COMPARATIVE LAW REVIEW

Comparative Law Review

VOL. 17 · N. 1 · 2026

SPECIAL ISSUE

European Law and Digital Technologies

ISSN
2038 – 8993

OPEN ACCESS JOURNAL

COMPARATIVE LAW REVIEW
The Comparative Law Review is a biannual journal published by the
I. A. C. L. under the auspices and the hosting of the University of Perugia Department of Law.

Office address and contact details:
Email: complawreview@gmail.com

Comparative Law Review is registered at the Courthouse of Monza (Italy) - Nr. 1988 - May, 10th 2010.

COMPARATIVE
LAW
REVIEW
VOL. 17/1 – 2026

SPECIAL ISSUE

European Law and Digital Technologies

Edited by Federica Giovanella

THE EUROPEAN DIGITAL IDENTITY WALLET AS A TOOL TO INCREASE INDIVIDUAL AUTONOMY: FROM THEORY TO CRITICAL REALITY

Sara Garsia – Bilgesu Sumer *

TABLE OF CONTENTS:

With the proliferation of online services, digital identity management (IdM) systems have become essential for both public and private interactions, giving rise to complex ecosystems of personal data. This paper critically examines two key developments in this domain: the rise of Self-Sovereign Identity (SSI) models, which emphasise individual autonomy and identity transportability through digital wallets, and the EU's regulatory response via eIDAS 2.0, which mandates the issuance of European Digital Identity (EUDI) wallets by Member States. While eIDAS 2.0 embraces some SSI principles, our analysis questions whether its implementation truly aligns with the value of autonomy as an objective of privacy and data protection, particularly under the GDPR and the EU Charter of Fundamental Rights. Using autonomy as an evaluative criterion, we investigate whether the promises of SSI have been meaningfully integrated into the regulatory architecture or remain rhetorical. In drawing this cross-domain conceptual comparison between digital identity and privacy/data protection frameworks and to make it more concrete, we explore the implications of the use of the EUDI wallet in two prospective scenarios: the European Health Data Space (EHDS) and Very Large Online Platforms (VLOPs). This exercise led us to further consider the risk that the operationalisation of EUDI wallets blurs the line between legal and non-legal digital identities, potentially enabling disproportionate data processing and surveillance in digital ecosystems.

Keywords: digital identity, legal identity, eIDAS, GDPR, autonomy, Self-Sovereign Identity, European digital identity wallets.

I. INTRODUCTION

With the widespread use of the internet, digital identity management (IdM) systems have become an indispensable component of daily life. Identity management on the internet is

*This research was supported by the European Union through the project no. 101135927 NOUS and Cybersecurity Research Program Flanders – second cycle funded by the Flemish Government. The presentation of this research at the Young Scholars Workshop "European law and digital technologies" held at the University of Udine on 4-5 September, 2025 has received funding from the Research Foundation Flanders (FWO) travel grant.

Sara Garsia (sara.garsia@kuleuven.be), Doctoral researcher, Centre for IT & IP Law - KU Leuven University, Belgium
Bilgesu Sumer (bilgesu.sumer@kuleuven.be), Doctoral researcher, Centre for IT & IP Law - KU Leuven University, Belgium

The authors contributed equally to § I, V.I, VI. In a context of mutual contribution to the conception of the paper, Sara Garsia drafted § II.I, II.II, III.I, III.II, IV.II, and Bilgesu Sumer drafted § II.III, IV.I, V.II.

a highly complex topic that spans both the public and private sectors, resulting in enormous personal data ecosystems with numerous players.

Two crucial developments can be observed in this context.

First is the emergence of the Self-Sovereign Identity (SSI) model, which aims to safeguard the autonomy and independence of natural persons from closed silos, i.e. 'transportability'. Digital wallets – essentially software that functions as a personal data store for encrypted data - are the core technical reflection of the SSI theoretical foundations.

The second development took place at the regulatory level. In the European Union (EU), the eIDAS Regulation[1] established a system of cross-border recognition of national digital legal identities, however, limited to public services and voluntary for Member States. In view of granting seamless access to public and private services, the newly approved eIDAS 2.0[2] sets up a European digital identity (EUDI) framework by mandating Member States to issue digital identity wallets. The digital identity wallet is promoted as an empowerment tool for the user/citizen in terms of control over data and privacy.[3]

Existing research has already highlighted the potential and pitfalls of digital wallets.[4] Our study builds on — and diverges from — this research, as our objective is to evaluate the eIDAS 2.0 promises in light of the notion of autonomy that is highly related to the right to personal data protection. In fact, we move from the premise that the SSI ideal is advocated by the eIDAS 2.0. and that autonomy is at the core of SSI principles and is deeply connected to the right to data protection in the General Data Protection Regulation (hereinafter GDPR).[5]

Our research question is: how and to what extent does the eIDAS 2.0 framework reflect the SSI-inspired promises of natural person autonomy and identity transportability, especially in light of the autonomy objectives of the EU privacy and data protection frameworks?

Our analysis involves a cross-domain conceptual comparison, whereby we examine the concept of autonomy within different epistemic frameworks. While the contribution does not undertake a doctrinal comparison of legal frameworks, it adopts a comparative method at the level of legal concepts and underlying normative assumptions. One of these is theoretically foundational in a technological context (e.g., eIDAS' introduction of SSI

[1] Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market OJ L 257/73 (hereinafter eIDAS).

[2] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework OJ L1/56 (hereinafter eIDAS 2.0.)

[3] EU Digital Identity Wallet Home - EU Digital Identity Wallet - (last visited Jan. 16, 2026).

[4] *Ex multis* B. Lukkien et al., *Barriers for Developing and Launching Digital Identity Wallets*, Proceedings of the 24th Annual International Conference on Digital Government Research, 289–299 (ACM, Gdańsk, 2023); A. Giannopoulou*, Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity,* Digital Society 2(18, 2023); L. Weigl, M. Reysner, *The Governance of the European Digital Identity Framework Through the Lens of Institutional Mimesis*, Regulation and Governance (2025).

[5] B. Sümer*, Can Self-Sovereign Identity (SSI) fit within the GDPR?: a Conceptual Data Protection Analysis (Part I)* (June 3, 2022) available at https://www.law.kuleuven.be/citip/blog/can-self-sovereign-identity-ssi-fit-within-the-gdpr-part-i/ (last visited Jul. 30, 2025); 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, OJ L 119/1.

elements and digital identity wallets), while the other is legally embedded (e.g., privacy and data protection). Our comparison shows semantic drifts and normative tensions between the two two conceptions of the concepts (autonomy and transportability, and we also touch upon the potential governance implications of these differences. Our overarching aim is to evaluate how the stated legislative objectives of personal autonomy associated with the EUDI wallet are translated into operational provisions, by looking at the developments in specific contexts and policy areas. While our analysis concludes with recommendatory inputs for future directions for research, it does not provide fully elaborated normative recommendations.

The article is organized as follows.

We will first outline the conceptual foundations of digital identity and the stages of evolution of IdMs up to the SSI and digital identity wallets (§II). Second, we delve into the theoretical model of SSI and we conceptualise its essential properties (§III). Third, we present the baseline EU regulatory framework applying to digital identity wallets, focusing on privacy, data protection and the eIDAS 2.0 (§IV). Finally we assess how the eIDAS 2.0 framework responds to the SSI-inspired promises of natural person autonomy and identity transportability, by exploring the implications of the use of the wallet in two prospective scenarios: the European Health Data Space (EHDS)[6] and Very Large Online Platforms (VLOPs) (§ V). Given that the EUDI wallets are currently not operative,[7] we will conduct our analysis in light of the legislative text and its ongoing operationalisation through Implementing Regulations[8] and technical specifications,[9] included in the Architecture and Reference Framework (ARF).[10]

These two scenarios will allow us to respond to our initial question, by drawing a comparison between the prospective implementation of the SSI-inspired promises of natural person autonomy and identity transportability and the autonomy objective enshrined in privacy and data protection.

By answering the research question, we also incidentally explore whether the implementation of the EUDI wallets risks blurring the lines between digital legal identity and non-legal identities often used online. The lack of conceptual distinction has practical consequences, as it may involve disproportionate personal data processing, which, combined with the evolutionary features of online identification, from age verification, to

[6] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space OJ L 1/96 (hereinafter EHDS).

[7] The deadline for EUDI wallets to be operative is set for December 2026, eIDAS 2.0. art. 5a (1).

[8] The European Digital Identity Regulation - EU Digital Identity Wallet -(last visited Jan. 26, 2026).

[9] In parallel to the eIDAS 2.0. Proposal, the EU Commission published the Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework OJ L 210/51. It consists of a collaboration between the EU Commission and Member States to develop the technical architecture and reference framework (ARF), a non-binding document specifying standards and protocols. The ARF is used a basis for the Implementing Regulations, https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/Technical+Specifications (last visited Jul. 21, 2025).

[10] Architecture and Reference Framework (ARF) v2.7.3., available at https://eudi.dev/2.7.3/architecture-and-reference-framework-main/ (last visited Jan 15, 2026) (hereinafter ARF v2.7.3.).

gateway to all sorts of online venues, such as VLOPs and Data Spaces, points to increased surveillance.

II. DIGITAL IDENTITY: FOUNDATIONS AND EVOLUTION

Identity is not easy to define, as it is prominently multi-faceted.[11] The word comes from the Latin *idem*, which means *the same*.[12] ISO/IEC 24760-1 defines identity as a '*set of attributes related to an entity*', regardless of whether it is natural or legal.[13] These attributes should be sufficiently distinguished within their context.[14] Therefore, identity consists of a subset of attributes limited by a framework and recognized by a State or another authority, e.g., a name and national number or an e-mail address associated with a password, with predefined boundary conditions (the context), e.g., a country or a website. This definition appears broad enough to serve as the guiding definition for our analysis. Against this premise, in this section, we will illustrate the conceptual foundations of identity, specifically in the digital dimension, and briefly retrace its main stages of evolution.

II.1 *Foundations - From Analogue to Digital Identities*

In analogue settings, identification is required to transact only in specific cases, normally determined by the law. Entering into contracts to carry out the vast majority of daily activities does not occur prior to identification (e.g., buying public transport tickets, paying for groceries, etc.). Identification is required to access public services (e.g., healthcare), whereas in the context of private transactions, identification only takes place when it is necessary to ensure that a contract is executed in favour of a specific person and not another (e.g., insurance, banking and financial contracts, air travel). Instead, within the digital domain, users are required to identify themselves according to the variable rules adopted by each domain. This is because internet enables operations at a distance that, in the physical world, are facilitated by face-to-face interactions and require less information to be transferred. For instance, buying a book on Amazon compels users to log in with their 'Amazon identity', consisting of the association between a username and a password, while buying a book in a physical bookstore does not require a comparable check. This continuous detection of the user is fragmented since it occurs according to the different attributes defined by each domain. This is due to the absence of a unifying internet identity

[11] A. Ceyhan, *Technologization of security: Management of uncertainty and risk in the age of biometrics*, Surveillance & Society 116 (5(2) (2008).

[12] See personal identity: "*The sameness of a person or thing at all times or in all circumstances; the condition or fact that a person or thing is itself and not something else; individuality, personality.*" Oxford English Dictionary, available at www.oed.com/oed2/00111224 (last visited Jul. 30, 2025).

[13] ISO/IEC JTC 1/SC 27, IT Security and Privacy — A Framework for Identity Management — Part 1: Terminology and Concepts, ISO/IEC 24760-1:2019 (2nd ed. May 2019; amended 2023), § 3.1.1 (Switzerland: ISO, 2019/2023), available at https://cdn.standards.iteh.ai/samples/77582/096db3202a3d43108fee339becdbf3a4/ISO-IEC-24760-1-2019.pdf (last visited July 30, 2025).

[14] ITU (International Telecommunications Union) X.1252: Baseline Identity Management Terms and Definitions 04/202, https://www.itu.int/rec/T-REC-X.1252-202104-I/en, 4. (last visited Jul. 30, 2025).

layer that establishes '*who is connecting with what*'.[15] In this sense, the Digital Identity Guidelines of the National Institute of Standards and Technology of the US Department of Commerce (NIST) specifies that a person has normally multiple digital identities and the real-life identity of the individual behind the digital identity is usually not known. [16]
Another significant difference between analogue and digital identity is the role played by the human factor. After the initial registration of the user in a certain digital identity scheme (enrolment), the user can transact by simply providing the system with the information required, which matches the information registered (authentication).[17] This information constitutes the so-called *transaction identity*, defined as the minimum and mostly static set of identity information necessary to transact.[18] For example, when a local gym issues physical membership cards, it is more difficult to transfer them to someone else, even if it is possible; however, a human must be present for authentication. Online, a person or even a bot can create an account on a gaming platform. The platform then compares two sets of information: it is the information that is crucial for the transaction, rather than the human being.[19] Thus, the information can easily be transferred to someone else than the legitimate user.
In light of the features described, digital identity can be defined as the unique representation of a subject engaged in a specific online transaction, where the uniqueness is relative to the context of the transaction, and the representation may not align with the subject's real-life identity in the physical world.[20] To create a link between a person and their digital representation, the set of information forming the digital identity normally contains a piece of information, commonly referred to as an *identifier*.[21] Technically, it is just a pseudonym,[22] in the form of a data string, associated with the person and attached to the set of information forming the digital identity.

---

[15] K. Cameron, *The laws of Identity* (May 2005) available at www.identityblog.com/?p=352 (last visited July 30, 2025). The IP address can only trace back to the device connected to the network and the holder of the Internet connection, see J. McNamee *et al.*, *How the Internet works*, The Edri Papers, 5 (2012).
[16] NIST, SP 800-63 Digital Identity Guidelines available at NIST Special Publication 800-63-4 (last visited June 13, 2025).
[17] F. Wang, P. De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, Frontiers in Blockchain 7 (2, 2020).
[18] Sullivan refers to this concept in several publications: C. Sullivan, *Digital Identity: an emergent legal concept* (2011), 43; C. Sullivan, *Digital identity and mistake,* International Journal of Law and Information Technology 7 (20, 2012); C. Sullivan, E. Burger, *Blockchain, Digital Identity, E-government* in H. Treiblmaier and R. Beck (eds), *Business Transformation through Blockchain* 237 (2019).
[19] Sullivan, Burger, *Blockchain, Digital Identity, E-government*, 239 (2019).
[20] The definition is derived from the National Institute of Standards and Technology of the US department of commerce (NIST), see Paul A. Grassi et al., Digital Identity Guidelines (NIST Special Publication 800-63-3, 2017), confirmed by the second public draft of the ongoing revision, available at NIST Special Publication 800-63-4 (last visited Jun. 13, 2025). Similarly, A. Jøsang, *Identity Management and Trusted Interaction in Internet and Mobile Computing*, IET Information Security, 70 (8 (2) 2014).
[21] Wang, De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, 2 (2020).
[22] Note that from the EU data protection perspective such an identifier is personal data and it is unlikely to constitute a pseudonym, since 'pseudonymisation' requires that the additional information necessary to trace back the data subject "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". On the contrary, the

II.2 *Foundations - Digital Legal Identity*

Legal identity, also referred to as *foundational identity,*[23] enables persons in most legal systems to prove their identity based on credentials conferred by the State as proof of identity in an offline (analogous) setting, e.g., a national ID document. In addition to foundational identity systems, States often develop *functional identities* to manage sector-specific cases, e.g., voting, taxation, driving license, etc.[24] However, functional identities often overlap with foundational ones, and these two categories are increasingly used digitally. For instance, in Estonia, the digital identification required for government services sets the norm for private-sector transactions;[25] and civil registration is increasingly becoming essential in accessing even basic needs in life, e.g., registering at a hospital. Still, digital 'platform approved' identities typically do not require legal identification, due to the lack of a unifying Internet identity layer between real-life identities (i.e. legally recognised) and the individual's digital identities.

In light of this, what makes a digital identity legal? A digital identity with legal value, i.e., a digital legal identity, is such only if the association between a *legally identified person* and their *identifier* is *unique*,[26] such that this unique link can be subsequently used to prove legal identity across all digital domains where an *identity check is required.*

This unique link can be set up only *outside* the digital dimension. In practice, digital legal identity is established with an initial registration (i.e., enrolment), which requires an identification *de visu.*[27]

Ensuring trust regarding the association between natural persons and their identifiers requires external intervention. States, directly or by delegation, are in a privileged position, given their role as legal identity providers.

II.3 *The Evolution of Digital Identities towards SSI*

The first-generation IdMs have been silos models, where the association between username (i.e., email address) and password is used to guarantee access to registered users. By the end of the 2000s, identity management had begun to shift towards federated identity management, commonly known as 'Single Sign-On'.[28] It is the case of Apple, Google or Meta allowing their users to sign into third-party services with their existing

function of the identifier in the context of digital identity is precisely that of anchor to a natural person, see GDPR, art. 4 (1) (5).

[23] World Bank, ID4D Practitioner's Guide: Version 1.0 (Oct. 2019), available under Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), 217.

[24] The distinction between foundational and functional identity has been traced in the context of development initiatives see World Bank, ID4D Practitioner's Guide: Version 1.0 (Oct. 2019), available under Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO), 218.

[25] Sullivan, *Digital Citizenship and the Right to Digital Identity under International Law*, Computer Law & Security Review 475 (32, 2016).

[26] Sullivan, Burger, *Blockchain, Digital Identity, E-Government*, 236 (2019); Wang, De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, 3 (2020).

[27] Sullivan, Burger, *Blockchain, Digital Identity, E-Government*, 237-238 (2019).

[28] S. Canard *et al.*, *Identity Federation and Privacy: One step beyond*, Proceedings of the 4th ACM workshop on Digital identity management 25 (2008).

accounts. The inability of silos and federated IdMs to address digital identity fragmentation, coupled with asymmetries in the power held by providers and identity holders, has prompted research into more user-centric IdMs, focused on the properties of user consent and identity interoperability.[29]

In the 2010s, the decentralisation trend, mainly brought about by Distributed Ledger Technologies (DLTs) in the context of cryptocurrencies, has become dominant also in the digital identity debate, laying the foundations for an evolution of IdMs: the so-called self-sovereign identity (SSI), often referred to as decentralised identity.[30] Despite its increasing prominence across EU and non-EU jurisdictions, the term does not carry a single universally accepted meaning: technical definitions vary, and the idea of 'self-sovereignty' can imply different levels of control, governance, and legal entitlement in different socio-technical and legal contexts.[31] The original ideological basis of this model is rooted in the desire to overcome administrative mechanisms in the identification process, such that every individual is the source of their own identity, without the need for registration.[32] However, as an anchoring point, digital wallets are seen as the main determinants of an SSI network's level of decentralisation – that is why most regulatory frameworks and industry adoption of SSI are usually centered on wallets.[33] From a technical standpoint, it is, in fact, possible to imagine a self-sovereignty spectrum and classify digital wallets as an enforcing constraint for SSI.[34]

Figure 1. Evolution of IdMs

[29] C. Allen, *The Path to Self-Sovereign Identity* (April 26, 2016) available at The Path to Self-Sovereign Identity - Life With Alac... (last visited Jul. 23, 2025).
[30] O. Avellaneda *et al.*, *Decentralized Identity: Where Did It Come From and Where Is It Going?,* IEEE Communications Standards Magazine 10 (3(4) 2019).
[31] A. Giannopoulou*, Digital Identity Infrastructures: A Critical Approach of Self-Sovereign Identity,* Digital Society 5 (2(18) 2023).
[32] https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html (February 15, 2012) (last visited Jun. 30 2025); Doc Searls, *Self-sovereign vs. administrative identity* (March 25, 2012) available at http://blogs.harvard.edu/vrm/2012/03/25/ssi/ (last visited 30 June 2025).
[33] Some even argues that the wallets should be the starting point of explaining SSI. T. Ruff, *When Explaining SSI, Start with the Wallet* (Apr. 21, 2020), available at https://rufftimo.medium.com/when-explaining-ssi-start-with-the-wallet-bee5d2af6696 (last visited July 30, 2025).
[34] While the centralized, siloed storage of identification credentials are a restriction for SSI. L. Weigl et al., *The Social Construction of Self-Sovereign Identity: An Extended Model of Interpretive Flexibility*, Proceedings of the Hawaii International Conference on System Sciences, 2551 (2022). Also see M. Babel et al, *Self-Sovereign Identity and Digital Wallets,* Electronic Markets *28* (2025) 35

III. THE THEORETICAL MODEL OF SSI

III.1 *The ten principles of SSI*

There is no formal consensus about the characteristics that a digital identity scheme should have to be qualified as SSI, but the ten principles of self-sovereign identity presented by Christopher Allen in the blog post '*The Path to Self-Sovereign Identity*' have become a *de facto* reference to all the subsequent theoretical and technical developments.[35] These principles are: existence, control, access, transparency, persistence, portability, interoperability, consent, minimalization, protection.[36]

There is a crucial passage in Allen's blog post: '*Self-sovereign identity is the next step beyond user-centric identity and that means it begins at the same place: the user must be central to the administration of identity. That requires not just the interoperability of a user's identity across multiple locations, with the user's consent, but also true user control of that digital identity, creating* user autonomy. *To accomplish this, a self-sovereign identity must be transportable; it can't be locked down to one site or locale*'.[37] The two key concepts are: true user control resulting in '*user autonomy*', which can be achieved only if the identity is '*transportable*'.

III.2 *Natural Person Autonomy and Identity Transportability*

Building on Allen's conceptualisation, the two interdependent properties constantly identified by scholars, to achieve 'self-sovereignty' are: i) individual control over one's own identity and ii) independence of identity from closed environments, involving both the record/repository and the usability of identity information.[38]

The notion of 'control' is not limited to the individuals' static control over identity (e.g. refer to, update, hide).[39] It is dynamic, implying the ability to manage the information flow in a safe environment, to decide which data to disclose, to which subjects, in what cases, and with a high level of granularity.[40] Such 'true' control is more precisely defined as *autonomy of the natural person* who is the holder of the identity.[41]

---

[35] Allen, *The Path to Self-Sovereign Identity* (2016). The article is constantly referred to both by legal and ICT scholars when analysing the SSI model, see *infra* note 38 for subsequent references.
[36] *Ibid.*
[37] *Ibid.*
[38] Starting from Allen, these two concepts – with some lexical variation and nuances – are consistently used to explain the SSI model, see A. Tobin et *al.*, *The Inevitable Rise of Self Sovereign Identity*, The Sovrin Foundation 11 (8, 2017); Wang, De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion,* 9-10 (2020); Avellaneda et *al.*, *Decentralized Identity: Where Did It Come From and Where Is It Going*?, 11 (2019); K. Wagner et al., *Self-sovereign identity*, Blockchain Bundesverband, 27 (2018); A. Mühle *et al.*, *A Survey on Essential Components of a Self-Sovereign Identity*, 1 (30, 2018) Computer Science Review; U. Der *et al.*, *Self-sovereign Identity − Opportunities and Challenges for the Digital Revolution*, Arxiv Cornell University, 3 (2017).
[39] Allen, *The Path to Self-Sovereign Identity* (2016).
[40] Wang, De Filippi, *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion*, 9-10 (2020); Avellaneda *et al.*, *Decentralized Identity: Where Did It Come From and Where Is It Going*?, 11 (2019); Wagner *et al.*, *Self-sovereign identity*, 27 (2018).
[41] Allen, *The Path to Self-Sovereign Identity* (2016).

It can be argued that the property of natural person autonomy encompasses the SSI principles theorized by Allen. In fact, autonomy begins with the establishment of a representation of the natural person in the digital dimension (existence); it requires consent, (static) control, but also granular control over the information flow (minimalisation). Persistence of the identity is also included in autonomy because only ensuring the continuity of self allows the holder to manage their identity, which can evolve but needs to follow the continuity of the human being to which it belongs. Finally, no real autonomy is ensured if individuals' rights and freedoms are not respected: control over the identity data and flow presupposes the principle of protection, which provides for the full enjoyment of human rights.

While autonomy regards directly the prerogatives of the individual, the second property concerns identity data, and particularly their mobility. The identity belongs to the individual and not to a provider, and can be used across all desired domains, thereby overcoming the need for separate enrolments and subsequent authentication processes. Interoperability even when fully provided[42] does not change the fact that identity is held by a certain organisation, which locks the identity in its own site. Interoperability - here intended in the broad technical sense described by Allen as *widest possible usability* of the same identity[43] - enables the seamless movement of identities across silos, but it does not eliminate silos.[44] Instead, SSI addresses this weak spot by shaping a model where identity data are located in open 'containers',[45] connected to an infrastructure that enables the individual to both receive and transmit identity data to third parties.

This crucial passage is behind the idea of digital wallets, resembling the function of physical wallets.

This second property of the SSI model can be regarded as *transportability,* which involves the SSI principles of interoperability, portability, transparency, and access. Indeed, the mobility of identity data starts with wide usability across domains (interoperability) and evolves with independence from a single site (portability). Transportability also explains the principle of seamless access to data, enabled by the absence of a unique service provider and the principle of transparency, which allows the scheme to be open, accountable to operators and users, and independent of specific architectures.

Finally, natural person autonomy and identity transportability are complementary: as Allen points out, autonomy is enabled through transportability.[46] Ultimately, when a specific online transaction requires legal identification, the SSI model is meant to ensure a significant level of independence for the individual in the holding, management, and use of their identity information, specifically through wallets. Natural person autonomy,

[42] In federated systems, the interoperability is not full since it is limited to the members of the federation, see A. Tobin et al., *The Inevitable Rise of Self Sovereign Identity,* 7 (2017).

[43] Allen, *The Path to Self-Sovereign Identity* (2016). Note that interoperability is also a legal requirement of national electronic identity schemes under the eIDAS Regulation, confirmed under the eDAS 2.0. and enabled by common technical standards, see eIDAS 2.0., art. 12. "Seamless interoperability" is also identified in the recitals as a technological goal, see eIDAS 2.0., rec. 15, 19.

[44] A. Tobin et al., *The Inevitable Rise of Self Sovereign Identity,* 9, (2017).

[45] B. Pon et al., *Private-Sector Digital Identity in Emerging Markets*, Caribou Digital Reports 16 (2016).

[46] Note the expression "*to accomplish this"* in the passage reported *supra* in § III.I.

enabled by identity transportability, shapes an infrastructure where the identity is held directly by the individual, who can rely on it through granular disclosures. At first glance, this seems like a privacy-friendly development, but as we will argue, the wallet becoming a foundational identification tool shadows this initial ambition.

IV. BASELINE REGULATORY FRAMEWORK APPLICABLE TO DIGITAL IDENTITY WALLETS

It is now time to delve into the EU regulatory frameworks shaping the essential features of digital identity wallets. Our legal analysis is not exhaustive, meaning that it does not consider all the possible EU legal instruments potentially applicable to digital identity wallets. Rather it surveys the two pieces of legislation that set up the European digital identity (EUDI) framework and that shape the value of autonomy within the same framework, namely the eIDAS 2.0. and the GDPR. Our selection is justified by a number of reasons. First, our contribution seeks to evaluate how the concept of autonomy is substantiated within the EUDI system, and in this regard the eIDAS 2.0. and the GDPR are the most prominent legal instruments to look at, also in consideration of space constraints. Second, these two norms are currently the ones that exert the most concrete effects on the EUDI system. EU laws that remain outside the scope of this contribution regards prominently the recent EU data regulations, other than the GDPR. Primarily, it is legitimate to question the impact of the Data Governance Act (hereinafter DGA)[47] on the EUDI systems and specifically whether EUDI wallet providers could qualify as data intermediation services[48] under the DGA.[49] However, the issue is doubtful, mainly because the establishment of a *commercial* relationship must be the aim of DGA's data intermediation services, and the requirement is not in line with the aim of the EUDI wallet, at least as an electronic identification means.[50] The ongoing revision of the EU data legislation framework,[51] including the DGA, further complicates the data governance implications of an already complex, multistakeholder system as the EUDI system, which is worthy of dedicated analysis, beyond the scope of this paper.
Therefore, it follows the analysis of the GDPR and the eIDAS 2.0.

---

[47] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) OJ L 152/1.
[48] On data intermediation services see G. Carovano, M. Finck, *Regulating data intermediaries: The impact of the Data Governance Act on the EU's data economy,* in Computer Law & Security Review, 50 (2023); and B. Tervel, V.K. Dessers, C. Ducuing, M. Fierens, A. Palumbo, B. Peeters and L. Stähler, *White Paper on the Definition of Data Intermediation Services* (October 2, 2023). Available at SSRN: https://ssrn.com/abstract=4589987 or http://dx.doi.org/10.2139/ssrn.4589987.
[49] See notably DGA, rec. 30 referring to personal information management systems ("PIMS"), which however do not equate to digital wallets; on PIMS see H. Janssen and J. Singh, *Personal Information Management Systems*, in Internet Policy Review (11 (2) (2022).
[50] On the notion of commercial relationship see Tervel *et al.*, *White Paper on the Definition of Data Intermediation Services* 36 (2023).
[51] The Digital Omnibus Regulation Proposal includes significant modifications to the DGA's regime on data intermediaries, particularly making their registration merely voluntary; see Proposal for a Regulation of the European Parliament and of the Council [...] (Digital Omnibus) COM(2025) 837 final and B. Lazarotto, *The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act Rewrite* (December 19, 2025) available at The Data Omnibus: The Good, the Bad, and The Ugly Behind the DGA and Data Act Rewrite - MediaLaws (last visited Jan. 15, 2026).

IV.1 *Autonomy, the right to data protection, and the GDPR*

The evolution of digital identity regulation in the EU reflects a deep-rooted commitment to the European value of autonomy, understood as persons' right to self-determination and control over their personal data. As dissected in the previous section, the identity consists of a collection of personal data. In fact, the definition of personal data is closely intertwined with the definition of *identification*. Hence, digital identity as a regulatory field had been subject to several EU legislations before the GDPR. Each of these legislations appears to be motivated by technological and social developments affecting data protection and privacy. For instance, the advent of the Internet and the widespread use of centralised governmental databases for surveillance after the Second World War sparked the need to provide individuals with more control over their personal data.[52]

The European jurisdiction and legislation have responded to these developments with measures that protect the fundamental rights objective, e.g., the Census decision of the German Supreme Court is a seminal case in this direction.[53] This decision is crucial as it grounds individual autonomy in the control over personal data and affirms that data processing poses threats to the free development of personality.

Since 2009, with the enactment of the Lisbon Treaty, the EU's primary legal basis for personal data protection has been the EU Charter of Fundamental Rights.[54] Article 8 of the Charter has raised the level of personal data protection to that of a fundamental right and provides the main data protection principles, including fair processing, purpose specification, and legitimate basis. The Charter also includes a right to privacy in Article 7, which mirrors Article 8 of the European Convention on Human Rights (ECHR).

The rules and practices in IdM may have severe implications for the fundamental rights and freedoms set out in the EU Charter, particularly the right to the processing of personal data, as outlined in Article 8, which covers any information relating to an *identified or identifiable* individual.[55] Article 52(1) of the EU Charter establishes that limitations on rights must be recognised by law, respect their essence, and be necessary and proportionate. This requirement reinforces that the regulation of technologies, including identity management systems, must also be designed to preserve freedom, dignity, and informational self-determination.

An overview of the case law demonstrates that attributes such as identifiers and credentials qualify as personal data. For instance, in the *Linqvist* Case, the CJEU stated that a natural person's working conditions and hobbies constitute personal data.[56] Similar information is usually kept in digital wallets to create profiles of individuals as a part of their (broader)

[52] P. Hustinx, *European Leadership in Privacy and Data Protection* (2015), available at https://edps.europa.eu/sites/edp/files/publication/14-09-08_article_uji_castellon_en.pdf (last visited Jul. 31, 2025).
[53] G. Hornung, C. Schnabel, *Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination*, Computer Law & Security Review 84-88 (25, 2009).
[54] Charter of Fundamental Rights of the European Union, OJ C 326/391 of 26/10/2012.
[55] GDPR, Article 4(1).
[56] Judgment of the Court of 6 November 2003, *Linqvist,* C-101/0*, EU:C:2003:596*, para 24.

database identity.[57] On the other hand, their credentials typically serve as their transaction identity, i.e., the minimum and mostly static set of identity information necessary to transact.[58]

The Court found in the *Breyer* Case that personal data may consist of several pieces that do not identify an individual separately.[59] The case concerns dynamic IP addresses, which change for every connection; however, this still allows *indirect identifiability* of data subjects by the internet service provider. In the IdM context, for instance, identifiers or credentials themselves alone may not identify an individual. However, the possibility of identifying an individual when they are combined with other identifying data is sufficient for the information to qualify as personal data. In this case, the CJEU also pointed out that identifiability depends on the sources available to the controller, who was defined as '*the natural or the legal person […] alone or jointly […] determines the purposes and means of the processing of personal data […]*'. When the controller (ISP in this case) '*has the legal means which enable it to identify the data subject without additional data,*' this is '*a means likely reasonably to be used to identify the data subject*'.[60] The broad interpretation adopted by the Court points to individual's protection as the focal point in data protection, which enables individuals to exercise control over how their identity is constructed, shared and linked across digital infrastructures. Therefore, autonomy is operationalised by the Court as both a right and a foundational value of the EU legal order.

Similarly, the GDPR has been established on these grounds, as explained by the European Data Protection Board (EDPB), '*the data subject should be granted the highest degree of autonomy as possible with respect to control over personal data within the frames of the legal basis, and to determine the use made of their personal data, as well as over the scope and conditions of that processing*'.[61]

IV.1.1. *Control in relation to Autonomy in SSI and GDPR*

In light of the broad definition of personal data enshrined in the GDPR, in SSI, several actors, such as issuers, verifiers, and SSI technical or governance boards, may assume roles that qualify them as controllers or joint controllers.[62] SSI systems concern *entities* that can be organisations, devices, or software applications.[63] On the other hand, to clearly understand their respective obligations under the GDPR, their relative capabilities, i.e., reasonably likely means available to them to identify natural persons should be assessed

[57] "'*Database identity' comprises all the data and information recorded about an individual in the database/s accessible under the scheme*" C. Sullivan, *Privacy or Identity?*, International Journal of Intellectual Property Management 290 (2, 2008).

[58] See *supra* § II.I. and note 18.

[59] "*There is no requirement that all the information enabling the identification of the data subject must be in the hands of one person*" Judgment of 19 October 2016 *Breyer*, C-582/14, EU:C:2016:779, para.43.

[60] *Breyer*, C-582/14, para 48.

[61] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and Default Version 2.0. (2020), 16-18.

[62] See Article 26 GDPR for joint controllership.

[63] ISO/IEC JTC 1/SC 27, IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts, ISO/IEC 24760-1:2019 (2nd ed. May 2019), § 3.1.1, 24.

carefully.[64] Nonetheless, in some circumstances, a set of attributes related to a non-person entity may still qualify as personal data, for example, a device ID. In such cases, device IDs such as IMEI numbers, IP addresses can be used to re-link user sessions or trace behavioural patterns of users.[65]

Some of the SSI principles closely resemble certain provisions and principles outlined in the GDPR. For example, *control* is mentioned a few times in the GDPR as an overarching objective of the Regulation.[66] More broadly, SSI and the GDPR can be said to have a common purpose: to enhance individual control over personal data. As discussed above, this control can be provided by autonomous choice. The conceptualisation of autonomy in data protection is, however, broader, encompassing empowerment and resistance to power asymmetries.[67] A significant example is the right to portability, which is similarly seen as one of the most important accomplishments of the GDPR (Article 20) and following regulatory instruments such as the Data Act, providing data subjects with a right to move their personal data from one controller to another.[68] As mentioned, SSI promotes transportability through wallets.

Although the GDPR has strengthened the measures in its predecessor directive, its effectiveness is still being questioned.[69] One of the reasons for this is that the GDPR, like its predecessor, is written with centralised databases in mind.[70] However, the technological reality is changing. As a result, the ideal of autonomy in data protection is highly challenged.

---

[64] Judgment of the Court (First Chamber) of 4 September 2025, European Data Protection Supervisor v Single Resolution Board, C-413/23 P ECLI:EU:C:2025:645. Related to this, the Digital Omnibus Regulation Proposal includes significant modifications to the scope of the personal data that should be taken into account when discussing data protection responsibility under the GDPR, see Proposal for a Regulation of the European Parliament and of the Council [...] (Digital Omnibus) COM(2025) 837 final.

[65] The UK GDPR explicitly incorporates the term 'online identifiers' into the definition of personal data. These can include details about the device an individual is using, as well as applications, tools, or protocols. ICO, What Are Identifiers and Related Factors? (Nov. 19, 2024), available at https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/personal-information-what-is-it/what-is-personal-data/what-are-identifiers-and-related-factors/ (last visited July 29, 2025).

[66] GDPR, rec. 7.

[67] F. Ferretti, *A European Perspective on Data Processing Consent through the Reconceptualization of European Data Protection's Looking Glass after the Lisbon Treaty: Taking Rights Seriously*, European Review of Private Law 473-506, (20, 2012).

[68] P. De Hert et *al., The right to data portability in the GDPR: Towards user-centric interoperability of digital services*, Computer law & security review, 193-203 (34(2) 2018); B. Lazarotto, *The right to data portability: A holistic analysis of GDPR, DMA and the Data Act,* European Journal of Law and Technology, (15(1) 2024).

[69] W. Li *et al.*, *Mapping the Empirical Literature of the GDPR's (In-)Effectiveness: A Systematic Review,* Computer Law & Security Review 106129 (57, 2025); C. Prince *et al.*, *Online Privacy Literacy and Users' Information Privacy Empowerment: The Case of GDPR in Europe* Information Technology & People 37 (1 2024).

[70] M. Finck, *Blockchain Regulation and Governance in Europe*, (1st ed. Cambridge University Press, 2018).

IV.2 *The eIDAS 2.0 and its recall to the SSI model*

A single EU digital legal identity scheme is not feasible, as legal identity is a national prerogative.[71] Therefore, the former eIDAS set up a system of cross-border recognition of national schemes. This system proved to be limited due to its voluntary nature and the exclusion of private services.[72] Driven by the digitalisation boost caused by the COVID-19 pandemic,[73] the EU Commission published an amendment proposal in June 2021.[74] The so-called eIDAS 2.0. entered into force in May 2024.

The eIDAS 2.0. has established a 'European Digital Identity Framework', which, despite the terminology adopted, is based on a regime of interoperability among national instruments following common technical standards, aiming at facilitating the proof of digital identity within the EU. Under the eIDAS 2.0, each Member State is required to notify the EU Commission of at least one electronic identification scheme, which is then mutually recognised throughout the EU.[75] Second and most notably, the eIDAS 2.0. introduces the European Digital Identity Wallets (EUDI Wallets).[76] The wallet, whose holder can be a natural or a legal person,[77] must be issued at the national level and can be provided directly by Member States, under a mandate or independently, but with the recognition of the Member State.[78] The wallet has three 'layers': i) it is an electronic identification means, hence containing person identification data (PID); ii) it enables the holder to store, manage, and validate other information related to identity ('attribute')[79]. The attributes issued in electronic form ('electronic attestation of attributes', EAA) can be non-qualified, such as concert tickets, or qualified, such as driving licenses and diplomas.[80] Via the wallet, (Q)EAA can be selected and combined with PID and shared; iii) it allows the holder to sign, by means of qualified electronic signatures or seals.[81] The wallet must be accepted by online public services, private strategic services, and very large online

[71] eIDAS 2.0., rec. 19. However, the assurance levels required for national electronic identification schemes impose considerable constraints on Member States. See eIDAS 2.0. art. 8 (untouched by the amendments) and Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 OJ L 235/7.

[72] eIDAS, art. 6 and ff. and rec. 17.

[73] Impact Assessment Report Accompanying the document 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, (3 June 2021) SWD (2021) 124 final, 2.

[74] Proposal for a Regulation of the European Parliament and of the Council amending the Reg. (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (3 June 2021) COM (2021) 281 final.

[75] eIDAS 2.0, art. 6 and ff.

[76] *Id.*, art. 3(42) and art. 5a.

[77] Note however that for legal persons, both business and public sector bodies, the European Commission has published a separate legislative proposal on the establishment of European Business Wallets, that if approved, will substitute the EUDI wallet for legal persons, see Proposal for a Regulation of the European Parliament and of the Council on the establishment of European Business Wallets (19 November 2025) COM(2025) 838 final.

[78] eIDAS 2.0., art. 5a (2).

[79] *Id.*, art. 3 (43).

[80] *Id.*, art. 3 (44) (45).

[81] *Id.*, art. 3(42) and art. 5a.

platforms (VLOPs), while other private services remain free to not accept it.[82] The EUDI wallet is free of charge for natural persons and voluntary.[83]

The preparatory documents and the legislative text advocate the SSI model between the lines. The Explanatory Memorandum refers to a new market orientation towards the provision and use of specific attributes related to identities, instead of rigid digital identities.[84] The Impact Assessment report recognizes that society is already dealing with a '*paradigm shift*', whereby users expect '*a self-determined environment*', the so-called '*self-sovereign app-based wallets*', which allows managing person identification data, such as a national eID and other attributes under their full control.[85] The eIDAS 2.0. constantly refers to the principle of user control - in some cases accompanied by the adjectives 'full' or 'sole' - over their online identity and data,[86] and demands the selective disclosures of data and technical safeguards against tracking, correlations, and linkability of users' behaviour and data.[87]

We argued that SSI, with its properties of natural person autonomy and identity transportability, provides for a desirable model for the digital conversion of identity, including legal identity. Against the references made by the EU legislators, it is therefore relevant to consider whether and how the eIDAS 2.0. has implemented the SSI model *in concreto* and whether this implementation aligns with the concept of autonomy in the EU data protection framework.

[82] *Id.*, art. 5f. Those who rely on the EUDI wallet to provide their services are defined as "relying parties", see *id.*, art. 3(6) and 5b.
[83] *Id.*, art. 5a(13)(15).
[84] eIDAS 2.0 proposal *supra* n. 74, 1.
[85] Impact Assessment Report of eIDAS 2.0. proposal *supra* n. 73, 3.
[86] eIDAS 2.0, rec. 2, 3, 4, 13; rec. 5 and 15 (which use the expression "sole control"); art. 5a(14) stating that "Users shall have full control of the use of and of the data in their European Digital Identity Wallet".
[87] *Id.*, art. 5a (4)(a) and (16).

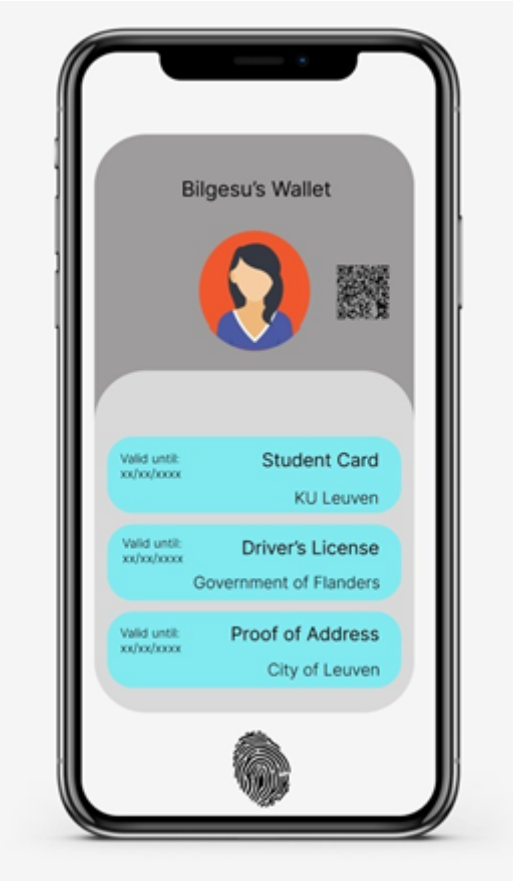

Figure 2. Representation of a digital identity wallet

V. REALITY CHECK: EUDI WALLETS AND DEBUNKING THE BIG PROMISES

V.1 *Testing Promises – EHDS and VLOPs*

In this section, we assess how the eIDAS 2.0 framework responds to the SSI's two primary promises: enhancing the autonomy of natural persons and the transportability of identity. We will provide prospective scenarios based on two contexts of use: the European Health Data Space (EHDS)[88] and Very Large Online Platforms (VLOPs).[89] We decided to focus on these two contexts of use since they respectively represent typical legal and non-legal identification scenarios.

The EHDS is a regulatory-technical project that led to the adoption of Regulation (EU) 2025/327, situated within the broader EU efforts to secure data sharing and harness the assumed economic, scientific, and informational value of data.[90] Specifically, the EHDS governs the cross-border access to health data both for use by patients, their

[88] Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space OJ L 1/96. Hereinafter EHDS.
[89] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (DSA) OJ L 277/1, art. 33. Hereinafter DSA.
[90] EU Commission, *A European strategy for data,* COM(2020) 66 final.

representatives, health professionals, and healthcare providers (i.e., primary use)[91] and for secondary uses in view of public interest or research objectives (i.e., secondary use).[92] The intersection between the EHDS and the eIDAS framework prominently concerns the first case,[93] whereby patients are granted the right to access their personal electronic health data.[94] Member States will be responsible for establishing health data access services, and patients are entitled to rely on eIDAS for online identification. [95] The prospective use of the EUDI wallet for the overall management of health-related documents seems to be in the intentions of the EU legislator,[96] as showcased by the eIDAS 2.0 large-scale pilot dedicated to ePrescriptions, [97] launched in parallel as an electronic cross-border health service under the eHealth Digital Service Infrastructure (eHDSI).[98]

As for VLOPs, they are defined as those with more than 45 million users per month in the EU in Article 33 and Recital (76) of the Digital Services Act (DSA).[99] VLOPs that require user authentication to access their online services must support and accept EUDI Wallets for this purpose.[100] It means that VLOPs, as Meta, Amazon, and Google,[101] are required to integrate the EUDI wallet as an option for logging in, identity verification (e.g., age verification), and verification of customers' identity (so called Know your Customer "KYC" standards) for marketplaces.

V.1.1. *Natural Person Autonomy*

In line with SSI, the EUDI wallet should equip users with autonomy over their digital identity. We assess three key features of eIDAS 2.0 in light of their impact on autonomy: (i) the circulation of identifiers; (ii) the extent to which individual wallet use is externally observable; and (iii) whether wallet use remains genuinely voluntary.

Overall, the eIDAS 2.0. addresses these potential concerns to autonomy respectively by demanding (i) the 'selective disclosure' of data by the wallet; (ii) 'the unlinkability' of

[91] EHDS, art. 2 (2)(d).
[92] EHDS, art. 2 (2)(e).
[93] On the connections between Data Spaces and eIDAS Regulation, see Centre of Excellence for Data Sharing and Cloud, *Impact of eIDAS revision and EU Digital Identity landscape on data spaces* (2024).
[94] EHDS, art. 3.
[95] EHDS, art 4 and 16 and eIDAS 2.0., art. 5f.
[96] J. S. Marcus *et al.*, *The European Health Data Space,* Study Requested by the ITRE committee 25 (2022) and P. Terzis, *Compromises and Asymmetries in the European Health Data Space*, European Journal of Health Law 349, (30 (3) 2022).
[97] ARF v2.7.3., 2.6.6.1 and <ePrescription - Potential - For European Digital Identity> (last visited Jul. 21, 2025).
[98] As initiated by Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare OJ L 88/45, art. 14; see also EHDS, art. 23 and https://health.ec.europa.eu/ehealth-digital-health-and-care/digital-health-and-care/electronic-cross-border-health-services_en (last visited Jul. 21, 2025).
[99] Also see: *Digital Strategy Europe Press Release, Digital Services Act: Commission starts collecting platform's user numbers and consults on its monitoring and investigatory procedures*, available at https://digital-strategy.ec.europa.eu/en/news/digital-services-act-commission-starts-collecting-platforms-user-numbers-and-consults-its (17 February 2023) (last visited Jan 31, 2026)
[100] eIDAS 2.0., art. 5f(3).
[101] https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (last visited Jul. 31, 2025).

person identification data and other attributes every time the identification of the user is not required; (iii) the principle of voluntary use of the wallet, such that access to services, to the labour market and the freedom to conduct business is not impaired by the choice not to use the wallet.[102] In particular, how do these principles appear to be enacted in the prospective uses of the EUDI wallet?

Preliminarily, it should be pointed out that even if, in principle, the selective disclosure of data by the wallet and the unlinkability of legally identifying person identification data with other attributes are two separate properties, they are both conceptually and functionally meant to prevent the tracing of the digital life of wallet holders. Therefore, at the implementation level, it is hard to trace a dividing line between the two.

As for the selective disclosure, art. 5(4) of the Commission Implementing Regulation on the protocols and interfaces to be supported by the eIDAS Framework mainly restates the eIDAS 2.0. text.[103] The ARF specifies the standards that can be followed to ensure selective disclosure.[104] The issue of the circulation of the identifier seems to be explicitly tackled by the implementing rules addressing the unlinkability of wallet activities. The principle is implemented in the ARF with reference to the so called 'relying parties', i.e., those who accept the wallet as a gateway for the provision of their services,[105] but no guarantees are posed with regard to the wallet provider. To conceal identifiers, the use of Zero-Knowledge Proofs (ZKP) by the EUDI wallet as privacy-enhancing technologies (PETs) is promoted.[106] ZKP is a process that only discloses a cryptographic proof of a valid signature, without revealing the original key. Thus, original keys cannot be easily linked back to a specific data subject. However, different ZKP constructions offer varying levels of identifiability, and so far the ARF has not promoted a specific type of ZKP. [107]

By contrast, transaction logs, which constitute personal data from the perspective of the wallet providers, are accessible by wallet providers, provided that the access is necessary for the provision of wallet services and that the user gives their explicit consent,[108] arguably two very weak conditions to effectively safeguard unlikability.

It is then legitimate to wonder how these concerns arise in the context of the EHDS, whereby the EUDI wallet stands as a gateway for the digital interaction of the patient with health professionals and healthcare providers, given that it is likely[109] and in any case possible that the wallet provider will be a private entity.[110] It is true that the use of the wallet remains voluntary, but strong campaigns have been put in place to maximise its

---

[102] eIDAS 2.0., art. 5a (4)(a), art. 5a(16)(b), art. 5a(15). Note that art. 5a(16)(b) has a typo, where "*unlikeability*" is actually "*unlinkability*".

[103] Commission Implementing Regulation (EU) 2024/2982 of 28 November 2024 OJ L 1/7.

[104] ARF v2.7.3, 5.3.

[105] ARF v2.7.3., 7.4.3.5.2. See eIDAS 2.0., art. 3 (6) for the definition of "*relying party*".

[106] ARF v2.7.3., 7.4.3.5.3.

[107] L. Zhou *et al.*, *Leveraging Zero Knowledge Proofs for Blockchain-Based Identity Sharing: A Survey of Advancements, Challenges and Opportunities,* Journal of Information Security and Applications 80, (103678, 2024); ARF v2.7.3., 7.4.3.5.3.

[108] Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 OJ L 1/14, art. 9(5).

[109] K. Degen, T. Teubner, *Wallet Wars or Digital Public Infrastructure? Orchestrating a Digital Identity Data Ecosystem from a Government Perspective*, Electronic Markets 20 (34, 2024) .

[110] eIDAS 2.0., art. 5a(2)(c).

adoption, [111] while the EHDS delegates the recognition of the right to opt out in primary use to Member States.[112]

As for VLOPs, the recent introduction of the age-verification obligation by DSA for adult websites demonstrates that the voluntariness of the wallet might not be applicable in every case. Users can opt for either their biometric data to be processed or use the EUDI wallet for age verification. France, for instance, now requires adult websites to implement age verification using methods such as biometric video selfies, credit card, or legal identity scanning. [113] VLOPs will thus enable their users to authenticate via EUDI wallets, based on attributes related to their legal identity, as wallets are inherently connected to this foundational identity established by governments, as will be further elaborated in V.1.2. below.

Therefore, we observe that the EUDI wallet and its technical specifications aim at introducing significant improvements in terms of autonomy for self-managing digital identities. However, the granular pieces of digital identities, i.e., personal data, can still be tracked and matched by wallet providers and online private services within this identity management network.

V.1.2. *Identity Transportability*

One of the most challenging aspects of digital identity management to ensure identity transportability is (i) the location of the repository necessary to perform the identity check and the verification of other attributes, as these determine the primary interoperability and portability of the scheme. During the operational phase, (ii) malfunctions of the system or other critical scenarios test the system's actual ability to maintain its transportability. The eIDAS 2.0. only partially engages with these profiles.

As for repositories, the Regulation is silent, except for mandating that attributes issued on the basis of '*authentic sources*', i.e., original repositories of official information, are verifiable against those sources. [114] The Implementing Regulation on the integrity and core functionalities of European Digital Identity Wallets requires wallet providers to use secure cryptographic devices (WSCDs) to manage critical assets, such as identifiers and attributes, and to perform authentication functions.[115] The ARF specifies that the WSCD can be

---

[111] G. Comandè, M. Varilek, *The Many Features Which Make the eIDAS 2 Digital Wallet Either Risky or the Ideal Vehicle for the Transition to Post-Quantum Encryption*, Computer Law & Security Review 8, (54, 2024).

[112] EHDS, art. 10.

[113] Reuters, *Five EU States to Test Age Verification App to Protect Children* (July 14, 2025), available at: https://www.reuters.com/sustainability/boards-policy-regulation/five-eu-states-test-age-verification-app-protect-children-2025-07-14/ (last visited July 30, 2025); The Guardian, *Pornhub Owner to Suspend Site in France in Protest at New Verification Law* (June 3, 2025), available at: https://www.theguardian.com/world/2025/jun/03/pornhub-france-id-verification (last visited July 30, 2025).

[114] eIDAS 2.0., art. 45e and art. 3(47) for the definition of authentic sources.

[115] Implementing Regulation (EU) 2024/2979, art. 4(1), see also Z. Ebadi Ansaroudi *et al.*, *Secure and Reliable Digital Wallets: A Threat Model for Secure Storage in eIDAS 2.0* in S. Katsikas, B. Shafiq (eds), *Proceedings of Data and Applications Security and Privacy XXXIX: 39th IFIP WG 11.3 Annual Conference on Data and Applications Security and Privacy, Norway,* 271 and ff. (June, 2025).

either remote, local, or hybrid.[116] This raises security concerns, due to the likely delegation of the repository to the mobile operating systems manufacturers [117] or other third parties, such as cloud providers, in the absence of a proper threat model in the development of the ARF.[118]

In the context of the EHDS, this translates into a similar concern for secure electronic health data repositories.[119] The central interoperability platform MyHealth@EU is being set up through implementing acts, [120] with no guarantee that the 'repository problem' will be addressed, while the EHDS refers specifically to eIDAS identification and authentication mechanisms to facilitate '*the transferability of personal electronic health data in a cross-border context*'.[121]

In the context of VLOPs, the current ecosystems of repository-based digital identities are built on proprietary systems that collect and manage extensive user's data. The EUDI wallets are unlikely to render these underlying infrastructures obsolete. For the sake of existing business models, VLOPs are likely to retain their current digital identity management systems, which will be linked to the wallets, representing the legal identity of individuals. As there is no regulation preventing the link between the existing accounts and wallet authentication, this is a practical likelihood.

As for the operational phase, EUDI wallets can be temporarily suspended by Member States in cases of security breaches or withdrawn when the severity of the breach justifies it – without more specific indications in the law. [122] This means that all wallets of a certain type will be affected by such decisions. However, the wallet provider, which may also be a private entity,[123] is entitled to revoke the so-called Wallet Unit Attestation (WUA), a piece of information that essentially makes the wallet operational.[124] Similarly, providers of PID and of EAA are also entitled to revoke them. [125] Surprisingly, the Implementing Regulations entrust wallet, PID and EEA providers with specifying the conditions and timeframe for revocation in their own policies, without providing further guidance.[126] This represents a significant weakness of the eIDAS 2.0 framework, which does not address this point at the legislative level, *de facto* accepting the risk that providers revoke individual wallets or the essential information forming the individual digital identity (i.e., PID and EEA) at their discretion, with even major impacts when access to health files is prevented.

---

116 ARF v2.7.3., 4.5.

117 Jaromil (D. Roio), *The Seven Sins of European Digital Identity (EUDI)* (Jan. 9, 2025), available at https://news.dyne.org/the-problems-of-european-digital-identity/ (last visited July 21, 2025) .

118 See Z. Ebadi Ansaroudi et al., *Secure and Reliable Digital Wallets: A Threat Model for Secure Storage in eIDAS 2.0,* 271 and ff. (2025).

119 R. Raab et al., *Federated Electronic Health Records for the European Health Data Space*, Lancet Digit Health e841, (5, 2023).

120 EHDS, art. 23(4).

121 EHDS, art. 16(2).

122 eIDAS 2.0., art. 5e and Commission Implementing Regulation (EU) 2025/847 of 6 May 2025 OJ L1/10.

123 eIDAS 2.0., art. 5a(2)(c).

124 Implementing Regulation (EU) 2024/2979, art. 2(8) and 7; ARF v2.7.3., 4.6.3.

125 Commission Implementing Regulation (EU) 2024/2977 of 28 November 2024 OJ L1/10, art. 5.

126 See *supra* n. 123 and 124.

V.1.3. *Preliminary conclusions*

As a preliminary result of our analysis, we contend that the ambitions of the initial SSI idea have not been fully achieved.

First, we showcase that the linkability of users' behaviors by wallet providers and a wide wallet adoption – possibly leading to a network effect[127] overcoming voluntary use - hinders the promise of natural person autonomy.

Second, we argue that the promise of transportability may not be a realistic ideal, because of the likely delegation of the repository of people's attributes to the mobile operating systems manufacturers or other third parties, such as cloud providers. Meanwhile, online platforms will likely not alter their existing identity management structures.

Third, and specifically in the context of VLOPs, we observe how the current promotion of the eIDAS 2.0 framework risks linking legal identities to the identities created to access online platforms, as regulations for these platforms increasingly require strong authentication, facilitated by the reliance on government-backed ID wallets. This unavoidable emergence of 'hybrid foundational identities' appears as a consequence of the fact that the eIDAS framework directly challenges and transforms the traditional model of fragmented, non-legal identities by creating a legally grounded identity layer for the Internet. Although this is not immediately apparent, the wallet holder authentication is tied to a verified and consistent identity, based on a device binding technique, which, even if not always mandatory, is recommended or, in any case, possible, pursuant to the ARF.[128] This is a security property within the EUDI architecture that ensures that an identifier is linked to a specific wallet so that it cannot be used independently from that device.[129] For instance, Greece has launched the 'Kids Wallet' app to promote child protection across the EU. Its goal is to verify users' ages to help prevent online addiction among minors. The app uses the Greek digital ID of a parent or guardian.[130]However, security measures based on device binding do not consider that the same device may be used by different people.[131]

Based on the results of our analysis, we caution that extending a digital legal identity scheme without grounds to do so results in a legal identity check that has no equivalent in the physical realm. In essence, the scope of a digital legal identity must be considered with

[127] A.J. Zwitter *et al., Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual*, Frontiers in Blockchain 12 (3, 2020), for more about the network effect. Simliarly, Kaplane underlies how the public and private push to use the wallet "may become irresistible" as non digital authentication proves difficult; see A. Kaplane, *The European Digital Identity Wallet: A New Human Right Unlocked?*, in Nordic Journal of Human Rights, 305, 315, (43(3) 2025).

[128] ARF v2.7.3., 6.6.3.8; see also ARF v2.7.3, 5.3.2. and 5.3.3. on the standards for selective disclosure enabling device binding.

[129] *Ibid.*

[130] Greek City Times , *Greece Launches 'Kids Wallet' App to Push for EU-Wide Child Protection*, (Mar. 14, 2025), available at https://greekcitytimes.com/2025/03/14/greece-launches-kids-wallet-app-to-push-for-eu-wide-child-protection/ (last visited July 30, 2025).

[131] A. Kaplane, *The European Digital Identity Wallet: A New Human Right Unlocked?*, in Nordic Journal of Human Rights, 314, (43(3) 2025).

utmost care, and our analysis indicates that the eIDAS framework is not sufficiently equipped to handle this task.

It is essential to note that we are not arguing that the EUDI wallet is created to control individuals, but rather, we challenge the assumption and promise that it can enhance the autonomy of individuals, in the unfolding of their online identities. Now we proceed with the final step of our assessment, questioning how this preliminary conclusion relates to the data protection principle of autonomy.

V.2. *Mismatches between eIDAS's SSI-inspired promises and autonomy as the foundation of privacy and data protection*

As explained, autonomy is one of the ultimate objectives of privacy and data protection laws – it enables data subjects to direct the processing of their personal data, and it manifests through auxiliary rights such as the right to erasure. However, the right to data protection is not an absolute right and can be limited by the GDPR or the eIDAS, as mentioned, by the extent provided in Art 52(1) of the EU Charter. However, the limitations shall be strictly necessary, as developed by a strong line of CJEU case law, rather than just being useful or convenient.

The objective of the EUDI wallets is justified as highly general, along the lines of safe, reliable and private identification. Here, first of all, there is no high-level legitimate aim for using a legally established digital identity for online services such as marketplaces. Second, less intrusive alternatives have not yet been investigated. Some techniques are suggested, such as the double anonymity, allowing selective disclosure of personal data.[132] However, it still raises questions about the residual linkability of datasets; the possibility of content providers linking tokens with cookies, which are placed by the platform before or after age verification. As mentioned, device identifiers can act as a link between this metadata. For instance, CNIL (the French Data Protection Authority) suggested to use cryptographic challenges - problems that involve encryption techniques similar to ZKPs - instead of double anonymity.[133] Another possibility is represented by Disposable Identities, designed to allow only temporally defined access, for a specific purpose and under specific circumstances or conditions.[134]

Furthermore, both eIDAS and GDPR safeguards, in addition to technical standards, should be evaluated in terms of their actual impact on the fundamental rights and

---

[132] ARCOM, *Référentiel technique sur la vérification de l'âge pour la protection des mineurs contre la pornographie en ligne (adopté le 9 oct. 2024; en vigueur depuis le 9 janv. 2025),* available at https://www.arcom.fr/sites/default/files/2024-10/Arcom-Referentiel-technique-sur-la-verification-de-age-pour-la-protection-des-mineurs-contre-la-pornographie-en-ligne.pdf (last visited July 30, 2025); Décret n° 2021-1306 du 7 octobre 2021 relatif aux modalités de mise en œuvre des mesures visant à protéger les mineurs contre l'accès à des sites diffusant un contenu pornographique, JORF n° 0235 du 8 octobre 2021 (France), available at https://www.legifrance.gouv.fr/eli/decret/2021/10/7/MICE2110638D/jo/texte (last visited July 30, 2025)

[133] E. Boucher, J. Gorin, CNIL – euCONSENT Speakers (YouTube video published March 2022), available at https://www.youtube.com/watch?v=fHD_sTwnATw (last visited July 30, 2025).

[134] J. Isohanni et al*., Disposable identities; enabling trust-by-design to build more sustainable data driven value*, IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 378-383 (2021).

freedoms. Meanwhile, it would be too naïve to argue that GDPR provisions are fit to achieve the data protection autonomy in the sense enshrined in the Charter.

As per article 6 of GDPR, the legal basis of performance of a contract or compliance with a legal obligation becomes the default for identification procedures. One prominent example of this is the age verification obligation introduced for the VLOPs that host adult content. While important to protect vulnerable individuals such as children, a legal identification obligation based on age verification raises concerns about the expansion of surveillance infrastructure. On the other hand, cybersecurity regulations and trust frameworks are extending such obligatory legal identification or biometric identification.[135] While not the central subject of this study, these type of practices also risks the increased use of sensitive human characteristics, such as biometric data, being used as a foundational identity, similar to the Aadhaar system in India.[136]

Based on the discussion above, we contend that establishing a standard identity layer online, founded on legal identities that permit linking a wallet to multiple relying parties, falls short of achieving autonomy, as a key proxy of privacy. This is mainly because the system is not genuinely user-controlled, as individuals have no actual choice to identify or not in most scenarios online. Legal identification impositions should require a rigorous, evidence-based justification showing that the limitation on the autonomy of individuals is the least harmful way, in accordance with the principle of necessity. In contrast, individuals are nudged to adhere to the rules of the platforms and regulations that steer us away from the initial ambitions of the decentralised internet.

VI. CONCLUDING REMARKS

As showcased, identity has acquired a central role for digital private and public services. It follows that whoever manages these identities has a privileged view of everyone's choices and, arguably, of everyone's orientation of thoughts. The acquisition of powers by companies and governments extends beyond the function of identity in the analogue world and has given rise to theoretical and technical research on digital identity models that can preserve individuals' prerogatives.

Our study illustrated how similar terminology can conceal fundamentally different normative orientations. We analysed the different conceptions and understandings of the same principle of autonomy in privacy and data protection, as reflected in the SSI theory and its implementation. We concluded that these understandings do not align in their

[135] This approach has also been supported by the CJEU in the recent case Russmedia Digital, in which the CJEU extended online marketplace operators' data protection obligations to include the identity verification of their users. Judgment of the Court (Grand Chamber) of 2 December 2025. X v Russmedia Digital SRL and Inform Media Press SRL Case C-492/23 ECLI:EU:C:2025:935. For cybersecurity regulations, see: E. Kun, *Searching for the Appropriate Legal Basis for Personal Data Processing for Cybersecurity Purposes under the NIS 2 Directive: Legal Obligation and/or Legitimate Interest?*, Computer Law & Security Review 56 (106098, 2025).

[136] Unique Identification Authority of India (UIDAI) available at https://uidai.gov.in/ (last visited July 30, 2025); E.Kun B.Sumer, *Setting the Standard or Breaking the Rules?: European Union Institutions*, Cybersecurity Law and Personal Data Processing (2026, Springer) (upcoming book chapter).

implications, particularly when considering the technical implementation of the SSI concept.

Our observation can also be interpreted as suggesting that digital regulation in the EU might move away from its past objectives. Moreover, the analysis showcases the ongoing configuration of autonomy in European digital governance, where technological implementation risks redefining legal principles rather than realising them. Additionally, in this paper, we argued that the EUDI wallet is inseparably tied to the legal identity of the person - without a state-backed identity as the anchor, the wallet as presented cannot legally function. Thus, the adoption of the eIDAS framework by public services and its expansion to online platforms risk creating a default reliance on legally anchored digital identities. This implies revealing significant insights on a person's online life and connections, specifically from the perspective of wallet providers and identity issuers. Even if it supposedly remains optional, the EUDI wallet should not become the default method of identification for all online transactions.

Therefore, we argue that introducing the EUDI wallet, an architecture established by and connected to legal identities, blurs the line between legal and non-legal forms of identification. This grey area has not yet been fully conceptualised in the scholarship. Further theoretical research, along with the technical implementation of EUDI wallets, should investigate overlaps between legal identification and other forms of online detection and develop a digital identity theory that considers current developments.

Moreover, the proposed system does not challenge the existing power imbalances regarding the collection of personal data by relying parties. Current structures of central management will continue with the additional layer of the EUDI wallet on top, which risks further facilitating surveillance by both public and private organisations. This not only limits control over digital identity but might also create a chilling effect through the over-normalisation of constant online tracking. Without clear limits and safeguards on when and why legal identity must be verified, there is a risk that digital identity becomes a precondition to participate in the public digital sphere, which was originally designed as a free space.

Based on our analysis, legal discourse can move beyond a narrow focus on 'identity' as a static concept and instead engage with how digital systems manage identity-linked relationships as a whole. This perspective is crucial because the governance of digital identity is the first building block that determines power allocation in the digital sphere.