THE IMPACT OF THE RIGHT TO PERSONAL DATA PROTECTION ON THE DESIGN OF THE EUROPEAN DIGITAL IDENTITY WALLET

Davide Baldini[*]

Abstract

The paper addresses the introduction of a unique persistent identifier in the context of the proposed reform of the eIDAS Regulation, exploring its implications in light of the fundamental right to personal data protection recognized by EU primary law. The new identifier aims to enhance identification accuracy and trust in the European Digital Identity Wallet envisaged by the eIDAS Proposal. However, it raises concerns vis-à-vis the principles of data protection by design, purpose limitation, and data minimization. It is suggested that these three principles, read together, set clear boundaries for the EU legislator when deciding the techniques used for the functioning of the European Digital Identity Wallet. The paper argues that the new identifier is not in line with the right to personal data protection, is at risk to be at odds with some Member States Constitutions, and concludes by proposing some possible ways forward.

TABLE OF CONTENTS

[*] PhD student in European and Transnational Legal Studies, University of Florence.

1. Electronic identities and EU Law

Electronic identities[1] have become increasingly widespread over the last few years, especially after the COVID pandemic[2], as they greatly facilitate activities across online platforms and services, both public and private. Within the EU, electronic identities may be either State-issued, or issued by private parties such as banks[3] or social network providers[4], albeit with different degrees of legal certainty and possibility of use, depending on Member State law and practice.

EU Law currently leaves, in fact, the possibility to create State-issued electronic identities at the discretion of Member States, providing only limited harmonization. In particular, Regulation 910/2014 on electronic identification and trust services (so-called «eIDAS Regulation»)[5] has been adopted by the European Union on 23 July 2014 and came into force on 1 July 2016. The stated aim of this Regulation, as laid down in its recitals, is to «enhance trust in

[1] Although no EU-level definition of electronic or digital identity exists, the EU Commission defines it as «a digital representation of a natural or a legal person which allows the identity holder to prove who they are during online or offline interactions and transactions», cfr. European Commission, *Commission Staff Working Document Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity*, SWD (2021) 124 final, pt. 1, par. 6.

[2] In the case of Italy, this has been the case especially for the «SPID» identities: Osservatori.net Digital Innovation, *Con la pandemia cresce l'identità digitale in Italia, ma il potenziale è ancora alto* (2021), available at https://www.osservatori.net/it/ricerche/comunicati-stampa/identita-digitale-italia, accessed on 2024.02.02.

[3] This is especially the case for Northern European countries, where electronic identity solutions are often provided by financial institutions. See European Commission, *Impact Assessment Report*, cit. at 1, pt. 1, 7-8.

[4] E.g., «Login with Google», «Login with Facebook» and «Login with Apple».

[5] Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L257/73.

electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities»[6], with a view to «remove existing barriers to the cross-border use of electronic identification means»[7]. Given its purpose to further the Internal Market, the legal basis of the Regulation rests on Article 114 TFEU.

The eIDAS Regulation governs electronic identification within the EU by defining, within its Chapter II, the principles regulating the transnational use of electronic identities across Member States. In doing so, it specifies the common technical architecture and policies for Member States schemes to achieve interoperability between each other. This aim is operationalized thanks to the so-called «Interoperability Framework»[8], which enables transmission of Member States electronic identities schemes through a set of nodes. Moreover, although it did not create a harmonized EU electronic identity, the eIDAS Regulation established the mutual recognition of national electronic identities, by encouraging Member States to notify their own identity solutions to the European Commission.

Against this background, on 3 June 2021 the European Commission has issued an amendment proposal to the eIDAS Regulation[9] (henceforth, «eIDAS Proposal»), with the aim of furthering the scope and overall enhancing the current eIDAS framework. The Commission's initiative stemmed from the mandatory periodical revision of the eIDAS Regulation, as provided under its Article 49. In the context of said revision, the Commission noted, on the one hand, that the eIDAS Regulation has furthered the development of the Single Market[10] while remarking, on the other hand, several shortcomings that have hindered the full achievement of its objectives related to electronic identities, amongst which:

[6] Recital 2 of the eIDAS Regulation.

[7] Recital 12 of the eIDAS Regulation.

[8] Art. 12 of the eIDAS Regulation.

[9] European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*, 2021/0136(COD).

[10] European Commission, *Report to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) (2021)*, p 7.

- Only 14 Member States had notified electronic national identity schemes to the Commission, while only 59% of the EU population had access to cross-border electronic identity solutions in accordance with the eIDAS Regulation[11].
- Failure to cover the provision of electronic attributes, such as medical certificates, driving licenses or professional qualifications[12].
- Limited possibilities for private parties, such as service providers or online platforms, to connect to the eIDAS system[13].
- Failure to fully comply with the data minimization principle, as users are not allowed to limit the sharing of identity data to what is strictly necessary for the provision of a given service[14].

As a result, the eIDAS Proposal advanced by the Commission endeavours to produce a shift from the current framework, based on voluntary notification of national schemes to the Commission and the subsequent mutual recognition of national electronic identities, to a system that allows users to share electronic attestations of attributes (such as driving licenses, student IDs, professional certificates and so on), while giving users more control over their personal data.

In doing so, the eIDAS Proposal advances the establishment of a so-called «European Digital Identity Wallet» or simply «Wallet», i.e., a mobile application which Member States will be obliged to offer to their citizens and residents, allowing for their online and offline identification, as well as allowing the electronic attestation of attributes. To ensure the widespread adoption of the Wallet, under the eIDAS Proposal both public administrations – when providing eGovernment services – and Very Large Online Platforms[15] –

[11] European Commission, *Impact Assessment Report*, cit. at 1, pt. 1, 4.

[12] *Ibid.*, pt. 1, par. 2-3, 10-12.

[13] *Ibid.*, pt. 1, par. 2.

[14] *Ibid*.

[15] Art. 25 of the eIDAS Proposal. The definition of «Very Large Online Platform» is to be found within Art. 33 of the Digital Services Act (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC, OJ L

when providing authentication to their services[16] – will be obliged to accept the new system as a means of identification.

One of the major features of the eIDAS Proposal is the introduction of a unique persistent identifier amongst the minimum set of person identification data that compose the Wallet[17]. The identifier consists of an alphanumerical string aimed at uniquely identifying a person for an indefinite amount of time. While the introduction of this identifier aims at facilitating identity matching and ensure the unique identification for each user, it also brings about significant concerns in terms of compliance with the current EU legislation on personal data protection and, more generally, in terms of its impact on the rights and freedoms of individuals.

In this respect, given that the identification of a natural person via electronic means amounts to a «processing of personal data» under applicable EU legislation on personal data protection, the eIDAS Proposal will have to comply with such legislation – which is part of EU primary Law – with particular reference to Article 8 of the Charter of Fundamental Rights of the European Union (henceforth, the «Charter»)[18] and to the General Data Protection

277, 27.10.2022, at 1–102. Other online platforms can be forced by the Commission to support the Wallet in the future, via delegated acts.

[16] The aim of the obligation is to provide users with an alternative means of identification when using Very Large Online Platforms, thereby providing an alternative to the use electronic identity solutions envisaged by the platforms themselves (such as «Login with Facebook», «Login with Google», and so on), and thereby provide a counter-balance to their role as de facto electronic identity gatekeepers, as noted by the Commission within the Report mentioned in n. 10, *supra*. In this respect, there is a clear connection with Art. 5, par. 7, of the Digital Markets Act, which prevents gatekeepers from forcing users to use the gatekeeper's own electronic identity solution (Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, OJ L 265, 12.10.2022, at 1–66).

[17] Art. 11a of the eIDAS Proposal.

[18] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, at 391–407. Art. 8 of the Charter reads: «1. Everyone has the right to the protection of personal data concerning him or her. 2. 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. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority».

Regulation (henceforth, the «GDPR»)[19]. This paper will specifically address the issue posed by the introduction of the abovementioned unique persistent identifier in light of the current EU data protection legislation and, in so doing, it seeks to highlight the impact that the principle of data protection by design has on the shaping of technical solutions at the legislative level, where those solutions involve the processing of personal data.

In order to do so, while this Section 1 has introduced the matter, Section 2 will explore what are unique persistent identifiers and their uses, both in general and with particular reference to the eIDAS Proposal. Subsequently, Section 3 will analyse the compliance of the eIDAS proposed identifier vis-à-vis the current EU legislation on personal data protection, with specific reference to three foundational data protection principles enshrined in the GDPR: data protection by design, purpose limitation and data minimization; the last part of Section 3 will also briefly touch upon the possible contrasts between the unique persistent identifier and data protection guarantees provided by some EU Member States Constitutions. Section 4 will address some possible privacy-friendly technological alternatives to the use of the unique persistent identifier. Finally, Section 5 sketches some conclusions.

2. Unique persistent identifiers: functions and use-cases

2.1 Unique persistent identifiers in general

A unique persistent identifier can be defined as a «string of letters and numbers used to distinguish between and locate different objects, people, or concepts»[20]. When used to identify objects, such as academic or literary work, the use of unique persistent identifiers is irrelevant from a data protection standpoint, as it does not trigger the material scope of application of data protection law: the Digital Object Identifier («DOI») used to locate specific digital objects such as academic papers, is an example of this type of identifier.

[19] 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), OJ L 119, 4.5.2016, at 1–88.

[20] National Library of Medicine, *Persistent Unique Identifier*, available at https://www.nnlm.gov/guides/data-glossary/persistent-unique-identifier, accessed on 2024.02.02.

However, unique persistent identifiers can also be assigned to natural persons, therefore triggering the applicability of data protection law. In this respect, a distinction can be drawn when such identifiers are assigned to a natural person in an online or offline context[21]. Given their persistent nature, which may in some cases even allow to identify and trace the activities of a person for their entire lifetime, this type of identifiers is highly intrusive on the rights and freedoms of natural person, as shall be seen in Section 3 below. In practice, when used to identify a natural person online, some of the most common persistent unique identifiers are the following[22]:

- Device identifiers, such as the «IMEI («International Mobile Equipment Identity»)[23], «MAC Address («Media Access Control Address»)[24] or static IP Addresses («Internet Protocol Address»)[25].
- Cookies, with specific reference to the «permanent» variant of cookies.
- Web beacons.

The processing of this type of identifiers can take place for a number of reasons, but in the online context the tracking of users

[21] However, this distinction is somewhat blurred, as offline identifiers such as the passport number may be used also in an online context, for example when voluntarily disclosed by the user to an online actor.

[22] Medium.com, *What are 'persistent identifiers'?* (2019), available at https://medium.com/golden-data/what-are-persistent-identifiers-af62d135d4c0, accessed on 2024.02.02.

[23] The IMEI consists of an electronic serial number used in some countries to blacklist devices that have been identified as stolen, therefore preventing the device from working on a mobile network (*ibid.*).

[24] The MAC Address consists of a unique identifier for a piece of hardware (such as a mobile device) on a network. This identifier enables tracking of individual devices as they move across different network connections (*ibid.*).

[25] The IP Address consists of a series of digits assigned to networked computers to facilitate their communication over the Internet. When a website is accessed, the IP address of the computer seeking access is communicated to the server on which the website consulted is stored. That connection is necessary so that the data accessed may be transferred to the correct recipient. See Court of Justice of the European Union, *Patrick Breyer v Bundesrepublik Deutschland*, Case C-582/14, ECLI:EU:C:2016:779, par. 15-16.

for advertising purposes is one of the most relevant[26]: digital advertising companies strive to identify a user as persistently as possible over time, in order to track their behaviour across multiple platforms for as long as feasible with a view to being able to create an accurate profile of the user and – ultimately – target them with highly personalized advertising[27]. Other applications of user-related persistent unique identifiers in the online context include anti-fraud purposes: for example, e-commerce retailers may want to consistently identify a user across multiple sessions to prevent fraudulent behaviour, such as creating multiple accounts in order to benefit from offers reserved to new clients.

While online unique persistent identifiers are usually assigned and subsequently processed by private actors such as digital advertising firms, so-called «offline» unique persistent identifiers are usually State-issued and are used for public-related purposes, such as for streamlining the assignment of social welfare benefits, paying taxes, registering a change of residence, and so on: examples of this type of identifiers are the tax code (e.g., the «*Codice Fiscale*» used in Italy), the VAT code, the ID-card number, passport number, and so on.

It should be noted that the abovementioned identifiers have varying degrees of permanence over time: for example, the «*Codice Fiscale*» used in Italy remains the same for the whole life of an individual, while the ID-card number is re-assigned as soon as a new ID-card is issued to the individual (e.g., in case of loss or expiration of the previous card), the IMEI changes as soon as the person buys a new phone, and so on.

In the next sub-Section, we will specifically address the main elements of the unique persistent identifier introduced by the eIDAS Proposal.

[26] *Ex multis*: I. Sivan-Sevilla et al., *Unaccounted Privacy Violation: A Comparative Analysis of Persistent Identification of Users Across Social Contexts* (2020), Federal Trade Commission, available at https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-ido_sivan-sevilla.pdf, accessed on 2024.02.02, at 1.

[27] For an overview on how the personalized advertising ecosystem works, see: Information Commissioner's Office, *Update report into adtech and real time bidding*, (2019), available at https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf, accessed on 2024.02.02.

2.2. The unique persistent identifier in the context of the eIDAS reform

As mentioned above, the eIDAS Proposal introduces, within its Article 11a, a unique persistent identifier amongst the minimum set of «person identification data» that compose the Wallet. The identifier consists of an alphanumerical string aimed at uniquely identifying a person for an indefinite amount of time.

In order to understand the purpose of this identifier, it is firstly necessary to address what is the minimum set of «person identification data» referred to above. With this expression, Article 3.3 of the eIDAS Regulation defines «a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established». Currently, this set of data is composed of four mandatory and four optional attributes that are to be transmitted in cross-border identifications cases. Mandatory attributes are (i) the first and (ii) the last names of a person, (iii) their date of birth and (iv) a unique identifier[28]: this is the minimum amount of data which any electronic identity solution must transmit to public or private service providers (so-called «Relying Parties») who use the eIDAS identity to authenticate users in the context of cross-border authentication to access online public services.

As a result, within the current text of the eIDAS Regulation, the unique identifier which is part of the mandatory set of data is not necessarily persistent, but rather «as persistent as possible in time»: in practice, the identifiers currently used for issuing eIDAS-compliant identities at Member State level are often not persistent, based on Member State determination [29].

In this respect, the function of the abovementioned set of four data items – and, in particular, the unique identifier – is to unambiguously identify the holder of the electronic identity. However, within the eIDAS Proposal, the identifier which is part of this set is now required not only to be «unique», but also «persistent»: in this respect, a unique identifier which is also indefinitely persistent in time has a higher identifying power vis-à-vis the identity holder, facilitating identity matching when using an electronic

[28] Annex 1 to the eIDAS Regulation. The optional attributes – which may be required or not, depending on the Member State choice – are (i) the first and last name(s) at birth, (ii) the place of birth, (iii) the current address and (iv) the gender.

[29] As will be seen *infra* in Section 3.5, this has mostly been done to accommodate those Member States where the presence of a persistent identifier would contrast with national constitutional law.

identity solution and ensuring the unique identification of each individual. According to the European Commission's impact assessment of the eIDAS Proposal, this change would therefore «considerably facilitate the comparison/matching of various identities of the same person, issued in various contexts or by different Member States (record matching / identity matching) which currently hinders citizens' effective authentication and access to services»[30].

This identifier, along with the other data items referred to above, would then be used to add electronic attestations of attributes to the Wallet, and – more importantly – the identifier would also be shared by the Wallet app with any Relying Party, i.e., with any public or private digital service provider that relies on the Wallet for the purpose of authenticating users to its services.

As already mentioned, given their persistent nature, this type of identifier is highly intrusive on the rights and freedoms of natural person, and has been critically defined as capable to «uniquely identify every person with an alphanumeric string that stays with them for the rest of their lives»[31]. This issue shall be better explored in the next Section.

3. The eIDAS proposed unique persistent identifier through the lenses of the right to personal data protection

3.1 EU Data Protection Law and unique persistent identifiers

The use of unique persistent identifiers has long been considered problematic from a data protection perspective by EU Data Protection Authorities: for example, as far back as 2013, the Article 29 Working Party stated, in relation to the use of identifiers by mobile applications, that: «*App developers (…) should not use persistent (device-specific) identifiers, but, instead, use low entropy app-specific or temporary device identifiers to avoid tracking users over time*»[32]. For this reason, Google and Apple – i.e., the two most important gatekeepers governing user access to mobile applications – have developed

[30] European Commission, *Impact Assessment Report*, cit. at 1, pt. 1, 5.

[31] European Digital Rights (EDRi), *eIDAS Policy Analysis* (2022), available at https://epicenter.works/sites/default/files/eidas-policy_paper-ewedri_0.pdf, accessed on 2024.02.02, at 1.

[32] Article 29 Working Party, *Opinion 02/2013 on apps on smart devices* (2013), available at https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf, accessed on 2024.02.02, at 19.

temporary device identifiers which app developers are contractually bound to use in lieu of device-specific persistent identifiers[33], if they want to distribute their application through Apple's AppStore or Google's PlayStore[34].

As already seen, in light of current EU data protection legislation, the creation and processing of identifiers which are linked to a natural person amounts to a processing of personal data[35]. It follows that the use of these identifiers has an impact on the right to the protection of personal data, recognized and protected by EU primary legislation under Articles 8 of the Charter[36] and 16.1 of the TFEU[37]: the validity of the new provisions of the eIDAS Proposal have therefore to comply with this fundamental right. In this respect, as illustrated by the official explanations of the Charter[38], the content of the right to personal data protection is to be found within secondary Union legislation on data protection, especially the GDPR[39]. Whether the unique persistent identifier envisaged by the current eIDAS Proposal respects the right to personal data protection has therefore to be assessed in light of the relevant GDPR rules and principles.

In this respect, as we will see below, the principles which are most impacted by the introduction of the unique persistent identifier envisaged by the eIDAS Proposal are the principles of purpose limitation[40] and data minimization[41], read in the light of the overarching principle of data protection by design and by default[42].

3.2 The principle of data protection by design

[33] Such as the IMEI or MAC address: see section 2, *supra*.

[34] These temporary identifiers are Apple's «Identifier for Advertisers» («IDFA») and Google's «Google Advertising ID» («AAID»).

[35] Arts. 4(1) and 4(2) GDPR.

[36] See n. 18, *supra*.

[37] «Everyone has the right to the protection of personal data concerning them».

[38] Explanations relating to the Charter of Fundamental Rights, OJ C 303, 14.12.2007, at 17–35, esp. the paragraph «Explanation on Article 8 — Protection of personal data». See also: O. Lynskey, *The Foundations of EU Data Protection Law* (2015), at 132-134.

[39] The official explanations refer to Directive 95/46/EC, which has however been superseded by the GDPR: as a result, any reference to the Directive should now be read as a reference to the GDPR (*ex* Art. 94 GDPR).

[40] Art. 5.1(b) GDPR.

[41] Art. 5.1(c) GDPR.

[42] Art. 25.1 GDPR.

The principle of data protection by design, embedded in Article 25 GDPR, requires the data controller to implement data protection principles[43] through the adoption of «appropriate technical and organisational measures», both «at the time of the determination of the means for processing and at the time of the processing itself»[44]. A key point of this principle is that the «appropriateness» of the technical and organisational measures has to be assessed by the data controller following a risk-based approach, meaning that the higher the risk for the rights and freedoms of data subjects created by the personal data processing activity, the stronger and more robust the technical and organisational measures will need to be.

The overarching aim of the data protection by design it to ensure the appropriate and effective embedding of data protection principles within the very design of data processing activities. In the words of the European Data Protection Supervisor, the principle «requires consideration of safeguards both at the design and operational phase, thus aiming at the whole project lifecycle and clearly identifying the protection of individuals and their personal data within the project requirements»[45]: in this sense, the data

[43] Data protection principles are the six fundamental principles envisaged in Art. 5 GDPR: (a) lawfulness, fairness, and transparency, (b) purpose limitation, (c) data minimization, (d) accuracy, (e) storage limitation, (f) integrity and confidentiality.

[44] The full text of the provision reads as follows: «Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects».

[45] European Data Protection Supervisor, *Opinion 5/2018 – Preliminary Opinion on privacy by design* (2018), available at https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_en_0.pdf, accessed on 2024.02.02, at 6. It should be underlined that this principle, alongside other rules and principles of the GDPR, is aimed at data controllers and – as a result –does not apply to data processors, or to producers of product and services. However, in the context of the eIDAS Proposal, this principle applies to the design and architectural choices of the electronic identity solutions themselves: see N. Tsakalakis et al. *Data Protection by Design for Cross- Border Electronic Identification: Does the eIDAS Interoperability Framework*

protection principles outlined in Article 5 GDPR can be considered as goals to be achieved via the implementation of technical and organisational measures.

Against this background, it is therefore necessary to address the requirements stemming from the principles of purpose limitation and data minimization, by reading them in light of the overarching principle of data protection by design.

3.3. The principle of purpose limitation

The principle of purpose limitation, enshrined under Article 5.1(b) GDPR, provides that personal data must be «collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes». Applying this provision in line with data protection by design requires the data controller to shape the design of the processing in a way which avoids – or at least minimizes – the risk of further unlawful processing with a different purpose than the original one: in the words of the European Data Protection Board, «the purpose of processing should guide the design of the processing and set processing boundaries».[46]

It follows that the techniques envisaged by the eIDAS Proposal must be designed and implemented in a way that minimizes the risk of further processing of the mandatory attributes – including the identifier – for purposes incompatible with the original one. As already seen, in the case of the eIDAS Proposal, the stated purpose connected with the processing of the persistent unique identifier is to facilitate the comparison and matching of various identities related to the same individual.

In order to adequately address the level of risk that the use of the identifier produces for the rights and freedoms of the data subject, it should be again stressed that the set of attributes – including the identifier – is shared with Relying Parties each time the identity holder uses the Wallet to authenticate to an online service. As mentioned above, Relying Parties are those providers of online services that rely on the Wallet to authenticate users: they involve not

Need to Be Modernised?, in E. Kosta et al. (eds.), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data* (2018), at 2-3.

[46] European Data Protection Board (EDPB), *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default* (2020), available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf, accessed on 2024.02.02, at 20.

only public, but also private service providers. Amongst the latter are also Very Large Online Platforms, often operated by «Big Tech» companies such as Google, Meta, and Amazon, who rely on online tracking and profiling as their main means of generating revenue[47], but also other private organizations may decide to allow users to authenticate via the Wallet. In this respect, it has been noted that «Facebook and other companies are only waiting to add such an official unique, lifelong identifier to their users' identities and will find a way to trick users into doing so»[48].

Although each sharing of the identifier with a Relying Party will have to be actively and specifically consented by the individual, it is now widely understood that consent is often not an effective means to enable users to make genuinely informed decisions, especially in online environments, due to the «consent fatigue» phenomenon[49].

As observed above in Section 2, the more persistent the identifier, the more effectively it can be leveraged to track and profile individuals overtime. In this respect, it should also be underlined that the identifier envisaged by the eIDAS Proposal is even more long-lasting than device-persistent identifiers, such as the IMEI or the MAC Address, because it typically remains the same for the entire lifetime of the individual (as opposed to the lifetime of the device). It is therefore reasonable to assume that AdTech and Big Tech companies, such as those operating Very Large Online Platforms, will do anything in their power to leverage the new identifier to boost their data-driven practices, based on tracking and profiling of users[50]. It is now widely understood that profiling – especially when the profile is highly precise, persistent over time and based on vast amounts of data – produces, in turn, risks of discrimination, manipulation of users' behaviours, and other interferences with fundamental rights[51].

[47] *Ex multis*: S. Zuboff, *The Age of Surveillance Capitalism* (2019).

[48] *eIDAS Policy Analysis*, EDRi, cit. at 31, 2.

[49] *Ex multis*: A. Mantelero, *The Future of Consumer Data Protection in the E.U. Re-Thinking the "Notice and Consent" Paradigm in the New Era of Predictive Analytics*, 30 Computer Law & Security Review 6 (2014).

[50] EDRi, *eIDAS Policy Analysis*, cit. at 31, 1-2.

[51] *Ex multis*: Article 29 Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (2018), available at https://ec.europa.eu/newsroom/article29/items/612053, accessed on 2024.02.02; European Union Agency for Fundamental Rights, *Bias in Algorithms -*

Further risks created by the use of the unique persistent identifier may arise in cases where the Wallet app is compromised by a malicious attack: if this were to happen, an attacker could easily link together all uses of the Wallet made by a single user by leveraging the identifier, thereby bypassing the security measures envisaged to achieve unlinkability of user actions[52], such as the mandatory separation between person identification data and other information required by Articles 6a.7 and 45.f.3 of the eIDAS Proposal[53].

In light of the above, it seems reasonable to conclude that the processing of the persistent unique identifier does not achieve purpose limitation by design; on the contrary, the identifier will likely risk being used for purposes incompatible with its stated aim, ultimately creating high risks for data subjects' rights and freedoms. In this case, the high risks produced by the sharing of the unique persistent identifier are arguably inherent to its very existence and cannot be effectively mitigated via other technical or organizational measures[54]. As a result, the only viable solution to achieve by

Artificial Intelligence and Discrimination (2022), available at https://fra.europa.eu/en/publication/2022/bias-algorithm, accessed on 2024.02.02.

[52] Unlinkability refers to a privacy by design goal which aims at avoiding the possibility to link together different datasets, flows or processes, which could violate data minimisation and purpose limitation and lead to unlawful user profiling (see *inter alia*: Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, *The Standard Data Protection Model*. v 2,0b (2020), at 27). The eIDAS Proposal expressly seeks to achieve unlinkability in Arts. 6a.7 and 6a.4.b. According to the former provision, Wallet issuers are prohibited from monitoring the usage of the Wallet, and to combine person identification data with further information. Consistently, issuers must maintain the person identification data separated from any other data, both at a logical and physical level. Additionally, the latter provision prohibits service providers from knowing the recipients of the attributes, so that they are prevented from linking together the attributes. See: A. Ortalda, N. Tsakalakis, & L. Jasmontaite, *The European Commission Proposal Amending the Eidas Regulation (Eu) No 910/2014: A Personal Data Protection Perspective* (2021), Brussels Privacy Hub, available at https://brusselsprivacyhub.eu/onewebmedia/Proposal%20to%20amend%20eIDAS.%20A%20personal%20data%20protection%20perspective_BPH_December%202021.pdf, accessed on 2024.02.02, at 8.

[53] *Ibid.*

[54] This is also the conclusion reached by many policy analyses of the eIDAS Proposal: EDRi, *eIDAS Policy Analysis*, cit. at 31, 1-2; European Data Protection Supervisor (EDPS), *Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity* (2021), available at https://edps.europa.eu/system/files/2021-07/21-07-28_formal_comments_2021-0598_d-1609_european_digital_identity_en.pdf, accessed on

design compliance with the principle of purpose limitation seems to be the deletion of Article 11a of the eIDAS Proposal in its entirety[55].

3.4. The principle of data minimization

The principle of data minimization is established by Article 5.1(c) GDPR, and provides that personal data shall be «adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed». This principle requires the data controller to pay close attention to the actual relevance of each category of personal data which is to be processed in light of the stated purpose, as the controller has to be able to demonstrate such relevance[56]. In order to achieve data minimization by design, data controllers are required to ensure that each category of personal data is genuinely necessary to fulfil the purpose of the processing, and only process such data if it is not possible to fulfil the purpose by other, less intrusive means; according to the European Data Protection Board, this should be achieved by applying state-of-the-art technologies aimed at minimising the personal data processed[57] or even aimed at achieving full-fledged data avoidance, when appropriate[58]. In particular, to evaluate whether the unique persistent identifier is in line with said requirements, it is necessary to assess whether its processing is:

2024.02.02, at 4; C. Busch, *eIDAS 2.0: Digital Identity Services in the Platform Economy* (2022), Centre of Regulation in Europe (CERRE), available at https://cerre.eu/wp-content/uploads/2022/10/CERRE_Digital-Identity_Issue-Paper_FINAL-2.pdf, accessed on 2024.02.02, at 16-17.

[55] Although the possibility of revising the article to introduce an identifier which is "unique per service" has also been suggested, as more privacy-friendly alternative. See *ibid.*, at 17.

[56] Art. 5, par. 2, GDPR.

[57] A well-known example of such a technology is «pseudonymization», which is defined by art. 4, no. 5, as «the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person».

[58] «Data avoidance» entails refraining from processing personal data altogether, when possible in light of the relevant purpose: see EDPB, *Guidelines 4/2019*, cit. at 46, 21.

- genuinely necessary to achieve the stated purpose of the processing, namely, facilitating the comparison and matching of various identities related to the same individual, and;
- in line with state-of-the-art technologies aimed at achieving data avoidance and minimisation[59].

Again, in line with the risk-based approach and given the high risks for the rights and freedoms of data subjects which is linked to the unique persistent identifier, the assessment of these two elements should be conducted thoroughly and rigorously.

In this respect, while it is true that the use of the unique persistent identifier can facilitate the accurate authentication of the electronic identity holder, alternative measures can arguably achieve the same result without having to process any identifier at all, as shall be seen *infra* in Section 4.

Furthermore, as seen in Section 3.3 *supra*, the presence of this identifier undermines the unlinkability of user interactions, which is a privacy goal connected with the achievement of both purpose limitation and data minimization by design[60]. In turn, the lack of unlinkability produces risks of identity theft, surveillance, and of abuse by AdTech and Big Tech companies[61].

Lastly, the use of a unique persistent identifier also undermines the effectiveness of pseudonyms. The possibility for an individual to use a pseudonym is currently envisaged by Article 5.2 of the eIDAS Regulation[62], and is formally retained in the text of the eIDAS Proposal. The identifier, when disclosed to Relying Parties along the rest of the minimum data set, could be easily associated with the pseudonym, thereby negating any privacy benefit for the identity holder who decided to use a pseudonym[63].

[59] *Ibid.*

[60] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, *The Standard Data Protection Model*. v 2,0b, 2020, at 27

[61] W. Wiewiórowski, *Where are we heading with digital identities?* (2023), Cybersecurity Standardisation Conference, available at https://edps.europa.eu/system/files/2023-02/23-02-07_ww-enisa_en_2.pdf, accessed on 2024.02.02, at 5.

[62] «Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited».

[63] See: Ortalda et al., *The European Commission Proposal*, cit., at 52, 9.

3.5 Potential contrasts with personal data protection guarantees enshrined in some EU Member States Constitutions

Finally, it is worth noting that the presence of a persistent unique identifier could collide with the provisions of some EU Member States Constitution aimed at protecting personal data. This, in turn, could lead to a conflict between EU Law and fundamental rights protection at the national level, should Article 11a of the eIDAS Proposal enter into force in its current form.

Most notably, the German Federal Constitutional Court has ruled, in its seminal 1983 «Census Decision»[64] that the use of a general identifier that makes it possible to «register and catalogue the individual citizen in his or her entire personality» – which is arguably the case for the identifier envisaged by the eIDAS Proposal, as seen above – violates the right to informational self-determination recognised by the German Constitution[65].

Other Member States which prohibit or strictly regulate the use of persistent unique identifiers at the Constitutional level are Austria[66] and Portugal, where paragraph 5 of Article 35 of the Portuguese Constitution, titled «Use of information technology», expressly states that «the allocation of a single national number to any citizen is prohibited»[67].

4. Privacy-Enhancing Technologies as a way to implement techniques in line with data protection by design

As already argued, compliance with the principle of data protection by design requires to embed data protection principles – such as purpose limitation and data minimization – in the very design of the processing, in a way that minimizes interferences with the rights and freedoms of data subjects. In particular, the embedding of purpose limitation and data minimization by design when

[64] Federal Constitutional Court [1983] Case 1 BvR 209, 269, 362, 420, 440, 484/83, ECLI:DE:BVerfG:1983:rs19831215.1bvr020983, par. 119.

[65] See, *inter alia*: B. Sümer & J. Schroers, *The new digital identity Regulation proposal and the EU data protection Regime* (2021), https://www.law.kuleuven.be/citip/blog/the-new-digital-identity-regulation-proposal/, accessed on 2024.02.02.

[66] Bundesgesetz über das polizeiliche Meldewesen. BGBl. I Nr. 9/1992 (1992) s 16a. See also: Ortalda et al., *The European Commission Proposal*, cit. at 52, 9.

[67] Translation provided by the Portuguese Parliament official website: https://www.parlamento.pt/sites/EN/Parliament/Documents/Constitution7th.pdf, accessed on 2024.02.02.

using the Wallet points toward the achievement of unlinkability of user actions, as a specific privacy goal to be achieved by the eIDAS framework: in other words, in order to effectively mitigate the risks for the rights and freedoms of individuals, it must be technologically impossible for any of the actors involved in the eIDAS framework to track the usage of the Wallet across multiple services.

Although the use of a unique persistent identifier undermines the achievement of unlinkability, it is suggested that its underlying aim to reduce the risk of abuse, ambiguity, or errors when using the Wallet could still be effectively achieved by using other techniques which have a smaller impact on the rights and freedoms of data subjects. Similar data protection-friendly techniques are usually called *Privacy-Enhancing Technologies* or «*PETs*»[68].

While it is not the aim of this paper to analyse each possible PET which could be used in the context of the eIDAS framework, it is worth noting that many other solutions have been suggested in the literature or are already used in practice by Member States or even at Union level.

One possible solution – already deployed in Austria[69] – could be the use of an identifier that is «unique per service» as opposed to «unique per person»: this so-called sector-specific personal identifiers or «ssPIN» would prevent the possibility of tracking and subsequent profiling of individuals when using the Wallet to authenticate for different services[70].

Another example of the use of a PET that could be adopted as a replacement to the use of the envisaged identifier can be found in the (no longer in force) Regulation (EU) 2021/953 on the EU Digital COVID Certificate[71], which incorporated safeguards at the technological level to achieve the unobservability of user interactions, including an offline verification mechanism via a public key

[68] IlSole24Ore, *Cosa sono le Privacy Enhancing Technologies?* (2022), https://www.infodata.ilsole24ore.com/2022/02/13/cosa-le-privacy-enhancing-technologies/, accessed on 2024.02.02.

[69] European Commission, *eGovernment in Austria* (2018), available at https://joinup.ec.europa.eu/sites/default/files/inline-files/eGovernment_in_Austria_2018_vFINAL.pdf, accessed on 2024.02.02.

[70] C. Busch, *eIDAS 2.0*, cit. at 54, 17.

[71] Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic, OJ L 211, 15.6.2021, at 1–22.

infrastructure[72]. Other solutions based on cryptography, such as pseudonymous identifiers or pseudonymous electronic signatures, could also be explored[73].

The above examples show that effective use of electronic identities and implementation of data protection by design techniques are not incompatible goals, but can actually work together with the aims of the eIDAS regulation. In order to achieve compliance with the principles stemming from the fundamental right to personal data protection – enshrined in EU primary law – while at the same time facilitating user authentication, the eIDAS legislator should carefully consider a technical solution which replaces the current unique persistent identifier. This alternative solution should make it technologically impossible tracking and profiling of the user across multiple services, with the final aim of preventing any possibility of public or private surveillance of Wallet usage.

It seems that the European Commission is already aware of this, and it is reconsidering its position on the identifier[74]. However, the persistent unique identifier is still present in the Council general approach on the eIDAS Proposal adopted during December 2022, although its use is limited to instances where user identification is required by law[75]. At the time of writing, the trilogues are still ongoing, therefore it will have to be seen whether the persistent unique identifier manages to be included in the final version of the Regulation.

5. Conclusion

As argued above, the achievement of «by design» compliance with the principles of purpose limitation and data minimization – which are part of the fundamental right to personal data protection enshrined in Article 8 of the Charter – requires the legislator to ensure the unlinkability of users' interactions with the Wallet. In other

[72] *Ibid.*, Art. 4.2.

[73] W. Wiewiórowski, *Where are we heading with digital identities?*, cit. at 61, 5.

[74] L. Kabelka, *Commission says single identifier in eIDAS reform "not necessary"* (2022), Euractiv.com, https://www.euractiv.com/section/digital/news/commission-says-single-identifier-in-eidas-reform-not-necessary, accessed on 2024.02.02.

[75] Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity - General approach*, 2021/0136(COD), Art. 11a, par. 2.

words, the legislator must lay down techniques that make it technologically impossible for any of the actors involved in the eIDAS framework to track the usage of the Wallet across multiple services.

However, the unique persistent identifier currently envisaged in the eIDAS Proposal, including in the Council general approach, seems not to be the appropriate instrument to ensure compliance with these principles: the extensive circulation of the unique persistent identifier with Relying Parties creates high risks of misuse and exploitation, to the detriment of fundamental rights and freedoms of identity holders.

It is suggested that a possible way forward, which may allow the Union legislator to achieve its legitimate aims, while at the same time complying with the principles of purpose limitation and data minimization by design, is the adoption of Privacy-Enhancing Technologies in lieu of the identifier currently envisaged by Article 11a of the eIDAS Proposal.

More broadly, this analysis has allowed us to highlight the influence that the relevant principle of data protection by design, provided by Article 25 GDPR (also relevant to the Charters of some EU Member States), has on the eIDAS regulatory framework: this principle requires the legislator to shape the techniques envisaged in the legal instrument in a way that minimizes interferences with fundamental rights and freedoms of individuals involved in the processing.