WE BUILD CONSORTIUM

Deliverable D1.4

Data Protection & Ethics

Version: 1.0
February 2026

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Project and document data

Item	Description
Project title	**W**allet **E**cosystem for **B**usiness and payments **U**se cases on **I**dentification, **L**egal representation and **D**ata sharing (WE BUILD)
Grant Agreement no	101224751- DIGITAL-2024-BESTUSE-TECH-06
Deliverable title	D1.4 Data Protection and Ethics
Deliverable type	R – document, report
Responsible party	Arthur's Legal
Authors	Cristina Timón López, Arthur van der Wees
Contributing parties	Arthur's legal
Reviewers	General Council of the Spanish Notariat (Consejo General Del Notariado), Royal Dutch Association of Civil-Law Notaries (Koninklijke Notariële Beroepsorganisatie)
Dissemination level	PU – Public

History of changes

Version	Date	Change
V0.1	15th of December 2025	Drafting of initial table of contents
V0.2	26th of December 2025	Drafting of Chapters 1 and 2
V0.3	2nd of January 2026	Drafting of Chapters 3 and 4
V0.4	7th of January 2026	Drafting of conclusions
V0.5	10th of January 2026	Review and creation of consolidated document
V0.6	13th of January 2026	Draft for internal review
V0.7	2nd of February 2026	Integration of reviewers' comments
V0.8	6th of February 2026	Integration of comments from the Management Board
V1.0	9th of February 2026	Final version

Table of contents

List of figures

List of tables

1. Executive summary

WE BUILD, as part of the second round of LSPs, aims to further support the implementation of the European Digital Identity Framework through the design and testing of a set of use cases. These involve various stakeholders in the digital identity wallet ecosystem, issuers, digital wallet providers, and relying parties, who participate in order to test and understand the benefits as well as potential challenges associated with deploying digital identity wallets across the European Union.

While WE BUILD builds on the foundation of the EUDIW, its primary focus is on developing and testing digital identity wallets for legal entities. This includes use cases such as business banking, logistics, and procedures for registering and managing legal entities. Although these use cases were initially prompted by the inclusion of legal entities in the scope of the EUDIW under the EUDI Regulation, they now also need to consider a separate regulatory framework, the Proposal for a Regulation on the Establishment of European Business Wallets. Grounded in the EUDI framework, this proposal regulates a new digital identity wallet tailored to market needs, aiming to enhance competitiveness and reduce administrative burdens. Consequently, the regulatory framework relevant to Consortium partners extends beyond the EUDI Regulation, now requiring consideration of the Business Wallet Regulation Proposal, along with other relevant regulations, including the GDPR concerning personal data, as well as the measures recently published as part of the Digital Omnibus Package.

Whether it concerns natural persons or legal entities, the digital identity wallet centres around identity attributes and involves various data flows. From a personal data protection perspective, a fundamental distinction exists between data related to an individual, identifying or potentially identifying a natural person, and data pertaining to a legal entity, which, in principle, does not qualify as personal data per se. This distinction suggests that, while protecting personal data is a central element and a core driver of the EUDI Regulation in natural person digital identity wallets, the European Business Wallet primarily aims to enhance efficiency and legal admissibility in procedures. This focus may imply a trade-off, prioritising traceability over privacy. Nevertheless, such objectives do not exempt measures for personal data protection; GDPR and privacy requirements must still apply when personal data are involved, especially since the Annex to the regulatory proposal referencing the wallet requirements cites the EUDI Regulation Implementing Acts. Consequently, these considerations must be addressed within the scope of the specific interactions involving digital identity wallets, which may be limited to legal entities or involve natural persons in various capacities.

In addition, it is also important to recall that the European Digital Identity Framework outlined several overarching objectives that extend beyond privacy concerns, fundamentally centred on establishing a publicly guaranteed, user-centric, and accessible digital identity. In the case of the European Business Wallet, a significant

distinction is already evident, given its configuration as a trust service provided by the market, aimed at offering benefits to targeted users who are willing to pay a fee. However, it is crucial to understand that both digital identity wallets are expected to interoperate within a common ecosystem, generally based on shared principles, and notably, where digital sovereignty is reinforced while dependency on third countries is diminished.

Finally, these considerations must be tailored to the specific scope of WE BUILD activities, which are characterised by specialised testing environments that, while closely resembling production settings for scalability purposes, remain controlled environments explicitly designed for testing objectives. Regulatory and ethical requirements apply to these environments in specific ways, making it particularly important to ensure the free and informed consent of participants and to protect personal data whenever involved. Additionally, appropriate measures, proportionate to the associated risks, must be adopted to support secure and effective testing processes. In this context, Consortium partners involved in testing a use case shall collaborate, clearly delineate roles, and assume responsibilities to comply with the applicable legal and ethical requirements associated with these activities.

Overall, while WE BUILD activities are subject to regulatory and ethical requirements underlying the European Digital Identity Framework, as well as broader considerations associated with the EU's research framework, piloting activities will also occur during a period of regulatory change and uncertainty. This is particularly relevant given that the European Business Wallet Regulation is a proposal, and its provisions may evolve. Consequently, although this presents certain challenges, it also provides the WE BUILD Consortium with an opportunity to offer feedback on the feasibility of specific aspects, such as the implementation of privacy-enhancing techniques in use cases involving legal representatives for eventual production scenarios (outside of the scope of WE BUILD activities), ultimately facilitating an iterative process that supports the adoption and implementation of the regulatory proposal.

2. Introduction

This chapter (Introduction) provides a brief overview of the context relevant to the scope of this deliverable, along with the methodology pursued, combining desk research and analytical reflection to best meet the requirements set under the Grant Agreement (hereinafter GA).

2.1 Deliverable's scope and context

WE BUILD is part of the second round of Large-Scale Pilots (hereinafter LSPs), aiming to advance the efforts initiated during the first phase by further developing and refining ecosystems for the European Digital Identity Wallet (hereinafter EUDIW). It also represents the initial work conducted under the auspices of the recently published Proposal for a Regulation on the Establishment of European Business Wallet [1] (hereinafter also referred to as Business Wallet Regulation Proposal or European Business Wallet Regulation Proposal), which introduces a novel concept of a digital identity wallet specifically tailored for legal entities, with particular emphasis on business-to-government (B2G) and business-to-business (B2B) operations.

While sharing a conceptual foundation and aiming to leverage a common technical framework, the EUDIW and the Business Wallet present relevant differences, justified by the different types of interactions and operations they are intended to support. One of these aspects is the protection of personal data, which this deliverable seeks to address by providing some preliminary reflections.

Pursuant to the GA, this deliverable aims to provide relevant guidance on data protection and ethics for the Consortium and, more broadly, for piloting activities within WE BUILD. Data protection is a key concern in digital identity wallets, as the concept inherently involves data that can identify individuals and thus falls under the General Data Protection Regulation's [2] (hereinafter GDPR) definition of personal data. Strengthening the protection of these data has been a primary driver in transforming the digital identity ecosystem, restoring user control over their data, including decisions about sharing with third parties, and prioritising non-traceability as a fundamental requirement in designing this new ecosystem.

The emerging EUDIW ecosystem has already presented specific challenges in applying data protection roles and obligations, especially regarding personal data processed within the wallet. These challenges become more pronounced with the integration of business wallets, which are intended to interact with the EUDIW ecosystem. This is particularly evident in the case of self-employed or sole traders, but also in potential interactions between business and public sector entities with final consumers or citizens, which offer benefits such as fraud reduction.

In addition to data protection, testing activities within EU-funded research projects must comply with the highest ethical standards, particularly when involving participants. Participant engagement in piloting activities extends beyond the protection of personal data; it necessitates that participants are fully informed about the activities, their potential implications, and their roles during testing. Furthermore, Consortium partners should implement appropriate measures to ensure participants are adequately informed and provide voluntary, informed consent. Testing environments should, whenever feasible, be completely separate from operational activities and constructed with robust security measures and organisational safeguards.

This deliverable begins with a concise overview of the regulatory landscape, emphasising provisions relevant to its scope. The overview includes, as expected, a reference to the European Digital Identity Regulation [3] (hereinafter EUDI Regulation), along with two other significant regulatory proposals: the Business Wallet Regulation Proposal and measures related to personal data protection adopted as part of the Digital Omnibus package. Additionally, this deliverable builds upon lessons learned from previous LSPs, particularly regarding challenges encountered by partners, and offers initial insights into the applicability of data protection requirements to the digital identity wallets ecosystem, including the introduction of business wallets into the testing activities in line with the Proposal's text.

Finally, it is important to note that this deliverable is submitted at an early stage of the Project (M6), wherein the Business Wallet Regulation remains a proposal and is therefore potentially subject to amendments. Additionally, the various testing activities and use cases are still being defined. Consequently, while this deliverable aims to establish an overarching framework, it is equally essential for Consortium partners to concretise these elements within the scope of their specific use cases. This process is forward-looking and iterative, functioning as a feedback mechanism rather than a standalone outcome. More specifically, the work captured in this deliverable does not end with this document; instead, it is intended to actively inform and guide ongoing and future practical advisory on design and testing activities within each specific use case in the WE BUILD context and potentially reflected through future deliverables, such as *D2.1- Pilot Design*, *D2.2- Implemented use case*, *D3.1-Pilot design* or *D3.2-Implemented use case*.

2.2 Methodology

As previously mentioned in the preceding section, this deliverable seeks to establish an initial framework to support data protection and ethics within the scope of WE BUILD activities. Notwithstanding the early phase of the Project, the content of this deliverable embodies a research exercise to understand eventual implications of business wallets within the ecosystem concerning the protection of personal data. The content of this deliverable is based on:

a. The GA.

b. Knowledge acquired in previous LSPs, specifically, testing activities.

c. Internal state-of-the-art knowledge and expertise.

d. Desk research.

2.3 Target audience

This deliverable is intended for the entire Consortium and relevant stakeholders.

2.4 Structure

This deliverable includes the following chapters:

Chapter 1 serves as an introduction to the deliverable, outlining its objectives, scope, and methodology, and how these elements relate to future work.

Chapter 2 provides an overview of the relevant regulatory framework within the scope of this deliverable, with a focus on specific aspects related to the protection of personal data and other ethical considerations.

Chapter 3 analyses key data protection aspects concerning personal data in the digital identity wallet ecosystem, offering initial insights and potential scenarios relevant to the future testing and operation of business wallets.

Chapter 4 presents an overview of the relevant ethical considerations within the scope of WE BUILD activities, addressing both the broader objectives of the digital identity ecosystem and specific issues related to participant engagement and testing environments.

Chapter 5 sets out the main conclusions of this deliverable.

3. The regulatory landscape: current requirements and future developments

Digital identity wallets emerged as a new concept within the industry domain. While digital wallets have long been present in our daily lives, primarily in the contexts of payments and cryptocurrencies, their use has usually been confined to the financial sector. Although there is a point of convergence between digital identity wallets and payment wallets, exemplified by the EUDIW and the mandatory acceptance for strong customer authentication, digital identity wallets are fundamentally centred on identity attributes. These attributes, which are characteristics or elements associated with an individual's identity, are managed through the wallet and can be shared with third parties under the individual's control.

From a regulatory perspective, the emergence of digital identity wallets has been marked by the adoption of the EUDI Regulation. The EUDIW has become a cornerstone of this regulatory proposal, serving as a tool that, within the legal framework of electronic identification, effectively bridges electronic identification and trust services. Ultimately, it creates an ecosystem where, although the EUDIW is still conceived as being provided or guaranteed by Member States, it also actively leverages the market, particularly trust services, through the new trust service offering electronic attestations of attributes (hereinafter EAAs).

Privacy and data protection were fundamental values within the EUDIW ecosystem and served as primary drivers for the transformation of the digital identity landscape. Non-traceability, privacy by design, and selective disclosure emerged as core requirements of EUDIW, necessitating extensive technical development to ensure the desired level of privacy while maintaining operational efficiency.

While several aspects of the EUDI Regulation have already been addressed through the initial phase of LSPs, certain points remain underdeveloped or warrant further reinforcement in this subsequent phase. Additionally, the regulatory landscape is expected to become increasingly complex with the anticipated adoption of the Business Wallet Regulation Proposal. Unlike the EUDIW, this proposal emphasises traceability as a fundamental feature to meet the requirements of B2G (and B2B) operations. However, the business wallet is not projected to operate independently of the EUDIW; rather, both wallets are designed to ultimately interoperate in a common ecosystem.

Consequently, to shed some light on this point, it is necessary to consider a set of regulations or regulatory proposals that will ultimately be relevant to the activities and development of use cases within WE BUILD.

3.1 The EUDI Regulation

As previously mentioned, one of the primary motivations behind the adoption of the European Digital Identity Framework was to strengthen the privacy of European citizens when using digital identity services. The regulatory landscape for these services, which was largely fragmented, led to reliance on third-country identity providers when accessing a wide range of services, often under inadequate privacy conditions.

The EUDIW was established as a fundamental component within the EUDI Regulation, imposing strong privacy requirements integrated into the technology's design. Specifically, these requirements mandate non-traceability, preventing 'surveillance' by both the digital identity wallet provider and trust services, particularly those responsible for issuing EAAs. Achieving non-traceability has required extensive effort, especially in authentication protocols and signatures, to ensure user non-traceability and unlinkability from both the service provider and the digital identity (wallet or attestation) provider.

Beyond privacy, it is essential to note that the EUDIW is governed by a set of functional and non-functional requirements, which have been further refined through the Architecture Reference Framework (hereinafter ARF). These requirements have been incorporated into the initial round of LSPs and emerging digital identity wallets and must be maintained within the scope of WE BUILD as long as digital identity wallets for natural persons are developed and tested.

Furthermore, beyond privacy considerations, the EUDIW aims to transform the digital identity ecosystem by reestablishing user control over their data. This control requires that other entities within the ecosystem retain only the data necessary to deliver their services. Concurrently, users must be able to use the EUDIW in a manner that is accessible and transparent, enabling them to make informed decisions.

Overall, the EUDI Regulation establishes a new digital identity ecosystem that aligns more closely with the concept of a decentralised, user-centric digital identity, while leveraging the legal frameworks for eID and trust services. While the EUDIW represents an initial form of identity for natural persons, particularly through its configuration, which links person identification data (hereinafter PID) with the wallet application, this form is expected to be expanded through additional credentials, notably EAAs that have emerged as a new trust service, and therefore, constitute part of a regulated market.

Since the EUDI Regulation has been thoroughly examined in the scope of previous LSPs and, given that this document does not intend to reiterate such an analysis, it is hereby reaffirmed, for clarity, that the requirements established by the EUDI Regulation, along with those formulated through the adopted Implementing Acts, remain applicable within the scope of WE BUILD whenever EUDIW is involved. Consequently, development efforts under the WE BUILD use cases should strive to conform to these requirements.

3.2 The General Data Protection Regulation

The GDPR, enacted in 2018, established comprehensive privacy and data protection requirements for EU citizens and for services provided within the scope of the EU (regardless of the provider's location). These extend from specific roles and the provision of services involving the processing of personal data to technological measures, including principles such as privacy by design and privacy by default.

The GDPR is the foremost regulatory framework that has significantly enhanced, and in many ways pioneered, the protection of personal data not only within the EU but also beyond its borders. The regulation is anchored in a set of fundamental principles. These principles mandate that personal data must be processed lawfully, fairly, and transparently; collected solely for specific and legitimate purposes; and confined to what is necessary. Data must also be accurate and kept current, stored only for as long as necessary, and safeguarded through appropriate security measures to ensure confidentiality and integrity. Ultimately, organisations are required to be accountable, bearing responsibility for adhering to these principles and demonstrating compliance.

While the EUDI Regulation has established specific privacy requirements, such as non-traceability, the GDPR remains entirely applicable to the EUDIW and European Business Wallet ecosystem. As discussed in Chapter 3, the applicability of the GDPR raises certain questions, particularly concerning the allocation of roles, such as data controller and data processor, as well as the exercise of specific rights, including the right of access or the authorisation to share particular data through the EUDIW which differs fundamentally from the legal basis for processing personal data within the specific processes enabled by the EUDIW.

3.3 Digital Omnibus Package, proposed measures impacting personal data processing

The Digital Omnibus Package [4] introduces several measures that impact regulations in the digital sphere, particularly in the areas of artificial intelligence, data protection, and cybersecurity, through the Proposal on the simplification of the digital legislation. While this regulation is still a proposal and the articles may be amended before final adoption, some measures warrant consideration within the scope of WE BUILD activities, as they are likely to impact the digital identity wallets ecosystem.

Regarding personal data, the abovementioned Proposal has introduced significant measures that could influence data protection within the EUDIW ecosystem. One of the most notable measures is the revised definition of personal data. Specifically, paragraph 1 of Article 3 adopts a relative approach to classifying personal data, meaning that data is considered non-personal if the entity possesses no reasonable means to identify the individual to whom the information pertains. This concept has been discussed in

relation to the differing approaches of the GDPR, the Article 29 Working Party [5], and case law, which distinguish between an absolute approach, where data must be fully anonymous to all parties, and a relative approach, where data need only be anonymous to the data controller.

Another significant development in the scope of data protection, particularly relevant for data processing within the EUDIW ecosystem, is the introduction of new exemptions regarding the classification of biometric data. In this context, the Proposal reopens a debate that has previously existed regarding the distinction between biometric data used for identification and authentication. As highlighted by the Europea Commission's White Paper on Artificial Intelligence [6] as well as the Article 29 Working Party Opinion 3/2012 [7], it was necessary to distinguish between biometric identification as the process of comparison of biometric data with templates or data stored in a database (search of correspondence), and biometric authentication, as the process of comparison of biometric data with a single biometric template stored in a device, which is not considered as the processing of special categories of personal data. Some data protection authorities, such as the Spanish Data Protection Agency, had already confirmed this idea through its Report 0036/2020 [8].

The Proposal formalises this approach in the legislative text, highlighting that the data subject must retain control over the verification process, which may involve storage on the device or with the controller, provided that the encryption key remains under the data subject's control. Furthermore, the controller should not gain access to the biometric data, or only for a very limited period. Consequently, this provision would clarify that authentication (or verification) processes conducted through the wallet do not fall within the special categories of data, thereby simplifying these processes, which are expected to be recurrent with the use of the wallet. However, there may be some processes in which the crucial factor will be the exact time at which the controller gains access to the biometric data, and the potential for interception or security compromise (e.g., certain identity proofing processes in which verification of identity does not take place solely within the device itself).

Furthermore, the text of the Proposal introduces additional relevant measures in the scope of personal data protection. Specifically, certain data subject rights, such as the right of access, may be exempted when there are reasonable grounds to believe the data subject already possesses the information. This is particularly significant in the context of data processed within the wallet. Additionally, other provisions are noteworthy, although they are expected to have less direct impact on the digital identity wallet ecosystem, such as data breach notification requirements limited to cases likely to result in a high risk, and the anticipated adoption of implementing acts by the European Commission to specify criteria and means for determining when data derived from pseudonymisation no longer qualifies as personal data for specific entities.

3.4 The Proposal for a Regulation on the Establishment of European Business Wallets

From a regulatory perspective, a key milestone of the WE BUILD activities was the adoption of the Proposal for a Regulation on the Establishment of European Business Wallets, published alongside the Digital Omnibus Package. This initiative builds on the Competitive Compass for the EU, which previously outlined the role of business wallets, leveraging the European Digital Identity Framework, aiming to become the foundation for conducting business in a simple and digital manner within the Union.

Without attempting to provide an exhaustive analysis, it is important to note that the Proposal defines business wallets in a manner equivalent to the EUDIW, enabling the issuance, storage, management, combination, and sharing of identification data, EAAs and electronic signatures and seals. However, the Proposal also emphasises additional functionalities beyond the scope of the EUDIW, such as the creation, management, and delegation of mandates to authorised representatives. Consequently, within the scope of business wallets, the concept of authorised representatives is crucial, as onboarding already requires an authorised representative of the legal entity that emerges as the business wallet owner. Therefore, for the purposes of this deliverable, it is crucial to highlight that this interaction inherently involves personal data.

In addition to these fundamental features, also present in the EUDIW, the business wallet is expected to offer supplementary functionalities tailored to the specific scope of its deployment. Such features may include the ability to link attestations (forming chains of attestations or chains of trust), the capacity to receive and transmit electronic documents, as well as issuance management and revocation of authorisations. Furthermore, while these functionalities are considered core and the minimum required to be provided by the Proposal, it is foreseeable that providers of the European Business Wallet may also offer additional features beyond those explicitly outlined.

From a non-functional requirements perspective, the Proposal emphasises a set of technical features, with a strong focus on security by design and traceability. Of particular significance is the capability for automatic interaction, occurring without manual intervention or direct user action. This represents a crucial distinction from the EUDIW, which is chiefly governed by user control and sovereignty.

Furthermore, it is also particularly notable that the Proposal explicitly introduces the principle of equivalence when utilising any of its core functionalities, a concept already outlined in the eIDAS Regulation within the scope of trust services. Consequently, from the Proposal's perspective, the European Business Wallet provider is considered a trust service. This perspective is further supported by Article 7, which mandates that European Business Wallet providers comply with trust service requirements as well as those outlined in the NIS2 Directive. Regarding personal data, it requires providers to be

established within the territory of the Union, to have their principal place of business and primary operations located in the Union, and to pose no risk to the security of the Union. Additionally, providers must not be controlled by a third country or a third-country entity. Furthermore, business wallet providers are expected to be subject to the trust services supervisory and oversight regime and are exempt from certification obligations concerning the EUDIW.

To facilitate the deployment of business wallets, the Proposal envisions the European Digital Directory as a trusted source maintained by the European Commission that provides information for European Business Wallet owners. Recital 39 of the Proposal establishes that where the European Digital Directory processes personal data, such processing shall be carried out in accordance with relevant data protection principles, such as data minimisation and purpose limitation, as well as other obligations such as privacy by design and by default, including, where appropriate, pseudonymisation.

Regarding the acceptance of the European Business Wallet, Article 16 mandates its recognition by public sector entities for identification and authentication purposes, as well as for electronic signatures or seals, submission of documents, and notifications. Furthermore, the Proposal envisions the use of a qualified electronic registered delivery service as a standalone, separate service from the business wallet, serving as a gateway for document submission and notification receipt.

Finally, it is important to note that a particular aspect of the Proposal regarding the scope of acceptance is the potential international use of business wallets beyond the European Union. Specifically, Article 17 envisions that the Commission, through implementing acts, may recognise third-country business wallets, which could facilitate mutual recognition scenarios. While this could enhance economic efficiency, it may also raise concerns about interactions, such as issues related to the protection of personal data.

While the Proposal includes detailed provisions across various aspects, this section or deliverable does not aim to provide an exhaustive analysis of the legislative text. Nonetheless, to facilitate alignment of WE BUILD use-case activities with the legislative framework, its development will be closely monitored, and assistance will be provided to Consortium members whenever a particular provision necessitates a more in-depth review.

Consequently, for the purposes of this deliverable, three key aspects of the Proposal are highlighted:

a. First, while the European Business Wallet represents a legal entity, it is fundamentally based on the authorisation of a natural person to act on behalf of that entity.

b. Second, the Proposal notably lacks explicit privacy requirements, instead prioritising traceability, which may necessitate addressing the appropriate balance, as discussed in greater detail in Chapter 3.
c. Third, business wallets are conceived as trust services, a qualification that entails significant implications not only for guarantees relating to service provision, but also for the applicable oversight and notification regimes.

3.5 eIDAS, European Business Wallets, and the interplay of intertwined EU Regulatory Frameworks

While this deliverable primarily focuses on data protection and ethics, it is important to recall that the EUDI Regulation and the forthcoming European Business Wallet Regulation are not standalone instruments. Rather, they are closely interconnected and should be understood as part of a broader regulatory and policy framework. In this context, although digital identity, whether for natural persons or legal entities, lies at the core of contemporary digital ecosystems, these ecosystems rely on additional enabling 'components' to function. Notably, at least two such components can be clearly identified: data governance and risk management.

With regard to the first element, several regulations may fall within the scope of the WE BUILD use cases, depending on the specific pilot, its focus, and objectives. These include, in particular, the Data Act [9] and the Data Governance Act [10], which have emerged as overarching regulatory frameworks for data sharing in the EU. In addition, sector-specific legislation may also be relevant. As examples of this, in the financial sector, we identify the proposed Financial Data Access Regulation (FIDA) [11], as well as the proposal for a third revision of the Payment Services Directive (PSD3) [12] or the proposal for a Payment Services Regulation (PSR) [13]. Within the transport ecosystem, it is also relevant the **Electronic Freight Transport Information (eFTI) Regulation [14],** which establishes a framework for the electronic exchange of freight transport information.

Furthermore, in line with the Digital Decade 2023 policy programme, which emphasises the delivery of risk-based strategies such as the EU Cybersecurity Strategy, cybersecurity-related legislation also becomes highly relevant. In this context, relevant regulations include the NIS2 Directive [15], which is directly applicable to trust services. In addition, other instruments are also relevant, including the Cybersecurity Act [16] and the Cyber Resilience Act [17], or even within specific domains, such as the financial sector, regulations such as the Digital Operational Resilience Act (DORA) [18] apply.

Likewise, it is important to consider that artificial intelligence has become an integral part of contemporary digital ecosystems and is expected to have a significant impact on identification processes. This impact is already evident, for example, in the emergence

of deepfakes and in the increasing risks associated with digital identification and verification procedures, demanding the consideration of the applicable regulatory framework, the Artificial Intelligence Act [19], as well as the potential impact of artificial intelligence on other regulations (e.g., the Commission Implementing Regulation 2015/1501).

Consequently, while it is not the objective of this deliverable to provide an exhaustive regulatory analysis, it is important to recall that the EUDI Regulation is not an isolated instrument, nor is the Proposal for the establishment of European Business Wallets, and therefore, when assessing the applicable regulatory framework, it is essential to take into account the broader set of surrounding regulations that shape digital ecosystems. Furthermore, careful consideration should be given to sector-specific legislation that enforces additional or customised requirements, particularly when traditional legal procedures are adapted to digital (and cross-border) formats. A relevant example in this regard is precisely the EU Digital Power of Attorney, which explicitly incorporates interaction with the eIDAS framework in the latest revision of the Company Law Directive [20].

3.6 Applicability of regulatory requirements within the scope of WE BUILD

Although WE BUILD aims to evaluate EUDIW and European Business Wallets in environments very close to production (i.e., referred to as pre-production), its activities remain specifically tailored to the LSP scope. Therefore, regulations might have 'limited' applicability, especially given that the European Business Wallet Regulation is still a proposal and may change.

Consequently, while within the scope of the WE BUILD activities, data protection requirements and the ethical principles underpinning the relevant regulations should guide the activities, it is possible that full compliance with all obligations may not be feasible due to the use of closed or testing environments. Nevertheless, the following recommendations are proposed.

a. When a regulation has already been adopted, and its applicability to a production environment has been determined, the use case must conform to those requirements, even if it is within a controlled environment, to ultimately facilitate transition into production. Such consideration applies not only to the EUDI Regulation and Implementing Acts but also to other pertinent regulatory frameworks, such as laws transposing the NIS2 Directive.
b. When a regulation has not yet been adopted, but a proposal and its development are publicly available, it is essential to incorporate its fundamental concepts and objectives, which should steer development and testing activities. This approach will be especially evident in the case of the Proposal for a Regulation on the Establishment of European Business Wallets.

c. When the testing environment is separated from production, its specific characteristics should be addressed. These characteristics could impact aspects such as the qualification of parties involved in the same data processing activity, which may share a common purpose, such as research, or the legal basis for personal data processing, as well as considerations related to potential research uses. Additionally, security measures might need to be adapted to the specific research environment.

4. Personal data protection implications

As mentioned in previous chapters, the processing of personal data is fundamental to digital identity wallet ecosystems, which are built on the sharing of identity attributes; consequently, they often involve the sharing of personal information. The introduction of business wallets within the ecosystem, however, may present particular considerations, as the information involved does not necessarily pertain to an identifiable natural person. Nonetheless, this distinction is not absolute; in some cases, interaction may arise from the required involvement of an authorised representative, while in others, it may result from interactions with natural persons in a professional capacity, or as citizens or consumers.

4.1 Processing of personal data in digital identity wallet ecosystem

The digital identity ecosystem introduced by the EUDI Regulation delineates several roles that converge within the ecosystem across separate data processing activities [21]. These can be fundamentally categorised into three activities:

a. Data processing for the issuance of the identity credentials (PID or EAAs).
b. Data processing within the wallet itself.
c. Data processing during the sharing of information with relying parties to access services.

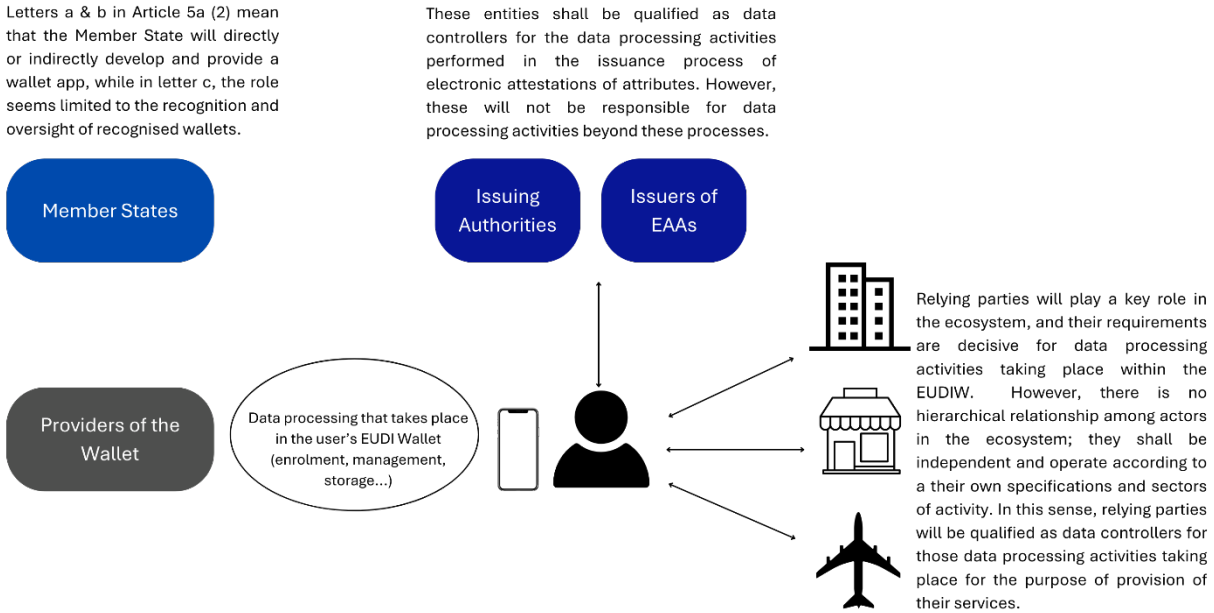

Figure 1. Digital identity wallet data processing ecosystem

Among these processes, a fundamental distinction exists compared to traditional digital identification models, in which information is transmitted directly from the identity provider (hereinafter IdP) to the service provider or relying party. In contrast, within the

digital identity wallet ecosystem, the EUDIW plays a central role in empowering users to control their personal data by enabling identification and authentication through the request and selective disclosure of credentials to relying parties. As a result, this new ecosystem shifts responsibility for authentication away from the IdP and towards the wallet itself, since, due to privacy and user-control considerations, the EUDIW provider should neither actively participate in nor exercise control over these processes.

While this approach was needed nowadays and aligns with the EUDI Regulation main drivers, technologies involving the processing of personal data and exclusively managed under user control can challenge traditional legal notions of data controller and data processor according to the GDPR (Article 4 paragraphs 7 & 8), which are, in principle, thought for a scenario where there is a physical control of the data processed by the controller.

Article 5a paragraph 1 of the eIDAS 2 Regulation establishes that 'each Member State shall provide a European Digital Identity Wallet'; however, paragraph 2 of this Article provides three different possibilities for the provision of the EUDIW, allowing the independent provision by private entities recognised by that Member State. Considering that the data controller qualification is purpose-based, in those scenarios where there is a direct or indirect provision by the Member State, it seems clearer that, insofar as this has the obligation and, therefore, the interest to provide it, the public entity attributed with the administrative authority for the issuance of the EUDIW will hold a data controller role.

However, this conclusion is less straightforward in the context of Member State recognition of wallets. In this scenario, it may be argued that wallet application developers exercise the greatest degree of control over the determination of the purposes of data processing, insofar as they technically operationalise the processing by transforming data into concrete actions or effects [22]. Moreover, as established by European case law (see, in this regard, paragraphs 69 and 82 of *Fashion ID* [23] and paragraph 69 of *Jehovan Todistajat* [24]), qualification as a data controller does not depend on having actual access to the personal data concerned. Nevertheless, this is an issue that should be clarified by the relevant data protection authorities. As a temporary solution, it is recommended that wallet providers incorporate a brief privacy notice highlighting the technology's functionalities and user control over data (e.g. data erasure), as well as the wallet provider's inability to access the data when applicable.

In addition to the data processing carried out within the wallet itself, other stakeholders in the ecosystem are responsible for their own processing activities, including issuers of EAAs and relying parties. Furthermore, certain technology providers may assume the role of data processors within the ecosystem, thereby requiring the conclusion of appropriate data processing agreements with the relevant data controllers.

All actors within the ecosystem are subject to the principles and obligations of the GDPR. In this respect, issuers of identity credentials or personal identification data must inform users, in a transparent manner, of the data processed for those purposes and must limit collection to what is strictly necessary. Likewise, relying parties should request only the data essential for the provision of their services and retain such data only for the period strictly required.

Furthermore, beyond the data processing within the wallet, other ecosystem stakeholders are responsible for their own data processing, such as issuers of EAAs or relying parties. Furthermore, it is also possible that certain technology providers hold a data processor role within the ecosystem, requiring the signature of the necessary data processing agreements with the respective controllers.

In addition, a joint controllership arrangement may arise when there is a common determination of the purposes and means of processing, for example, when two companies are actively involved in the issuance of a credential. More specifically, in the context of a piloting activity within the scope of WE BUILD, it may be considered that all participating entities jointly determine the purposes and means of the processing, namely, the performance of the piloting activity, and should therefore be regarded as joint controllers for that specific pilot. In such cases, it is essential that at least one entity, typically the pilot leader, assume a coordinating role and serve as the primary point of contact for the data subjects involved in the piloting activity (e.g., via a consent/information form or other appropriate means).

As a specific requirement, compliance with these principles should be implemented through the EUDIW interface. Accordingly, even within the scope of WE BUILD activities, it is essential that all stakeholders participating in a given use case incorporate these safeguards directly via the EUDIW, rather than through separate documents or alternative mechanisms. This approach contributes to the further development of the EUDIW ecosystem and strengthens the wallet-based ‘authorisation model’ for data sharing.

In this regard, it is also important to recall the requirement established under Article 5a, paragraph 4 letter d of the EUDI Regulation, further specified in Article 9 of Commission Implementing Regulation (EU) 2024/2979 [25], which mandates EUDIW to store transaction logs of transactions performed through the wallets. This requirement is also set out in the Business Wallet Regulation Proposal (Article 5 paragraph 1, letters l and m). In addition, it is important to note that the EUDI Regulation is not limited to transaction logs; wallets shall support the ability of relying parties to easily request the erasure of personal data and to report relying parties to competent data protection authorities. In the scope of WE BUILD piloting activities, such functionalities should also be supported by privacy officers or equivalent roles.

Likewise, it should be recalled that, where the non-traceability and unlinkability requirements under the EUDI Regulation apply, the underlying technological solutions must be designed and implemented in full compliance with those requirements.

Another important feature to mention concerns the different possible types of credentials potentially associated with a digital identity wallet ecosystem. In this regard, while PID would be issued under the wallet national scheme, other credentials are issued as EAAs either by trust service providers or issued by public sector entities. In this regard, it is also important to recall that the EUDI Regulation opened the door to qualified trust service providers to verify, by electronic means, those attributes listed in Annex VI, including the powers to and mandates to represent natural or legal persons. This, however, should be limited to a verification interface, pursuing the EUDI Regulation and more specifically Article 9 of the Commission Implementing Regulation (EU) 2025/1569 [26] but also relevant technical standards, such as ETSI 119 478 [27]

Experience from previous LSPs revealed a recurring issue: insufficient recognition that multiple, separate entities were involved in separate data processing activities, potentially relying on different legal bases. As a result, it was necessary to ensure that users were properly informed of these separate processing operations, as well as to clearly distinguish consent given for the protection of personal data from consent provided for participation in the piloting activity.

In addition, technology providers that may operate 'in the middle' of issuance and data-sharing processes should be subject to strict privacy obligations under the EUDI Regulation. Consequently, certain technical or organisational approaches used in pilot environments may not be compliant in a production setting. Furthermore, the potential involvement of non-EU countries, whether jointly with EU-based actors or independently, in data processing activities must be carefully assessed, including the need for Standard Contractual Clauses (hereinafter SCCs) or the existence of an applicable adequacy decision. In this regard, following the Consortium's composition and the indications in the Ethics Summary Report, Norway is part of the European Economic Area and the UK and Switzerland have adequacy decisions in place. However, in the case of Moldova, Mauritius, and Bosnia and Herzegovina there might be a need to rely on SCCs. Regarding Bosnia and Herzegovina, the country has recently amended its data protection law to be aligned with EU standards.

Consequently, to facilitate the integration of data protection obligations within the scope of WE BUILD activities, the following brief guidelines, comprising a set of questions and potential scenarios, are provided.

Question	Possible answers
Does the testing activity or use case involve the processing of personal data?	Yes
	Partially, only limited to the information of participants
	No, the activity is limited to synthetic data
Which data processing activity is my entity responsible for?	Issuance of credentials
	Wallet storage and setup
	Provision of the service (relying party)
	Technical support in the issuance or sharing of identity credential
	No technical process, but coordination of piloting activity and collection of information from participants
What role does my entity hold in the data processing activity?	Controller
	Processor
Is my entity involved in data processing with several entities in the same data processing activity?	No, I am sole controller
	Yes, we are joint controllers and have allocated responsibilities in a transparent and accountable manner
	Yes, we are data controllers and processors and have signed a data processing agreement
Is my entity located outside the EU, or does it engage with any entity outside the EU's borders?	No
	Yes, but there is an adequacy decision
	Yes, but there is no adequacy decision requiring SCCs
Does my entity provide transparent information about data processing and have a suitable legal basis?	Yes, my entity requests informed consent
	Yes, my entity relies also on other legal bases, but provides information to data subjects about the processing
Does my entity ensure data minimisation in the processing of personal data?	My entity requests the strictly necessary data, and when personal data are not required, it does not request personal data
	My entity limits the storage to the minimum required time

Table 1. Common data processing questions in digital identity wallet testing

4.2 Specificities of personal data processing in the European Business Wallet

The European Business Wallet is presented as a concept that, while based on the ARF as highlighted in Recital 4 of the Proposal, and mandated to comply with the EUDI Regulation Implementing Acts as per Annex 1, is structured around a fundamentally different basis. For example, as previously noted, the European Business Wallet is conceived as a trust service and therefore does not fall under the electronic identification scheme of the eIDAS Regulation.

The EUDIW, under the electronic identification legal regime of the EUDI Regulation, is fundamentally structured around privacy requirements, as noted in various provisions, such as Article 5 letter b, and Article 5 paragraph 14, among others. These requirements have also been incorporated into the scope of the ARF.

The Proposal on the Establishment of European Business Wallets does not include such provisions regarding the requirements for business wallets. However, there is a mention of the processing of personal data within the scope of the European Digital Directory. Such processing should adhere to relevant data protection principles, including data minimisation and purpose limitation, as well as obligations such as data protection by design and by default, and, where appropriate, pseudonymisation.

Nevertheless, in the operation of the business wallet itself, the independence from personal data processing is not absolute, and the following points are identified.

a. **Use of the European Business Wallet by self-employed individuals and sole traders.**

   The European Business Wallet does not cover all possible business scenarios. In particular, the proposal foresees that self-employed individuals and sole traders may use the EUDIW for business purposes. Consequently, the EUDIW will inevitably involve the processing of personal data, as is typical in cases where professional and personal roles overlap.

   In this context, it is essential to clearly distinguish between professional uses of the wallet and situations in which privacy considerations may be secondary to traceability requirements, such as compliance with reporting and regulatory obligations. Possible measures could include informing users, through explicit warnings, about the data required for specific transactions, or limiting the use of certain privacy-enhancing technologies, such as zero-knowledge proofs, where full traceability is legally required. Furthermore, the use of pseudonyms within the EUDIW is subject to national legal admissibility, and, conversely to the EUDI Regulation, the Business Wallet Regulation Proposal does not provide for the use of pseudonyms.

b. Selective disclosure and privacy-enhancing technologies in the European Business Wallet

Although the Business Wallet Regulation Proposal does not introduce 'strict' privacy requirements, Article 5 letter b provides that the wallet shall enable selective disclosure. Accordingly, where the relevant use case allows, the disclosure of data should be limited to what is strictly necessary for the specific operation. However, the Proposal makes no reference to zero-knowledge proofs, which suggests that such techniques are not envisaged within the scope of the business wallet use cases, and therefore, while these are not prohibited, advanced privacy-preserving techniques should be further assessed per use case.

c. GDPR obligations, governance, and supervision of European Business Wallet providers

GDPR obligations apply to European Business Wallet providers and, more broadly, to trust service providers, which are subject to specific regulatory requirements and technical standards. The European Business Wallet identification data provider is also envisaged as a trust service and is therefore subject to GDPR obligations. In addition, providers of European Business Wallets must be established within the Union, meaning they must have their principal place of business and core operations in the EU and must not pose a risk to the security of the Union. In particular, they must not be subject to control by a third country or a third-country entity.

Furthermore, in the context of governance and supervision, Article 13 paragraph 5 letter g requires supervisory bodies responsible for Business Wallet providers to cooperate with data protection authorities by informing them without undue delay of any situation in which data protection rules may have been breached.

d. Enrolment and identity proofing requirements

Enrolment in the European Business Wallet requires identity proofing of a legal representative at a substantial or high level of assurance pursuant to the Commission Implementing Regulation 2015/1502 [28]. This process necessarily involves the processing of personal data and therefore requires the systematic incorporation of privacy and GDPR considerations throughout the enrolment phase.

e. Use of the European Business Wallet with or without identification of the legal representative

From a privacy perspective, a key consideration is the distinction between scenarios that require full traceability of the natural person acting as a legal representative of the business wallet owner and those in which it may be sufficient to demonstrate that the wallet is authorised to act on behalf of the legal entity without revealing the

identity of the natural person behind it. In this context, as noted above, techniques such as selective disclosure may allow proof of authority (e.g. confirmation that the user is an authorised representative) without requiring disclosure of the individual's full identity.

When the authorised representative needs to be identified, different legal bases may apply to the processing of that data. Nevertheless, these processing would primarily take place on the basis of a contractual necessity pursuing Article 6 paragraph 1 letter b (e.g., when the data is necessary to establish, manage or perform a contract with the other legal entity), a legal obligation pursuing letter c of the same article (e.g., when the data are necessary for tax or accounting purposes), or on the basis of legitimate interests pursuing letter f (e.g., when the aim is to verify the authority to represent the entity or maintain business communication). The same reasoning applies to self-employed individuals or sole traders.

The applicable legal basis will need to be assessed in the context of the specific data flow for which Consortium partners can request support from the Ethics Mentor, bearing in mind that the legal grounds may differ in a production scenario (i.e., outside of the scope of WE BUILD activities or 'pre-production stage'), such as legal obligation, contract performance, or legitimate interest, compared to a pilot activity, where the processing of personal data ultimately depends on consent due to the necessity of the data for executing the pilot.

f. International interoperability and cross-border data transfers

Business Wallets, unlike the EUDIW, open the door to operating in an international and cross-border context directly through the regulatory proposal, being Chapter IV dedicated to these international aspects. Where the interaction involves the processing of personal data, such as data relating to a legal representative or an ultimate beneficial owner (UBO), the GDPR applies.

When such personal data are transferred to recipients located outside the European Union, the requirements for international data transfers under the GDPR become applicable. In particular, this includes the need for an adequacy decision or, in its absence, the use of appropriate safeguards such as SCCs.

4.3 Scenarios of interaction between digital identity wallets

Although the Business Wallet Regulation Proposal explicitly focuses on the use of business wallets in relation to the public sector, particularly for reporting obligations and administrative procedures (imposing mandatory acceptance by public sector entities), it does not exclude the possibility of using business wallets in other interactions, such as

with other business wallets or with natural persons in both professional and personal capacities.

At least, the following scenarios should be considered

a. Business to Government (B2G) - Example: cross-border public procurement

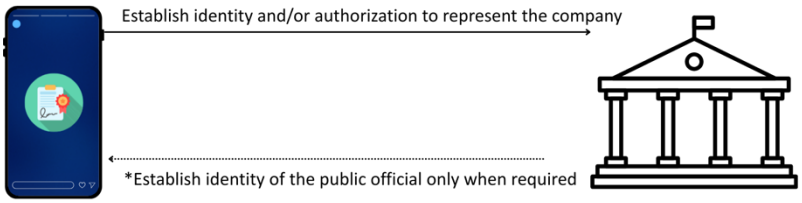

Figure 2. B2G interaction

In a B2G scenario such as cross-border public procurement, it is generally necessary to disclose the identity of the natural person acting as the authorised legal representative of the company, together with proof of their role and their power to bind the company for the specific contract. This disclosure is typically required to ensure legal validity, accountability, and enforceability of the contractual relationship.

From a data minimisation perspective, it may be considered whether disclosure could be limited to proof that the person acting is an authorised representative, without revealing their full identity. However, the feasibility of such an approach depends on the nature of the operation. In the context of public procurement, the conclusion and signature of a contract usually require full identification of the signatory parties. By contrast, in other B2G use cases, such as regulatory reporting or information exchange, it may be sufficient to identify the legal entity and provide proof of valid representation, without requiring the disclosure of personal data relating to individuals on the public authority's side.

b. Business to Business (B2B) - Example: signature and conclusion of contracts

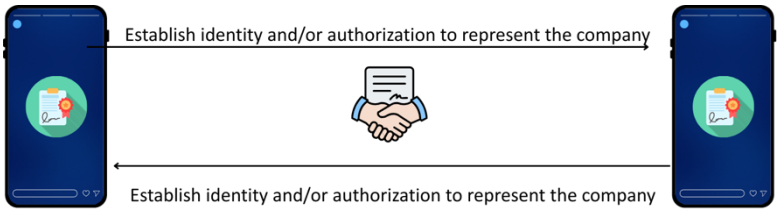

Figure 3. B2B interaction

Beyond interactions with public sector bodies, European Business Wallets may also be used in transactions between legal entities, for example, for the conclusion of contracts. In such scenarios, personal data are typically disclosed on both sides in order to demonstrate that the natural persons acting are authorised legal

representatives and have the power to bind the respective legal entities for the specific process.

It may be questioned whether the use of identification and signatory data in this context constitutes processing of personal data. However, given the broad definition of processing under the GDPR, the use of such data for the purposes of authentication, validation, and attribution of signatures falls within the scope of personal data processing.

c. Business to Natural Person in a Professional Capacity -Example: hiring a freelancer

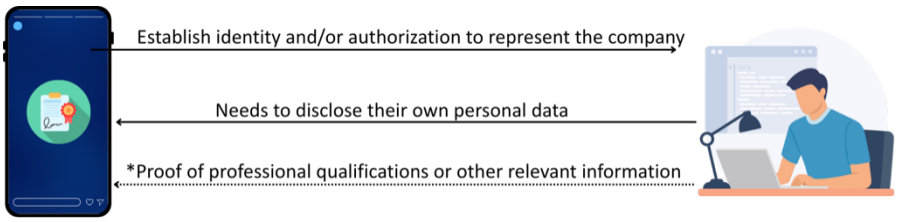

Figure 4. Business to professional interaction

As noted in the previous section, self-employed individuals are expected to use a natural person wallet (i.e., EUDIW). A freelancer acts under their own name, which means that any interaction will necessarily involve the disclosure of personal data. Consequently, in most interactions with a self-employed person, the processing and disclosure of personal data are unavoidable, particularly where contractual validity, taxation or liability considerations apply.

Nevertheless, selective disclosure may still be applied to additional attributes, such as professional qualifications or regulatory status, in order to limit the disclosure of unnecessary personal data. Furthermore, given that self-employed individuals rely on a natural person wallet, it is necessary to distinguish between interactions in which full identification is required for legal validity and those in which pseudonymous or other non-traceable and unlinkability mechanisms could, in principle, be used but are excluded due to applicable legal requirements.

d. Business to Natural Person as a Consumer - Example: conclusion of an energy contract

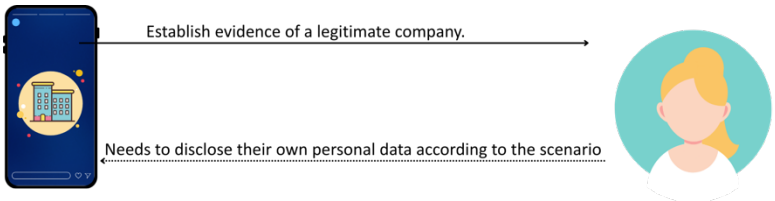

Figure 5. Business to consumer interaction

In addition to interactions with natural persons in a professional capacity, European Business Wallets may also be used in interactions with natural persons acting as consumers. From the consumer's perspective, such interactions will generally require the disclosure of personal data in order to conclude a valid contract. Nevertheless, privacy safeguards should be in place to ensure that personal data is disclosed only to the extent strictly necessary.

From the business perspective, it is generally not necessary to disclose the identity of the specific natural person acting on behalf of the company. Rather, what must be demonstrated is the legitimacy of the legal entity and, where relevant, that the person acting is authorised to represent it. In this context, the European Business Wallet primarily serves to verify the company's legal status and regulatory authorisation, rather than the identities of its individual representatives.

5. Ethical considerations in WE BUILD activities

Beyond data protection considerations, it is important to recall that other objectives define the European Digital Identity Framework, notably the establishment of a publicly guaranteed, accessible, and user-controlled digital identity. In the case of the European Business Wallet, while some elements are similar, it differs significantly, such as being configured as a trust service and, accordingly, as a market-provided service aimed at specific users and offering functionalities designed to attract them.

Additionally, it is essential to recall that within the scope of piloting activities, ethical considerations mandate that participants are fully informed and provide transparent consent to their involvement, being aware of the implications. Furthermore, Consortium partners involved in piloting activities should anticipate and implement a set of controls within a specifically designed environment optimised for testing purposes.

5.1 Overarching objectives of the European Digital Identity Framework and their application to European Business Wallets

The European Union has made digital identity a top priority, especially with the adoption of the EUDI Regulation. The new legislative framework is built on the EU's Digital Decade 2023 policy programme, which emphasises user-centric, interoperable digital identity. More specifically, the EU's Digital Decade policy places digital identity at the core of Europe's digital transformation. Digital identity is seen as essential for enabling access to digital public services and online transactions across the EU, while supporting economic and societal developments. The Declaration on Digital Rights and Principles [29] reinforces this vision by establishing a 'people-centric approach' to digital identity, which building on earlier EU initiatives, such as the Tallin Declaration on eGovernement [30], or the Berlin Declaration on Digital Society and Value-Based Digital Government

[31], highlight that digital identity systems must be secure, interoperable, accessible, and based on open standards, while avoiding vendor lock-in. Citizens should have trust in digital technologies, retain control over their personal data, and be protected from identity theft or misuse.

The insufficiency of the first version of the eIDAS Regulation was recognised in public documents, such as the Evaluation study of Regulation no.910/2014 (eIDAS Regulation) [32] published by the European Commission. This report noted that the eIDAS Regulation had only partially achieved its objective for mutual recognition of eID means because, on the one hand, it did not include an obligation for Member States to notify eID schemes, and, on the other hand, because the acceptance of a notified eID scheme requires that the eIDAS node is in production and the services are connected, which is not always the case.

Beyond the content of this study, digital identity has been facing significant challenges for some time. Specifically, it is a highly fragmented regulatory environment where the applicable regulations and the level of guarantees of digital identities strongly depend on the issuing entity and their intended purpose or context of operation (e.g., public or private services). The lack of guarantees extends to the issuance itself; in many everyday operations involving digital identity, the citizen does not have any guarantee that this digital identity will be provided.

In addition, the predominant models for digital identity, commonly referred to as federated digital identity, were raising problems from the perspective of privacy and cybersecurity. Notably, the surveillance practices enabled by the 'Big Brother' position assumed by the IdP have become a pressing concern that the exercise of the right to privacy, primarily articulated around the protection of individual interests, has not been able to address effectively. Likewise, from the cybersecurity perspective, IdPs usually appear as a single point of failure, becoming the target of cyberattacks. Furthermore, the digitalisation era has been marked by the growing power of digital platforms and technology providers, creating notorious power asymmetries. In the digital identity domain, power asymmetry arises from the limited number of identity solutions available to the user. The novel nature of the situation, combined with the lack of alternatives and the growing need for technology, had resulted in a cautious application of regulations in this sector to date [33].

The EUDI Regulation set the framework for a new digital identity ecosystem within the EU, with the EUDIW playing a central role. The core objective of the EUDI Regulation is to provide all EU citizens with an eID means; at the time, it aims to ensure the provision of a highly secure digital identity solution that grants access to both public and private services and, importantly, enables users to control their personal data and only share the data necessary for the requested service. In line with the last point, the EUDI Regulation overcomes the vision of rigid digital identities towards identity attributes,

offering the user greater flexibility and tools for data protection and management as discussed in the previous chapters.

Consequently, through the EUDIW, the EUDI Regulation introduces a new harmonised eID means, which is also bound to unlock the potential of a whole new digital identity ecosystem. In this regard, as noted before, the Regulation is not limited to setting new legal roles, but it also demands a profound change in the ecosystem, supporting, from a regulatory perspective, a transition that was already occurring in the industry and Academia and commonly referred under the names user-centric digital identity or decentralised digital identity.

In short, it should be recalled that the EUDI Regulation digital identity ecosystem builds upon the following principles:

a. **Publicly guaranteed, user-controlled digital identity**. A fundamental principle of the new digital identity ecosystem is that Member States are required to provide a digital identity wallet. Regardless of the issuance modality adopted, Member States must adhere to the deadlines established by the Regulation. Furthermore, the EUDIW represents a harmonised form of eID, as it transcends a simple wallet application by establishing an electronic identification means through a binding procedure, and this electronic identification means is also subject to a comprehensive set of requirements concerning functionalities offered, privacy, security, and design. Notably, design requirements emphasise the importance of ensuring user control over the digital identity wallet via the EUDIW interface, which includes features such as displaying user interactions with other stakeholders and enabling the exercise of rights. Additionally, the 'authorisation' interface is crucial in reinforcing the control exercised by the EUDIW user.
b. **Accessible digital identity**. In addition to user control and publicly guaranteed digital identity, one of the primary objectives of the European Digital Identity Framework was to ensure accessibility. This commitment to accessibility is reflected in the choice of electronic identification means in the EUDI Regulation, the EUDIW, based on a user-controlled digital application. The design of this digital wallet application must adhere to the EUDI Regulation requirements and to specific regulations, such as the GDPR, including provisions for transparency in data processing and accountability. Furthermore, to enhance accessibility, the EUDIW relies on a set of common protocols and standards to deliver its functionalities and ensure compliance with non-functional requirements.
c. **Privacy and security considerations**. Privacy and security are fundamental to the design of the EUDIW. From a security standpoint, the EUDIW is expected to meet the LoA high requirements set out in Commission Implementing Regulation 2015/1502. Additionally, mutual authentication and security by design are essential requirements.

Regarding privacy, as noted in the previous chapters, standards used for authentication should limit the identity provider's traceability and support unlinkability. Providers of the wallet must also request the strictly necessary data, and when this provider is a private entity, a separate legal entity must be established. Furthermore, as noted, the EUDIW shall incorporate traceability functionalities and enable selective disclosure.

In the case of the European Business Wallet, as established in the Proposal, it should be based on the European Digital Identity Framework, which indicates that its underlying principles shall be adopted where applicable. However, some specific considerations are already being observed.

a. **Automation in business wallets**. While user control is a core principle of the EUDIW, European Business Wallets are also expected to operate without direct human intervention, potentially involving artificial intelligence agents. In this context, user control in relation to business wallets is not conceived in the same way as for natural person wallets. This difference reflects the different objectives underlying the Proposal, which are primarily focused on facilitating business operations rather than individual autonomy, objectives that are also reflected in policy instruments such as the Competitive Compass. Furthermore, the European Business Wallet is conceived as a trust service, making its provision dependent on the market.
b. **Target users and design objectives of business wallets.** Business wallets are not designed for the general population. Accordingly, while transparency and a user-friendly interface remain important, these do not focus on universal accessibility, but the primary objective is to provide a service that is attractive and reliable for business users, who are expected to ultimately pay for these services, conversely to the EUDIW, which must be provided free of charge.
c. **Privacy and security considerations.** As highlighted throughout this deliverable, while privacy requirements remain applicable to European Business Wallets, these requirements are less explicitly articulated in the text of the Proposal. This distinction reflects the fundamentally different use cases enabled by the EUDIW and the European Business Wallet, particularly in contexts where traceability and accountability may legitimately prevail over enhanced privacy features. By contrast, security is a critical issue for European Business Wallets. Risks such as unauthorised access could lead to breaches of confidential business information or facilitate fraud, including scams in interactions with natural person wallets.

Consequently, within WE BUILD, it is essential to consider the overarching principles of the European Digital Identity Wallet framework while tailoring its application to specific scenarios and the respective involvement of the EUDIW or European Business Wallets, in order to ensure that the use cases and testing scenarios ultimately promote the core values underpinning the framework.

Finally, it is important to highlight a last overarching principle of the European Digital Identity Framework: independence from large organisations outside the European Union. Although this was a key factor driving the adoption of the EUDI Regulation, alongside privacy enhancements, it is explicitly stated within the scope of European Business Wallets. Specifically, Article 7 mandates that 'providers of European Business Wallets shall be established in the Union, have their principal place of business and main operations within the Union, and not pose a risk to Union security. In particular, they shall not be subject to control by a third country or a third-country entity'.

5.2 Key guidelines for use case piloting

Piloting activities are characterised by the deployment of certain technologies, processes, and data flows within a controlled environment designed explicitly for testing purposes. While conducting these activities in a controlled setting significantly reduces risks, it is essential to consider certain aspects to further minimise potential risks and maximise the effectiveness of the outcomes. Piloting activities are at the core of WE BUILD, aiming to target the testing of a set of diverse use cases. In the development of these activities, at least the following aspects must be considered:

a. **Involvement of participants.** Typically, pilot activities involve participants who will ultimately be involved in specific processes in which the proposed technologies are tested. The involvement of human participants in these activities always requires their voluntary and informed consent, especially when such participation may entail some form of risk.

   Consequently, during piloting activities, a specific 'Participant Engagement Protocol' should be followed before, during, and after engaging participants, as described in the following figure.

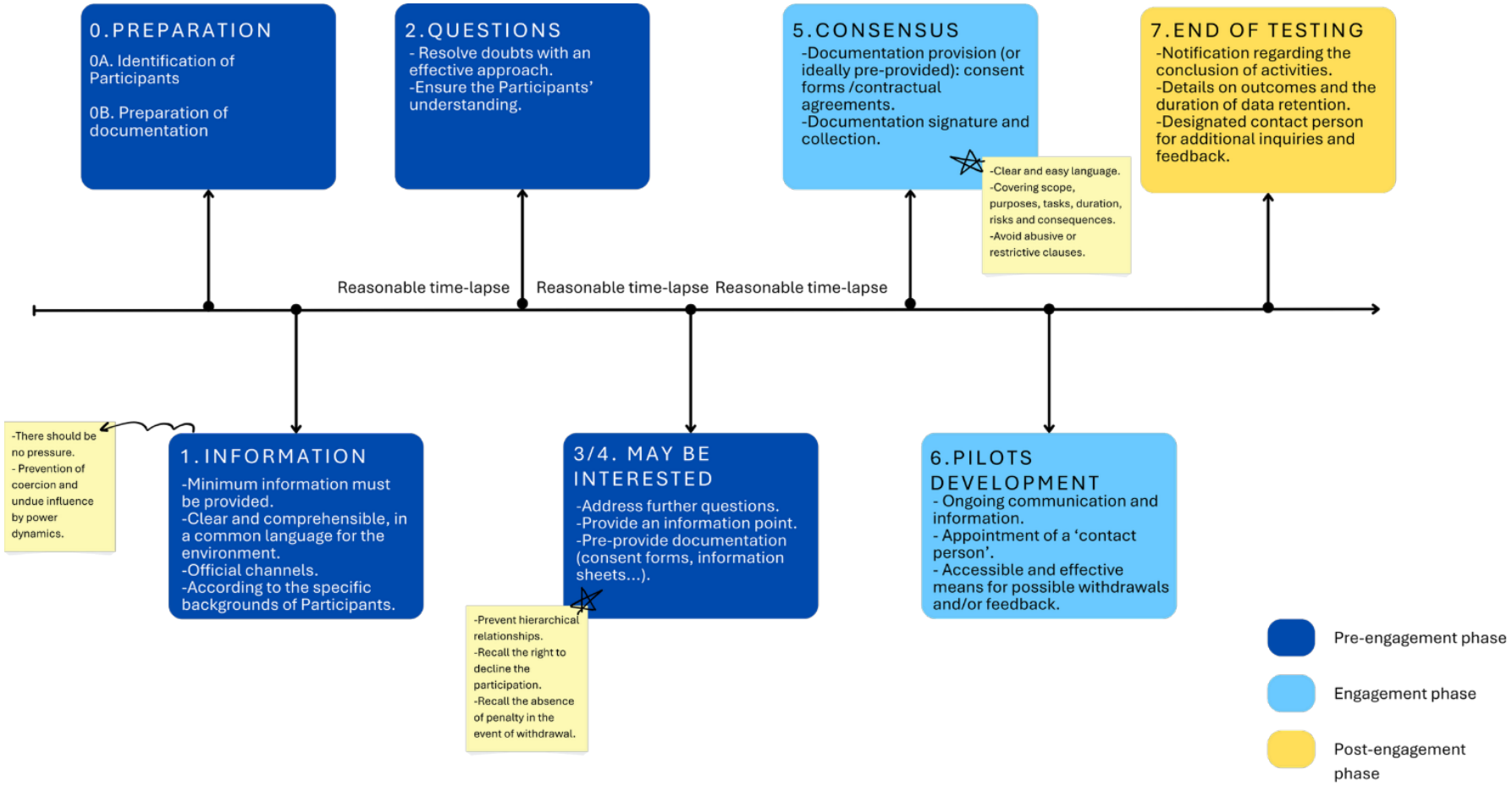

Figure 6. Participant engagement protocol

b. **Processing of personal data.** This aspect has already been discussed as part of Chapter 3. Among the risks associated with piloting activities involving digital identity wallets are issues related to the processing of personal data. As a general rule, the processing of personal data should be avoided when it does not provide for any relevant benefit in the testing activity and the same or equivalent results could be achieved by using synthetic data. Nevertheless, when processing personal data is required, certain steps must be followed to ensure compliance and data protection.

   Allocation of GDPR roles and organisational arrangements. As further detailed in Chapter 3, digital identity wallets operate within complex data processing ecosystems that require clear delimitation of roles and responsibilities among participating partners. It is common to encounter different data controllers handling separate processes, such as credential issuance and reception. Furthermore, multiple legal entities may be involved in a single data processing activity, necessitating formal agreements defining their roles as joint controllers or data controllers and data processors.

   Delimitation of data to be processed and compliance with GDPR principles. When requesting personal data from pilot participants, it is important to adhere to the principle of data minimisation by collecting only the information that is strictly necessary for achieving the pilot's objectives. Additionally, even in a controlled environment with lower risks, appropriate security measures should be implemented to safeguard the data.

   Provision of documentation and support to data subjects. When personal data are processed during a pilot, the entity acting as the data controller must have a valid legal basis for that processing. This legal basis could be consent or another legal basis, such as a contractual obligation. If consent is the legal basis, the data subject must be informed, and their consent obtained. If another legal basis applies, the data subject must still be informed of the processing. Such information should include not only the legal basis but also other essential elements of the processing, such as the types of data involved, data retention and deletion policies, and the rights of data subjects.

   In this regard, the approach proposed *in the* Spanish Data Protection Agency's model for double-layer information (*información de doble capa*) [34] is recommended for consideration. According to this approach, information provided to the data subjects should involve a first layer with a

summarised overview of the key elements of the data processing activities (i.e., responsible entity, purpose, legal basis, rights, and other essential information), potentially in form of a table; and a second layer which should then offer a more detailed overview of the data processing, covering security measures, data storage, adherence to the data minimization principle, and other relevant aspects.

Risk management and consultation. When personal data are involved, there may be circumstances where it is necessary to assess whether a high risk exists. In this regard, Article 35 provides for an obligation to perform a Data Protection Impact Assessment (hereinafter DPIA) when 'taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk for the rights and freedoms of natural persons'. Although digital identity wallets are not a new technology themselves, it is important to consider that the 'party receiving and using' the digital identity wallet might not be familiar with the technology, and therefore, increase the level of risk. The necessity of a DPIA must be assessed for a specific data processing activity or set of activities. Consequently, it will have to be assessed in each specific use case based on, among other elements:

a. The introduction of new technology.
b. The scope and nature of the data processing activity, including level of intrusiveness (e.g., basic administrative processing, automated decision-making…).
c. Type of data involved (e.g., identification data, contact data, professional data, biometric data…)

It should be recalled that when the DPIA concludes the existence of high risk in a data processing activity, pursuing Article 36 of the GDPR, the data controller shall consult the supervisory authority in the absence of measures to mitigate the risk, providing the DPIA results, the respective roles of controllers/ processors, the purposes and means of the processing, the safeguards and security measures and where applicable the contacts of the Data Protection Officer.

In the case of WE BUILD, it cannot be concluded in general that a DPIA is required for all use cases. Although the technology may be new to the parties involved, focusing on business use cases, the nature and scope of the processing, and the type of data involved may not necessarily pose a high risk to individuals' rights and freedoms. Nonetheless, this is an aspect that must be considered by the parties in each specific use case, in accordance with the conditions set out in Article 35 of the GDPR.

c. **Delimited environment.** The testing environment should be specifically designed for testing purposes and distinctly separate from operational environments. Although it can be very close to production for scalability purposes, it should still be possible to differentiate them and, particularly, limit the risks of the participants. Even in a controlled environment, security measures should be implemented proportionally to the assessed level of risk.

When planning, designing and implementing piloting activities, it will be essential to implement the following guiding principles:

a. **Consideration:** what factors were taken into account (e.g., ensuring informed consent, selecting privacy-preserving technologies, allocating GDPR responsibilities).
b. **Balancing:** how these factors were assessed and balanced (e.g., data utility vs. minimisation).
c. **Implementation:** what measures have been or will be put in place (e.g., consent forms and information sheets, security protocols, clear organisational roles).
d. **Monitoring and improvement:** how ongoing compliance and refinement will be ensured (e.g., participant feedback loops).
e. **Demonstration:** how the above steps (A–D) can be evidenced (e.g., documentation).

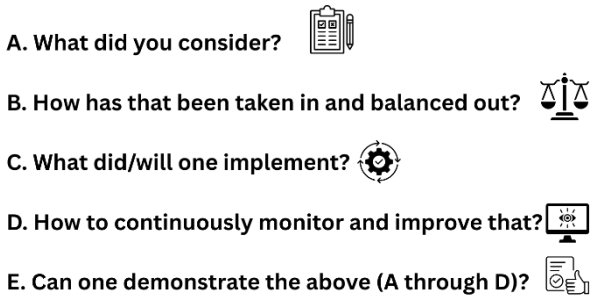

Figure 7. Key questions for pilot design and execution

More specifically, this checklist is provided to assist Consortium partners in designing piloting activities and identifying essential measures.

Risk	Control	Implementation	Responsibility
Genuine participation	For each piloting activity, pilot leader will act as a first point of contact for research participants, including GDPR related matters.	Pilot leader indicates contact details and provides for appropriate means to liaise with all involved partners, especially if personal data are processed.	Pilot leader
Genuine participation	Invitation and selection of research participants should occur among people with understanding of piloting activities, as well as on the basis of free consent.	Special attention should be paid to potential power imbalances that may affect the ability to provide free and informed consent. Depending on the level of risk associated with the piloting activity, participants must have a clear and comprehensive understanding of the activity and its potential implications.	Pilot leader
Genuine participation	Consent to participate is provided (e.g., form, email, acceptance in microsite...).	A detailed consent form is provided explaining the nature of the Project (WE BUILD), the pilot and the different steps that participants are required to complete.	Pilot leader
Legal basis for the processing of personal data	Data controllers should identify a valid legal basis for the processing of personal data during the research activity.	An information sheet, and, when applicable, a consent form, should be provided to research participants, clearly outlining the scope of the activity, its specific objectives, and the related data processing activities.	Partners acting as data controllers for specific data processing activities
Data minimisation	Collection of personal data should be minimal, and when not necessary, synthetic data should be used instead.	Each partner involved in the piloting activity should identify and document the (personal) data to be processed in order to achieve the specific testing and validation objectives. Whenever the use of personal data is not necessary, anonymised or synthetic data should be used instead.	All partners in the pilot, including technical partners
Storage limitation	Retention period of personal data should be minimal, and in any case, no longer than the duration of the research activity.	Piloting activities should ensure the erasure of personal data immediately after processing. In certain cases, an additional short retention period may be required; however, this period should remain strictly limited in duration and justified by the specific purposes of the pilot.	All partners participating in the pilot

Confidentiality	Adequate technical and organisation measures should be in place to avoid or mitigate any data breach.	Personnel involved in data processing activities should be clearly identified in advance, and partners must implement appropriate security measures where applicable (e.g., commercial-grade encryption, access control mechanisms, etc.).	All partners participating In the pilot, but specially technical partners
Transfer of personal data to non-EAA countries	Although, given the scope of the project, data transfers should in principle be avoided, any transfer of data that becomes necessary must be covered by an applicable adequacy decision.	In principle, data transfers should be avoided within the scope of the WE BUILD pilots. However, if such transfers are strictly necessary, they must rely on a valid legal basis and be covered by an applicable adequacy decision, and SCCs should be exceptionally considered.	Partner concerned with the data transfer
Data breach response	In case of a data breach an adequate response plan should be in place.	In the event of a data breach, each partner shall inform the others immediately upon discovery. If necessary, a designated partner will be responsible for contacting the relevant data protection authority and conducting a risk assessment.	Each partner involved in the piloting activity, but especially the pilot leader.
Data processors	The different roles within the piloting activities should be documented, and where necessary a data processing agreement should be concluded.	A data processing agreement should be established and signed whenever two or more legal entities are involved in the same data processing activity and assume controller–processor roles.	Partners assuming data controller and processor roles in the same data processing activities.
Identification and management of risk	When it is determined that a piloting activity presents a high level of risk, as Data Protection Impact Assessment (DPIA) should be prepared.	Prior to the piloting activity, the Data Protection Impact Assessment (DPIA) should identify the different data processing, associated risks, and if necessary, risk mitigation measures.	Partner acting as data controller where a high risk is identified.
Prior consultation	When a Data Protection Impact Assessment (DPIA) concludes the existence of high level of risk without adequate risk mitigation measures, the corresponding supervisory authority shall be consulted prior to the processing.	Prior to the piloting activity, the data controller shall provide the supervisory authority with the results of the Data Protection Impact Assessment (DPIA) the respective roles of controllers/ processors, the purposes and means of the processing, the safeguards and security measures and where applicable the contacts of the Data Protection Officer.	Partner acting as data controller where a high risk is identified.

Table 2. Control measures in the design and deployment of testing environments

6. Conclusions

WE BUILD is part of the second round of LSPs, where use cases build upon the work conducted in previous LSPs. However, it also has its own features, particularly a focus on business wallets and use cases involving legal entities, rather than on digital identity wallets for citizens or consumers to access services. Nevertheless, although WE BUILD places a strong focus on business wallets, the separation is not absolute. This is because, even if the legal entity is designated as the owner of the business wallet, its operation still depends on a natural person, namely an authorised representative. Furthermore, it is reasonable to expect that natural persons will interact with business wallets in certain scenarios, especially since, as established in the Proposal, the European Business Wallet replaces the provisions related to legal entities' digital identity wallets in the EUDI Regulation.

Activities within the scope of WE BUILD are characterised by their specific focus on testing and research objectives. As a result, the applicable legal requirements are more limited. However, from both regulatory and ethical perspectives, two key aspects must be addressed: (a) the involvement of human participants, and (b) the processing of personal data. In this context, particular safeguards must be implemented to address the unique features of digital identity wallets, taking into account the various processes and data processing activities that may ultimately serve the same goal, carrying out testing activities within WE BUILD. These data processing activities will be detailed during the pilot design phase, and partners are encouraged to seek guidance from the Ethics Mentor and relevant legal partners under *T1.4-Legal and Ethical Aspects* to clarify the implementation of the proposed guidelines when necessary, as each use case is likely to have its own distinct characteristics.

In this context, it is necessary to consider potential scenarios involving the disclosure of personal data by legal representatives and to recognise that, while privacy-enhancing technologies such as selective disclosure or pseudonymisation are central to the EUDI framework, they may not always be sufficient in European Business Wallet use cases to meet applicable legal obligations. Accordingly, one of the objectives of the WE BUILD activities is to identify the circumstances in which such techniques can be effectively applied while preserving legal certainty, for example, by enabling proof of valid authorisation of a legal representative. This assessment is of particular importance given that business wallets are designed to operate in cross-border and even third-country interaction scenarios.

Overall, WE BUILD will need to operate within a dynamic regulatory framework that may evolve during the course of the Project. This will necessitate ongoing monitoring of the Proposal and any subsequent amendments. Currently, the primary recommendation is to incorporate core elements or overarching principles, such as treating the business wallet as a trust service and ensuring compliance with relevant requirements and

governance framework. Additionally, it is important to focus on core functionalities, including demonstrating the authority of legal representatives, establishing a chain of trust through attestation or shared electronic documents, different from EAAs, and managing the interactions between these processes.

Ultimately, WE BUILD use cases will be based on scenarios where essential values, principles, and legal obligations remain applicable; however, there will also be a degree of regulatory experimentation, which could provide valuable feedback for refining the regulatory proposal and its implementation.

References

[1] Proposal for a Regulation of the European Parliament and of the Council on the Establishment of European Business Wallets. https://eur-lex.europa.eu/resource.html?uri=cellar:bfd78780-c5de-11f0-8da2-01aa75ed71a1.0001.02/DOC_1&format=PDF

[2] 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). *Official Journal of the European Union* , *L 119/1*. http://data.europa.eu/eli/reg/2016/679/oj

[3] 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. *Official Journal of the European Union* . *http://data.europa.eu/eli/reg/2024/1183/oj*

[4] Proposal for a Regulation of the European Parliament and of the Council amending regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as regards the simplification of the digital legislative framework, and repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus). https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

[5] Article 29 Working Party. (2014). *Opinion 05/2014 on Anonymization Techniques*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[6] European Commission. *White Paper on Artificial Intelligence: a European approach to excellence and trust*. https://commission.europa.eu/system/files/2020-02/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[7] Article 29 Working Party. (2012). *Opinion 3/2012 on developments in biometric technologies*. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

[8] Agencia Española de Protección de Datos. *Respuesta consulta N/REF:0036/2020*. https://www.aepd.es/documento/2020-0036.pdf

[9] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). *Official Journal of the European Union*. http://data.europa.eu/eli/reg/2023/2854/oj

[10] 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). *Official Journal of the European Union*. http://data.europa.eu/eli/reg/2023/2854/oj

[11] Proposal for a Regulation of the European Parliament and of the Council on a framework for Financial Data Access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0360

[12] Proposal for a Directive of the European Parliament and of the Council on payment services and electronic money services in the Internal Market, amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0366

[13] Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52023PC0367

[14] Regulation (EU) 2020/1056 of the European Parliament and of the Council of 15 July 2020 on electronic freight transport information. *Official Journal of the European Union*. http://data.europa.eu/eli/reg/2020/1056/oj

[15] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). *Official Journal of the European Union*. L 333/80. http://data.europa.eu/eli/dir/2022/2555/oj

[16] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881

[17] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). *Official Journal of the European Union*. http://data.europa.eu/eli/reg/2024/2847/oj

[18] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014

and (EU) 2016/1011. *Official Journal of the European Union*. http://data.europa.eu/eli/reg/2022/2554/oj

[19] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). *Official Journal of the European Union*. http://data.europa.eu/eli/reg/2024/1689/oj

[20] Directive (EU) 2025/25 of the European Parliament and of the Council of 19 December 2024 amending Directives 2009/102/EC and (EU) 2017/1132 as regards further expanding and upgrading the use of digital tools and processes in company law. *Official Journal of the European Union*. http://data.europa.eu/eli/dir/2025/25/oj

[21] Timón López, C. & Skarmeta, A. (2022). Allocating controllership in the European Digital Identity Wallet. CyberSecurity4Europe. https://cybersec4europe.eu/wp-content/uploads/2023/02/wallet.pdf

[22] Chen J., Edwards L., Urquhart L., & McAuley D. (2020). Who is responsible for data processing in smart homes? Reconsidering joint controllership and the household exemption, *International Data Privacy Law*, *10* (4), 279-293. https://doi.org/10.1093/idpl/ipaa011

[23] ECJ. Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV, July 29th 2019. ECLI:EU:C:2019:629

[24] ECJ. Jehovan todistajat, July 10th 2018. ECLI:EU:C:2018:551

[25] Commission Implementing Regulation (EU) 2024/2979 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the integrity and core functionalities of European Digital Identity Wallets. *Official Journal of the European Union*. https://eur-lex.europa.eu/eli/reg_impl/2024/2979/oj/eng

[26] Commission Implementing Regulation (EU) 2025/1569 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards qualified electronic attestations of attributes and electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source. *Official Journal of the European Union*. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202501569

[27] ETSI. (2026). ETSI TS 119 478 Electronic Signatures and Trust Infrastructures (ESI); Specification of interfaces related to Authentic Sources. https://www.etsi.org/deliver/etsi_ts/119400_119499/119478/01.01.01_60/ts_119478v010101p.pdf

[28] Commission Implementing Regulation (EU) 2015/1502 of 8 September 2015 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. *Official Journal of the European Union, L 235/7*. http://data.europa.eu/eli/reg_impl/2015/1502/oj

[29] European Parliament, Council & European Commission. (2022). European Declaration on Digital Rights and Principles for the Digital Decade. https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

[30]EU2017.55. *Tallinn Declaration on eGovernment*. https://digital-strategy.ec.europa.eu/en/news/ministerial-declaration-egovernment-tallinn-declaration

[31] EU2020. DE. Berlin Declaration on Digital Society and Value-Based Digital Government. https://ec.europa.eu/isa2/sites/isa/files/cdr_20201207_eu2020_berlin_declaration_on_digital_society_and_value-based_digital_government_.pdf

[32] Ceccanti, C., di Legge, A., Eichholtzer, M., Kuhl, A., McNally, P., Ongono Pomme, A., Van der Peljl, S. & Walsh, C. (2021). *Evaluation study of the Regulation no.910/2014 (eIDAS Regulation): final report*. European Commission. https://digital-strategy.ec.europa.eu/en/library/evaluation-study-regulation-no9102014-eidas-regulation

[33] Timón López, M.C. (2024). The eIDAS2 Regulation: the European Union's Strategic Vision to Regulate a Digital Identity Metasystem under Citizens' Control as a Public Service [PhD Thesis, University of Murcia]. [PhD Thesis, University of Murcia]. https://portalinvestigacion.um.es/documentos/666351d8b2c1d52ac040f585?lang=en

[34] Agencia Española de Protección de Datos. (2017). *Guía para el cumplimiento del deber de informar*. https://www.aepd.es/sites/default/files/2025-12/guia-modelo-clausula-informativa-en-revision.pdf

Annex - Preliminary observations on the Proposal for a Regulation establishing European Business Wallets

Although the Proposal for a Regulation on the establishment of European Business Wallets generally presents a consistent approach aimed at its intended purposes, some aspects raise legal questions. The following section includes a set of initial considerations regarding the regulatory proposal. These reflections are tentative and offered for discussion purposes; they do not claim to be definitive or necessarily accurate but rather aim to identify potential interpretative issues that may merit clarification.

a. The Proposal seems to refer to the **European Business Wallet provider as a trust service (or at least somehow equivalent**, and this idea was shared during the presentation of the Proposal), subject to the requirements established in Article 7 of the Proposal, which provides for compliance with trust service requirements pursuant to the eIDAS Regulation. In principle, it is understood that a European Business Wallet provider may operate either as a qualified or a non-qualified trust service provider. However, the European Business Wallet provider is not defined in the definitions set out in Article 3 (in contrast to the provider of European Business Wallet identification data). Furthermore, it is important to note that, where the Proposal refers to trust services, it does so by reference to the eIDAS Regulation, which contains an exhaustive list of trust services. Therefore, it might be worth clarifying which specific roles are considered a trust service.

b. In principle, if the European Business Wallet provider is considered a trust service provider, it would fall within the **scope of application of the NIS2 Directive**. However, the proposal explicitly states that the European Business Wallet provider is subject to the NIS2 Directive, which creates confusion. On the one hand, as noted above, it is not explicitly established that the European Business Wallet provider qualifies as a trust service. On the other hand, this explicit provision appears redundant. That said, such an explicit clarification could have been more meaningful in the case of European Digital Identity Wallet providers, since, even though the entities providing those wallets will, in most cases, be subject to the NIS2 requirements, there is no complete or automatic overlap in all cases. These aspects are, however, considered in the new cybersecurity package published in January 2026, including amendments to the Cybersecurity Act.

c. Article 4 introduces the **principle of equivalence**, extending it to any actions resulting from the use of the European Business Wallet, specifically with respect to its core functionalities as described in Article 5 paragraph 1. This approach, to a certain extent, appears to confer legal effects traditionally associated with trust services, but does so across a broader range of functionalities, which in some

cases may require further definition to determine in relation to which specific processes this equivalent legal effect is conferred.

d. Article 15 establishes a framework for the governance and supervision of **Union entities** (as defined in Article 3 of the Proposal) **that may act as providers of European Business Wallets**. This appears to imply that such Union entities may themselves provide the wallet, which in turn raises the question of whether they must be qualified as trust service providers or, alternatively, whether they should be regarded as public sector bodies and this qualification is not required (e.g., provision of EAAs by public sector entities). While this distinction is explicitly addressed with respect to European Business Wallet owner identification data, where the Proposal clearly allows the provider to be a qualified trust service provider, a public sector body, or even the Commission, it remains unclear whether the same approach applies to European Business Wallet providers as such. This uncertainty is further compounded by the fact that, following the logic of the eIDAS Regulation, the roles of identification data provider and wallet provider may be different and fulfilled by different entities.

e. The European Business Wallet is understood as a trust service, and the Regulation appears to **focus on economic operators**. However, it would be reasonable to expect that public sector bodies may also need to communicate or interact using similar mechanisms. This raises the question of whether the European Business Wallet is intended to target exclusively private-sector businesses, or whether it may also extend to other legal entities, such as public sector bodies, potentially through the use of a legal entity wallet. Under the EUDI framework, this issue was more clearly addressed, as the concept of a 'legal entity wallet' was sufficiently broad to encompass both private and public actors. By contrast, the current Proposal explicitly refers to a 'European Business Wallet', suggesting that legal entities that are not economic operators fall outside its intended scope.

f. As regards the possible **recognition of third-country wallets**, the Proposal refers to the trust framework established under the eIDAS Regulation. In principle, however, the relevant implementing acts appear to refer only to the European Business Wallet. This approach is consistent with the existing provisions of the EUDI Regulation, which already envisage such possible third-country recognition in relation to trust services. In this case, however, the provision specifically addresses European Business Wallets while simultaneously referring back to the eIDAS trust framework. Therefore, if the European Business Wallet is regarded as a trust service in its own right, this dual reference would arguably render the provision redundant.

g. The proposal for **the European Business Wallet Regulation does not lay down specific privacy requirements** of its own but instead refers to those already set

out in the eIDAS Regulation. As a result, the proposal does not, in principle, prohibit the use of privacy-enhancing mechanisms; rather, their applicability will depend on the specific use case. However, this approach may give rise to some uncertainty. In particular, the Annex, when referring to the requirements applicable to European Business Wallets, seems to point out, in some cases, to the implementing acts based on the requirements of the European Digital Identity Wallet (e.g., presentation of attributes to relying parties). At the same time, Article 5 provides that the Commission will adopt additional implementing acts setting out requirements specifically for European Business Wallets. It therefore remains unclear which set of requirements will apply in practice, especially in light of the fact that, in certain business-wallet use cases, traceability may constitute a legal requirement.

h. With regard to the **onboarding of the European Business Wallet**, it is envisaged that this process will take place through an authorised representative. In particular, the Proposal establishes that the onboarding must meet the requirements laid down in the Commission Implementing Regulation 2015/1502 for levels of assurance 'substantial' or 'high'. At this stage, there is therefore a clear interaction between the legal regime governing electronic identification and that governing trust services.