behind the compliance analysis of the Blockchain-based platform developed within the context of the PoSeID-on project.

The paper, in order to identify the ethics and legal requirements used to perform the assessment of the PoSeID-on technology, introduces the ethics and regulatory framework on human rights, privacy, and data protection. The procedure for the assessment of the technology is described as well. An overview of the Poseidon project and its implemented Blockchain-based platform allows the reader to fully understand the objectives of the project, as well as the peculiarity of the specific implemented technology that has been designed to overcome many obstacles (e.g. regulation compliancy, individuals and organizations trust, investment size). Consequently, the paper describes the results of the compliance assessment performed on the PoSeID-on Blockchain-based platform. The paper concludes by showing that important aspects such as trustworthiness and sustainability can definitely contribute to improve the social acceptance of disruptive technologies, such as the PoSeID-on one, and consequently their wide adoption.

* Su determinazione della direzione, in conformità all'art. 15 del regolamento della Rivista, l'articolo è stato sottoposto a referaggio anonimo.

Giovanni Maria Riccio - Adriana Peduto - Fabiola Iraci Gambazza - Luigi Briguglio - Elena Sartini - Carmela Occhipinti - Iván Gutiérrez - Domenico Natale

Summary

Keywords

PoSeID-on - right to be forgotten – blockchain - GDPR – data protection

1. Introduction

This paper is structured in 5 main paragraphs:

- "The Legal and Ethics Framework" aims at describing the legal and ethics conceptual framework of privacy and data protection as fundamental human rights. These fundamental rights are analysed historically so that the reader may comprehend the rationale behind GDPR's introduction. In particular, this chapter analyses the historical evolution of the "right to be forgotten", from its first interpretation and implementation in EU Member States' national courts according to the case-law of the European Court of Justice and finally to the definition set forth in Art. 17 GDPR.
- "Requirements and Assessment Procedure" describes the legal and ethics requirements with which designers and the implementers of a system dealing with personal data management are expected to be compliant. These requirements are fundamental elements of the assessment criteria. Moreover, the chapter describes the tools and techniques adopted for compliance assessment, including the procedure and the assessment report.
- "The PoSeID-on Project and Blockchain-based platform" describes the PoSeID-on project objectives and the specific features and advantages introduced by its implemented Blockchain-based platform. Details on the rationale behind the design choices are provided as well.
- "Compliance Assessment" begins by outlining the conceptual framework in which Art. 17 GDPR is included and the requirements identified to ensure its respect within the project. Then, the chapter describes how the platform generated by the PoSeID-on project is compliant with said requirements and, consequently, with the European legal and ethics framework. In particular, the chapter will consider the use of blockchain technologies by the platform and the fact that the solutions adopted are fully respectful of legal obligations, including those held by the GDPR. Due to the specific technology, that is based on "immutable storage", major focus is reserved to the right to be forgotten.
- "Trustworthiness, Sustainability, and Ethics-driven Technologies" describes how misrepresentation and/or lack of information can impact on trustworthiness and consequently on the social acceptance of disruptive technologies. On the other

hand, the ethics-driven approach adopted by the PoSeID-on project allows to overcome obstacles, such as regulation compliance, individuals' and organizations' trust, investment size. To that extent, a techno-regulatory interoperability lays the foundation for innovation, trustworthiness and sustainability.

This paper closes with "Conclusions" where the main achievements of the PoSeID-on project's research activity are summarised, focusing on the design and development of an ethics-driven approach for guaranteeing privacy and data protection, and specifically the right to be forgotten.

2. The legal and ethics framework

In order to properly understand the rationale behind the legislative solutions of the General Data Protection Regulation (Regulation (EU) 2016/679) ("GDPR")[1] and notably behind the right of erasure (or the right to be forgotten) it is necessary to review the path that these rights have traced during the last decades, firstly in the national case-laws and, in the last decade, in decisions of the European Court of Justice that have strongly influenced the text of the Art. 17 GDPR.

The right to privacy and the right to data protection are two fundamental rights aimed at protecting individual freedoms, as well as to enable the individual to exercise other fundamental rights such as free speech or the right to assembly.

The recognition of the right to privacy or to a "private life" as "fundamental" for both the individual and for society as a whole, has been made either at the international level (Universal Declaration of Human Rights - Art. 12), and at European level (the European Convention of Human Rights - Art. 8)). In particular, the EU constitutional "fathers", also taking into consideration decisions of the EU Member States courts, as well as their constitutional traditions, established that the right to privacy and the right to the protection of personal data are fundamental rights (respectively provided in Arts. 7 and 8 of the Charter of Fundamental Rights of the EU, 2007[2]).

In this respect, for the purposes of the present paper, the focus will be on Art. 8 of the Charter of Fundamental Rights of the European Union. Indeed, Art. 8 provides that «Everyone has the right to the protection of personal data concerning him or her» and, in the second paragraph of the above-mentioned article, that «Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law». Art. 16 of the Treaty on the Functioning of the European Union (TFEU)[3] provides similar statements, which are also recalled by the first recital of GDPR.

Even if the recognition of data protection as fundamental rights arrived only with the entry into force of the Charter of Fundamental Rights of the European Union, the introduction of protection of personal data has been already provided in the Direc-

[1] "General Data Protection Regulation (GDPR)", 2016.

[2] European Parliament, Charter of Fundamental Rights of the EU, 2007.

[3] Consolidated version of the Treaty on the Functioning of the European Union, 2012.

tive 95/46/EC[4].

After 20 years, an update was necessary for at least two main reasons. On one hand, the margin of discretion left to EU Member States led to several discrepancies among them, due to national implementation and provisions/decisions of the national data protection authorities. On the other hand, the technological evolution caused a dramatic change of the regulated scenario, which required a different and proper regulation since the actual one was not sufficient to meet all the new challenges.

In light of these considerations, in 2016, GDPR was finally approved, replacing and superseding Directive 95/46/EC. Specifically, GDPR provided for detailed explanation of data subject rights, set forth from Art. 15 to Art. 22, including among them, the right to erasure, also known as right to be forgotten (even if the two notions are not perfectly corresponding).

In particular, the right to be forgotten is a subjective right (not an absolute one) that can be understood as the right to an informative self-determination concerning the right, the power, of an individual to decide for the transformation into anonymity of the data related to him or her, or for its erasure/deletion[5].

This concept, from a historical perspective, first emerged in decisions ruled by US Courts in the last decades of the past century, as an evolution of the "right to be let alone", and in more recent times in Europe, at the turn of the 80s and 90s of the last century.

Following this evolution it is possible to say that the right to be forgotten holds that a piece of information concerning an individual, although true and appropriate, cannot be brought back to public opinion, after a considerable period of time, from its original diffusion or from the fact that the news itself occurred, provided that there is no longer a specific public interest, (i.e. the information is not relevant) tied to its publication or disclosure. This means that it is necessary to conduct a balancing operation among the interests, whereby the interest in information will therefore prevail on the right to be forgotten only where the piece of information is still relevant.

To better understand the scope of this right it is worth to quickly analyze some of the most important EU case laws. In this respect, however, it is important to stress that even if the great majority of these case laws concerns the balancing between the said right and the free press, the perimeter of scope of the right to be forgotten is not limited to that area, but, on the contrary, pursuant to the wording used in Art. 17 of GDPR its potential application is much more general.

Before GDPR, the main European jurisdictions developed an interpretation and application of the right to be forgotten, that has confirmed the existence of this right, although through an interpretative process shaped on a case-by-case analysis.

In 1973, the German Constitutional Court affirmed that, even if a right to publish information about the personal life of a criminal when it's sure she or he is guilty does

[4] 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.

[5] A. Berti, *Il diritto alla cancellazione*, in R. Panetta (ed.), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato*, Milano, 2019.

exist, the effect of constitutional protection of the personality would represent a limit to communication. Indeed, debating and spreading specific information beyond the essential ones about the offender private life is not allowed.

Again, it is worth to mention the decision of the Court of first Instance of Rome (November 21, 1996) which attempted to give a first definition of the right to be forgotten as: «the legal situation of which the precautionary protection is invoked appears identifiable in what defined "right to be let alone"». More recently, the Italian Court of Cassation (decision no. 16111/2013), stated that «the subject's right to claim that his or her past personal affairs are publicly forgotten is limited in the right to report only when there is an actual and current interest in their dissemination, in the sense that what has recently happened is directly connected with those events and renews their relevance, otherwise the public resolves an improper connection between the two bits of information in an illegal infringement of the right to privacy»[6].

Similarly, the French case-law specified that the right to be forgotten could be invoked by a person who, having paid his or her debts to justice by completing a path of social rehabilitation, legitimately asked not to be perpetually associated with events of her or his past, as they probably no longer reflect his/her current personality[7] (in contrast, a minority French doctrine has also questioned the need for a subcategory of the right to be forgotten, which specifically affects people who have suffered judicial convictions).

On the other side, in 1997 the Court of Appeal of Montpellier held that the right to be forgotten couldn't be recognized in an absolute form. Depending on the circumstances, such as the length of time passed from the crime, the gravity of the facts, at the end of the condemnation time, the judge admitted the legitimacy to obtain the erasure of the criminal information, when its recall no longer meets any ethic, historical, or scientific need.

Besides, in the Case EWHC 799/2018, the Queen's Bench underlined that the concept of journalistic news had to be interpreted in a matter not so flexible to include every activity that contains information or opinions[8]. Instead, in Spain, the right to be forgotten must be balanced with the historical interest of the facts[9]. Furthermore, the Belgian Court declared that a person who was condemned has the right to be forgotten, based on the Art. 8 of the European Convention of Human Rights of the Council of Europe and the 19 of International Act about civil and political rights[10].

However, at the EU level, the landmark case that better clarified the balance between the right to communication and the right to be forgotten was the *Gonzalez vs. Google Spain* (case C-131/12, Mario Costeja Gonzalez and AEPD – *Agencia Española de Protección de Datos*) decided by the Court of Justice of the European Union (CJEU) .

An analysis was conducted considering three different perspectives (i.e. the processing of personal data, the applicability of the Spanish laws to Google, and the obligation

6 Italian Supreme Court, judgment no. 16111 of 26 June 2013.

7 *Tribunal Grande Instance Paris*, 25 March 1987, in *Dalloz,* somm. 198, 1998.

8 Judgment available online at *judiciary.uk*.

9 Spanish Supreme Tribunal , 2013.

10 *Tribunal de Première Istance,* 1997.

to intervene to protect the right to be forgotten) concerning the relationship between the Internet and the right of erasure[11]. The CJEU concluded that, in order to be able to verify the applicability of Arts. 12(b) and 14(1)(a) of Directive 95/46/EC, it was necessary to ascertain whether the interested party had the right to the information concerning him to be no longer linked to his name, through a list of results deriving from a search carried out starting from his name. The right to be forgotten invoked by the interested party would prevail not only towards the operator of the search engine - and its underlying economic interests - but also in the interest of the public to access the information in question when searching the name of this person - unless it appeared, for some reason, that the role played by this person in public life was fundamental enough to justify the interest of the community in accessing this news. According to the CJEU, however, there was a limit to the claim of the right to be forgotten: obviously the search engine operator could not delete the personal data on the source of the information, but its duty should be limited to the deindexation or delisting of the reference among those included in the search engine's results.

After the Costeja Gonzales case, in November 2014, the Working Party Article 29 ("WP29") published the guidelines about the implementation of the right to be forgotten, in which a common line of interpretation for the national data protection authorities to follow was provided in order to ensure a correct adaptation of the internal regulations to the CJEU ruling[12].

After these guidelines, the French data protection authority – CNIL (*Commission nationale de l'informatique et des libertés*) - had ordered Google to delete the links redirecting users to obsolete news, not only stored within the European territory or on European sources of information but also outside Europe.

In the United Kingdom, the Google C-131/12 judgment has prompted the European Union Committee at the House of Lords to draft a report, in which it was argued that the new EU data protection legislation expressly provides that the search engines cannot be qualified as data controllers. As for the other national privacy guarantors, the Dutch Data Protection Authority (CBP) has not drawn up any guidelines regarding deindexing activities but refers to the indications of the WP29. The Spanish Data Protection Authority (AEDP) has introduced an ad hoc space on its website in which it explains the right to be forgotten, providing the guidelines to be followed for the privacy authorities.

Nevertheless, first the Google Spain ruling, then the interventions and decisions of the various data protection authorities and the guidelines of the WP29, influenced the

[11] CJEU, C-131/12, *Google Spain* (2014).

[12] Article 29 Working Party, Opinions and Recommendations. For the sake of completeness, it is appropriate to recall the previous judgment of the ECHR of 16 July 2013 (*Węgrzynowski and Smolczewski v. Poland*, app. 33846/2007). This ruling addresses a case similar to Google Spain, but with a different methodological approach. The European Court of Human Rights has ruled, with the decision of 16 July 2013, on the balance between freedom of the press and the right to reputation in cases of dissemination of articles via the internet. In the case in question, however, the right to be forgotten is not really emphasized. Specifically, the Court considered the elimination of an article from the website of an online newspaper a disproportionate measure, despite the fact that the national judges had considered the text published in the paper's adaptation of the newspaper defamatory, bringing it back to the context of protecting freedom of expression the web archives of newspapers.

drafting of the European Regulation on Data Protection.

As mentioned, Art. 17 of GDPR provides the right to obtain the cancellation of personal data, without delay, provided that specific conditions are met[13]. The second paragraph of the same article holds that the data controller who, in the presence of the conditions described, is obliged to delete personal data, must necessarily «taking into account the available technology and implementation costs, adopts reasonable measures, including technical, to inform the data controllers that they are processing personal data of the request of the interested party to delete any link, copy or reproduction of his personal data». Therefore, the reference to the right to be forgotten, placed only in brackets in the article next to "right to erasure", and in the context of a provision dedicated to the erasure of personal data, seems to frame this right within the right to erasure.

Indeed, the heading of the article was, during the preparatory work, "right to be forgotten or right to erasure", a formula then abandoned because the adversarial conjunction could have generated confusion.

Despite the mention made by Art. 17 of GDPR, the right to be forgotten as well as the right to erasure are not defined. However, the case-law of the CJEU made clear the boundaries of this notion, granting to individuals the right of being deindexed from search engines, and to the correct contextualization of data that are no longer actual.

In this respect, two judgments of the CJEU on the right to be forgotten on 24 September 2019 are useful to understand how the right to be forgotten is being conceived within the EU. The first decision relates to case C-507/17 between the CNIL and Google Inc. and concerns the territorial extension of the de-indexing. There is no obligation, deriving from Union law, to carry out such deindexing on all versions of its engine for the provider, but it must be done, however, in the search engine versions of all EU member states[14]. The other ruling of the CJEU (case C-136/17) raised from another question posed by the French Council of State, concerning the processing of sensitive data by search engines. The Court reiterated that the indexing activity carried out by search engines must be considered "processing of personal data" and therefore subject to the limitations currently provided for by the GDPR, and previously by Directive 95/46/EC, as regards the treatment of sensitive data[15].

This brief and necessarily incomplete overview on the right to be forgotten explains how this right has changed from its debut in the legal discourse. In fact, at the beginning of its application by the national courts, it was considered to belong exclusively

[13] The conditions are: a) personal data are no longer necessary with respect to the purposes for which they were collected or otherwise processed; b) the interested party revokes the consent on which the treatment is based, and there is no other legal basis for the treatment; c) the interested party opposes the processing for his/her particular situation and there is no prevailing legitimate reason to proceed with the processing, or she/he opposes in relation to personal data that are processed for direct marketing purposes; d) personal data have been unlawfully processed; e) personal data must be erased to fulfil a legal obligation under Union law or under the law of the Member State to which the data controller is subject; f) personal data have been collected in relation to the offer of information society services in accordance with the provisions of art. 8 regarding the consent given by minors.

[14] CJEU, C-507/17, *Google v. CNIL* (2019).

[15] CJEU, C-136/17, *GC and others* (2019).

to public figures and not to private citizens. In fact, only public figures were interested by the mass-media analysis, while private persons were outside this process and were only spectators of this news. The spreading of Internet and the facilitation of collecting and indexing information has determined that also private persons may be covered by this right. In fact, these persons may be "googled" as well and their personal information may be easily found through a search on the major search engines; thus, it is essential that the events which may be harmful for their reputation are not that effortlessly located by other users. Furthermore, the balance between the right to be informed or the right to research, on the one side, and the right to not being eternally "labelled" for an old behaviour, may coexist, provided that the information would not be cancelled from the source where it has been published, but exclusively deindexed.
However, the right to erasure cannot be limited to this aspect, because, as above exposed, Art. 17 provides a wider provision, with several limits. In other words, the right incorporated in Art. 17 is not absolute, but can be exercised only in specific situations, which are listed in the first paragraph of the article itself. In particular, this case occurs where «the data subject withdraws consent on which the processing is based» and «there is no other legal ground for the processing». Other interesting hypotheses, for the purposes of this paper, are mentioned by letters (a) and (d) of para. 1 of Art. 17 which respectively state that the right to erasure can be applied if the personal data have been unlawfully processed.
On the other side, this right is balanced by the provisions held in para. 3 of Art. 17, which enumerates the cases in which to right to erasure cannot be applied. The most relevant assumptions for our goals are those listed in letters (b) and (e), and which respectively allow the retention of the data if this retention is necessary in order to comply with a legal obligation or for the establishment, exercise or defense of legal claims.

3. Requirements and assessment procedure

In light of the abovementioned legal and ethics framework, special care must be devoted to (i) analyse the architecture's specifications of a system that manages personal data, (ii) selecting the technology available from the state of the art, and (iii) how the technology is instantiated. Indeed, these factors could raise legal and ethics concerns and have deep impacts on data protection.
In this regard, apparently, the right to be forgotten may be in conflict with blockchain technologies, as long as these technologies are shared and synchronized with digital databases based on a consensus algorithm and stored on multiple nodes and stored in an "append only" mode. Indeed, all the data are collected, stored and processed in a decentralized way, where each node of the network contains all the data and it can control them; blocks can be added, but they cannot be deleted (i.e. immutability property of blockchain).
Therefore, the right to be forgotten/to erasure cannot be guaranteed.
Nevertheless, in order to find some elements of compatibility, some solutions have been already advanced by the CNIL in September 2018 with the publication of the

official document "*Premieres éléments d'analyse de la CNIL*" according to which the possibility to plan the destruction of the private key (that is used to decrypt the data in the blocks) has been foreseen so as to render inaccessible the data that remain stored within the chain (i.e. data is not effectively erased from blockchain)[16], but at that point cannot be consulted[17]. In practice this solution makes data lost in a "black hole" and, at the current state of the art, it is impossible to recover these data.

Another possible solution might be the one concerning the implementation of some of the erasure methods that can make data "forgettable" in blockchain, even if they do not guarantee the permanent deletion of data. An example is represented by pruning, a technique used with bitcoin, that allows a reduction of the storage of data for the user of the blockchains[18], deleting the old and historical blocks[19]. However, this solution could impact on the reliability of the blockchain itself, and trade-off considerations must be taken into account (i.e. size of erased data versus size of the blockchain)[20]. Moreover, it is important to stress that, even if pruning consists in the removal of old blocks, all the information necessary to recreate the older state is still saved on each node[21].

The last solution is to "fork" the blockchain (i.e. resetting the rules of the chain) with the creation of a new ledger[22]. However, due to the nature of the blockchain, this solution implies the coordination of all involved nodes, and its implementation and management could be difficult to achieve and also unprofitable.

Many other futuristic solutions are also mentioned in the literature, proposing inter-alia reversibility or edit-ability features. However, these solutions are not mentioned in this paper in consideration of the fact that they don't focus on evaluating solutions based on blockchain technologies already available in the current state of the art. Moreover, these proposed solutions usually don't address the erasure of data, that in the end remain stored in the blockchain, and require the destruction of the private key as well.

Besides the aforementioned possible solutions, the European Parliamentary Research Service published in July 2019 a study entitled "Blockchain and the General Data Protection Regulation. Can Distributed Ledgers be Squared with European Data Protection Law?", in which three solutions to reduce the gap between the GDPR and blockchain, called "Policy Options", are presented. The publication considers the GDPR as a neutral technological regulation, and as such flexible enough to be adapted upon the evolution of new technologies.

The first solution presented concerns the adoption of a regulatory guidance, due to

---

16 CNIL, *Blockchain*, September 2018.

17 The European Union Blockchain Observatory & Forum, *Blockchain and the GDPR*, 16 October 2018.

18 G. Ateniese – B. Magri - D. Venturi - E. Andrade, *Redactable Blockchain – or – Rewriting History in Bitcoin and Friends,* 2016, in *eprint.iacr.org*.

19 S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System,* in *bitcoin.org*.

20 E. Palm, *Implications and Impact of Blockchain Transaction Pruning*, in *diva-portal.org,* July 2017.

21 European Parliamentary Research Service, *Blockchain and the General Data Protection Regulation. Can Distributed Ledgers be Squared with European Data Protection Law?,* July 2019.

22 M. Finck, *Blockchains and Data Protection in the European Union,* in *European Data Protection Law Review*, 4(1), 2018, 17 ss.

the difficulty to understand the blockchain structures and the application of, and correlation with, the GDPR, regarding some concepts such as data controller and right to erasure. The second one, concerns the implementation of codes of conduct and certification mechanisms; while the last one is an interdisciplinary research finding common approved solutions (such as: the creation of governance mechanisms, development of protocols, etc.)[23].

These proposed solutions, available at the state of the art, represent a set of suggested recommendations for the development team that is approaching a personal data management system.

Moreover, it is requested to the development team to integrate the legal and ethics requirements, defined in Table 1, in the system requirement specification[24]. These requirements focus on the individual rights of the data subject, and consequently these directly or indirectly guarantee the compliance with GDPR art.17, as well as the Arts. 15-21.

A relevant role is played by Arts. 5 (Principles) and 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject) of the GDPR, dealing with the transparency of the system: these articles encompass additional requirements that provide guidance in terms of transparent governance of data, communication and modalities for the exercise of the rights of the data subject. These requirements lay the foundation for the assessment procedure of the building personal data management system. In other words, each requirement has to be satisfied and the development process has to gather and provide detailed justification for the compliance.

Table 1: Legal and ethics requirements

Requirement Id	**Requirement description**	**GDPR**
LER1	Secure and reliable identification, authentication and data access should be ensured.	Arts. 5, 15, 25 and 32
LER2	A withdrawing mechanism should be available in the platform.	Arts. 7 para. 3, and 17
LER3	A mechanism should be implemented to identify the specific data that is to be blocked or restricted.	Arts. 18, 21 and 25
LER4	Extracted data should be limited to the identified and authenticated person concerned and communicated securely (e.g. encrypted).	Arts. 5, 25 and 32
LER5	Appropriate information should be provided to individuals to exercise their rights and to ensure transparency.	Arts. 5, 12, 13 and 14, and 37

[23] European Parliamentary Research Service, *Blockchain and the General Data Protection Regulation,* cit.

[24] PoSeID-on, *PoSeID-on blockchain - Interim implementation*, 2019.

LER6	Appropriate procedures for the governance of the system and its operations should be identified and adopted in case of exercise of the rights.	Arts. 5 and 12

4. The PoSeID-on Project and Blockchain-based platform

The PoSeID-on project – which stands for "Protection and control of Secured Information by means of a privacy enhanced Dashboard" – is a Research and Innovation project financed under the EU Horizon 2020 programme. Started in 2018, the project has been running for 30 months as of this paper's completion.

PoSeID-on arose from the General Data Protection Regulation (GDPR) implementation challenges, and the security issues related to the management of digital identities. Its final aim, indeed, is to transform the perception of GDPR as an administrative burden into a more widely accepted approach to see GDPR as an opportunity and an added-value for citizens, public, and private entities, reinforcing transparency and trust in society, especially towards public administrations.

To achieve this objective, PoSeID-on is developing an innovative and intrinsically scalable platform for personal data protection, aimed to safeguard the rights of data subjects as well as to support organizations in data management and processing, while ensuring compliance to the GDPR. The platform, accessible through electronic identification (eID) accounts, enables users to securely grant, revoke and check Personal Identifiable Information ("PII", i.e. information related to a Data Subject, that can be used to directly or indirectly identify the person) permission to digital service providers. As a result, the PoSeID-on platform empowers users in managing the PII processed by public and private organizations, and at the same time it helps those organizations to guarantee the rights of data subjects and be in line with the privacy legal framework.

The solution is based on the use of innovative technologies, such as a custom permissioned blockchain, which can allow secure data management and personal identifiable information exchange.

The goal of including an implementation based on a blockchain platform is to provide the secure and trustable means to operate with individual permissions. Indeed, it increases the confidence of European citizens in the operations that administrations and companies make with their personal data. The perception of control rises, and respect for the application of regulations - such as the GDPR - is greater.

To summarize the capabilities of the decisions made during the design phase, the following guidelines have been defined throughout the development process for addressing the ethics and legal requirements defined in Chapter 2:

- Personal data is not stored nor transmitted in the blockchain network, which handles permissions transactions over personal data. However, permissions themselves belong to PII.
- A permissioned blockchain network will ensure a secure and reliable identification, authentication, and data access, acting as a distributed and secure means to

audit PII transactions, enabling a secure control over personal data.

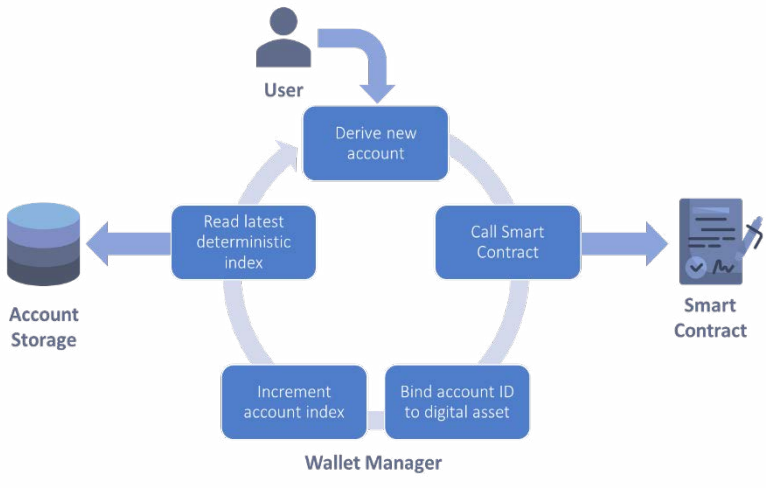
- Smart contracts, that define the user-centric permission management functionality, will be the mechanism to get the information only to the right person, ensuring the privacy of personal data transactions.
- The user operations will allow the Data Subject to enforce permission on specific data, whenever Data Controllers or Data Processors ask to use them on a service.
- The development of an application programming interface (API) allows the Data Subjects to access their own personal data and retrieve them within personal area (a.k.a. personal wallets) from mnemonic words. Only the Data Subject can know and access his/her wallet. The wallet can be created again in case of key loss, using the same mnemonic that was used the first time and giving the user the full control.
- A blockchain client is mandatory to control and get informed on the status of transactions in the blockchain. This decentralized access mechanism will prove that Data Processors are doing what they claim to do. It will be incorporated in the Privacy Enhanced Dashboard (PED) of PoSeID-on for ease of use.

Blockchain general philosophy is thought to permit the traceability of the user actions. Depending on the context of application and the platform/technology used, the level of knowledge the system has about the user identity can be greater or lesser. The strictest may require strong, even advanced, identifiers. While others (typically networks meant for public use) will allow pseudonymizing user identities by cryptographic means. Even if the Data Subject's Personal Identifiable Information (PII) is encrypted, it is still associated with a pseudonymous identity. The objective of this project is to ensure a use of blockchain that allows anonymizing operations to the point that the citizens themselves can exercise the data subject rights according to the GDPR.

To the controversial solutions from the current state of the art, mentioned in Chapter 2, the PoSeID-on project alternative approach for ledger management is based on the so-called "Burnable Pseudo-Identity" principle. This ensures that the PII of the Data Subject is not traceable by anyone looking to the transactions. The underlying principle of this proposal overcomes most of the state-of-the-art proposals by (i) implementing a mechanism of continuous refresh and rotation of identities in order to further reduce traceability; and (ii) giving back the PII control to the Data Subject by letting her/him the choice to "remember" or "forget" their identifiers. The aim of this shared mechanism is to allow user interactions in a way that they can only be traceable during the time the user is using the PoSeID-on services, and it can be compliant with GDPR and "right to be forgotten" when the user stops using these services (or upon request).

The behaviour of this method is described in Figure 1. The first step is the creation of the wallet that will contain the pseudo-identity, formed by the set of accounts belonging to the user. The wallet (as a container) and the accounts inside it are protected by encryption. A new account is derived when the user needs to interact with the blockchain network. That account is the one selected to call the Smart Contract. As this is the first time that the account is used, it is not related to other transactions and

will not leave any history trace when updating the ledger. Nevertheless, the account will be bound off-chain to the interaction, so the user can decide when to destroy it. When an account is already used and verified, the account index is incremented. That deterministic index is used to select the next account and get it prepared for the next user interaction.



(Figure 1: Schema of "Burnable Pseudo-Identities" principle)

The created mechanism is user-centred, since it allows users to have absolute control of the information known about them. Furthermore, although all protections are maintained, the difficulty of using blockchain is made transparent, and the problems related to understanding and storing cryptographic keys are smoothed out.
Each Data Subject will have an identity in PoSeID-on through the binding of a set of their pseudo-identities, made up of identifiers and actions. Only one action is performed per identifier and authorised Data Processors can provide their services managed by PoSeID-on. Once the Data Subject identity is burned, the cryptographic pseudonymous identifiers can't be re-engineered by the application, it will never again be used by the system and the Data Subject can't be traced in the future.
The pseudo-identities are created by the users, or by the PoSeID-on platform with authorization of the user. It involves a random seed (as an entropy source) and a secret for symmetric identity encryption. The user is the only one who knows the secret and the identity remains hidden and securely protected while it's not being used.
All these actions take place to ensure the compliance with ethic requirements. One of them is the prohibition of using an identifier after its lifetime period. Any data verified and chained to the ledger that is erased will cause a cryptographic error and a chain break. So, the data must be created in a way that it can be unlinked if needed. This is the purpose of the Burnable Pseudo-Identity. The other reason is the unlinkability, by which an irreversible way of creating new child keys from parent keys (but not otherwise) is not linkable with previous information.

5. Compliance assessment

In order to comply with the self-responsibility and accountability principles, on which the architecture of the GDPR is based, the Consortium stands by the opinion that the measures implemented ensure a full data protection assessment. In particular, these measures fulfill the transparency principle sets forth in Art. 5(1)(a) GDPR, and then better specified in Arts. 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject) and subsequent of GDPR, which requires that personal data are processed in a transparent manner in relation to the data subject.

Furthermore, this assessment analyses the technological implementation and guarantees the exercise of the rights of the individuals, whose personal data will be used by the platform and by third parties, and notably the right erasure regulated by Art. 17 GDPR.

From a strictly legal point of view, it has to be noted that the procedures to be executed are not compulsory as they are not formally necessary under the current regulations. Anyway, as mentioned, the approach of the GDPR is aimed, on the one hand, at empowering the data subjects, and, on the other hand, at leaving to the data controller and data processor(s) the choice of adopting the organizational and technical measures considered to be relevant for efficiently guaranteeing the personal data protection. For the PoSeID-on platform, the following seven measures have been considered, according to the Legal and Ethics Requirements as well.

Measure 1. Combination of digital certificates and digital signatures.

To ensure the identification and permission information access that are managed in blockchain by the PoSeID-on platform, a key component is combining the use of digital certificates with the digital signature in every transaction that ensures the non-repudiation. The digital certificates are directly related to the used Blockchain keys that allow recovering the user identifiers, because they help to keep them securely without being shared. These actions, along with the immutable character of the registry, allow an authenticated management of permissions and based on computational trust. The design of PoSeID-on has been made considering the distributed character of the registry too. The communication between parties to control the permissions satisfies the values of privacy, scalability, traceability, and access control needed by the Data Processors. The communication between them is done through private end-to-end encrypted messages that include mutually authenticated Transport Layer Security (mTLS) to avoid message spoofing attacks, and where the rest of the network parties are un-aware of that communication.

This measure satisfies the legal and ethics requirement identified as LER1 (Secure and reliable identification, authentication and data access).

Measure 2. Hiding complex technology implementation behind one-click button

Data subjects are allowed to withdraw consent for the access to PII in accordance to the GDPR. To achieve this, the web-based dashboard has implemented this functionality as a simple button, giving data subjects exactly this kind of control. Behind the scenes this button revokes the access permission using the Blockchain API and submits an automatic request for PII deletion to all data processors with delegated access to this information.

This measure satisfies the legal and ethics requirement identified as LER2 (withdrawing mechanism available in the platform).

Measure 3. Permission Lifecycle Model

A proper permission model has the power to avoid rogue parties and spammers. The PoSeID-on platform controls the allowance of permission requests by its Smart Contract design. The permissions can adopt different states (REQUESTED, ALLOWED, DENIED or EXPIRED), ordered in a flow that becomes the permission lifecycle. Those permissions can be updated to notify state changes. The access to information of a blocked or restricted permission requested by an unauthorised party is automatically denied by the Smart Contract, because the permission state is not ALLOWED.

This measure satisfies the legal and ethics requirement identified as LER3 (Mechanism to identify the specific data that is to be blocked or restricted).

Measure 4. Data Exchange management by design

The PoSeID-on platform offers a standardized data exchange management by design. Personal data is no longer exchanged between parties directly, but flows through the PoSeID-on platform enforcing access and security rules. This "man in the middle" functionality, however, introduces a privacy concern; whoever controls the PoSeID-on platform, can potentially access all personal information flowing through it. To prevent this from happening, the PoSeID-on platform comes with a Data Processor API Client, which is a piece of software that runs on the premises of the data processor. This application enforces end-to-end encryption among parties (both data processors and data subjects) using a custom protocol, leveraging cryptography supplied by libsodium[25] (a modern software library and fork of NaCl[26] Networking and Cryptography library). All personally identifiable information (including requests for data access permission to the data subject!) can only be read by the intended recipient.

This measure satisfies the legal and ethics requirement identified as LER4 (Extracted data are limited to the identified and authenticated person concerned and communicated securely).

Measure 5. Erasure Event and Notifications

The platform allows the data subject to erase data through the web-based dashboard, enabling the procedures for ensuring the right to be forgotten. Moreover, when this

[25] *Introduction – libsodium*, in *doc.libsodium.org,* 2020.

[26] *NaCl: Networking and Cryptography library – Introduction*, in *nacl.cr.yp.to*, 2016.

event occurs, the platform itself automatically sends a notification to the data subject, in order to transparently acknowledge receipt of the request and the enactment of erasure process.
This measure satisfies the legal and ethics requirement identified as LER5 (Appropriate information to be provided to individuals to exercise their rights and to ensure transparency).

Measure 6. Specified Events and Processes

For each specified event, the platform has defined a set of codified processes and the operations to be performed in compliance with the legal and ethics framework defined in Chapter 1, including EU data protection regulatory framework as well. These procedures include the actions to be taken inter-alia in case of permission restrictions, and in case of exercise of the right of erasure.
Specifically, for the latter, from the receipt of the request of the data subject, the data will be deleted by the platform within the period specified in the terms and conditions. Needless to point out that this means that the data can be deleted by the platform (and by all the instruments and tools connected with the platform itself), but not from databases, servers, and so on, if owned and managed by the Data Processors and their potential third parties. In other words, PoSeID-on (in its role of manager of the Platform) and the subjects which have joined the Platform, by accepting its terms and conditions, acts as independent data controller. PoSeID-on, therefore, is not in the position to delete nor to impose the deletion to these subject.
This measure satisfies the legal and ethics requirement identified as LER6 (Appropriate procedures for the governance of the system and its operations in case of exercise of the rights).

Measure 7. Contact details of Data Processors

To achieve the facilitation for the data subject of exercising the rights granted by the GDPR, PoSeID-on, once the request for the cancellation of the data has been received, automatically communicates to the applicant the contact details of the Data Processors and their potential third parties which processes his/her personal data and, in particular, the email address of these parties, and, if present, the email address (or other relevant contact information) of the data protection officer of the third parties.
This measure satisfies and enforces the legal and ethics requirement identified as LER5 (Appropriate information to be provided to individuals to exercise their rights and to ensure transparency), already satisfied by the measure 5.
Preliminarily, even if already mentioned, it is important to remark that the right of erasure and the right to be forgotten have specific limitations and that the retention of personal data, even in case of exercise of these rights, may be legitimate and allowed by the GDPR as well as by other privacy and sectorial regulations. For instance, this is the case of the retention of personal data which are connected to the performance and the execution of a contract is permitted, in the vast majority of the member States of the European Union, for ten years after the conclusion of the contract. Similarly, the storage of the data may be required by legal obligations (such as in case of many

regulations in the health sector, which demand the retention of the data for long periods) or is necessary for the performance of a task carried out in the public interest.

6. Trustworthiness, sustainability, and ethics-driven technologies

Blockchain (as well as – inter alia - Artificial Intelligence, Internet of Things, Gene Editing, Robotics, 5G) is widely recognised to be a disruptive technology, i.e. an innovation that significantly impacts the way that consumers, industries, or businesses operate. In this perspective, a blockchain-based system sweeps the traditional systems away and replaces habits.

For this reason, it is fundamental to perform a social acceptance analysis that lays the foundation for a "human first" approach in an "ethics-by-design" development process.

Now more than ever, there is a growing need for innovative technological solutions to help society achieve a sustainable future, for both current and future generations. Moreover, this need is strongly becoming a primary "ethics requirement" for the post COVID-19 emergency management.

How a technological innovation is perceived, how much it is trusted by the society and how much society is aware of the benefits deriving from its adoption, are the main questions to be understood for the social acceptance assessment of disruptive technologies.

It is not a matter of "good or bad technology", but rather, it is the approach to defining the solution, its implementation and instantiation, as well as the way to use it, that can definitely promote the innovation and sustainable scenarios for society.

The ethics-driven approach adopted for the development of the PoSeID-on platform (based on a better understanding of the technology, the respect for human rights, and willingness to use it) is definitely aiming at reducing the barriers of diffidence and mystification against blockchain, and fostering its wider and faster deployment.

7. Conclusions

This paper remarks how the ethics-by-design approach adopted by the PoSeID-on project has allowed its platform to comply with EU regulatory framework on data protection, and specifically the GDPR.

This achievement lays the foundation on the strongly cooperation among legal and technical experts of the project, while they usually work on different isolated rooms and without having the capabilities to understand each other.

PoSeID-on platform brings the blockchain technology for the management of personal permissions and, by adopting design guidelines based on legal and ethics requirements, enables the novel mechanism of "burnable pseudo-identities" in order to perform data erasure and reduce identity traceability. The underlying principle of this

mechanism, based on (i) continuous refresh and rotation of identities and (ii) giving back the PII control during its lifecycle to the Data Subject, overcomes proposals from the current state of the art applied in blockchain technology, when dealing with personal information and compliance with GDPR. Data Controller and Data Processors can access personal identifiable information if and only if Data Subject wants. When Data Subjects opt to exercise the right to be forgotten, the platform forgets the identifiers and doesn't allow in any way to retrieve and access information that can directly or indirectly refer to specific Data Subjects fallen into forgetfulness.

More than 10 legal and ethics requirements (LERs) have been identified within the PoSeID-on project and for the implementation of its platform. In this paper, focusing on the right to be forgotten, the assessment of the implemented platform has been performed based on six LERs, covering direct and indirect areas concerning the art. 17 of the GDPR. Seven measures have been adopted to comply with the six LERs. All these measures remark how PoSeID-on platform is giving back the full control of their data to the Data Subjects.