



EUROPEAN  
COMMISSION

Brussels, 19.11.2025  
COM(2025) 838 final

2025/0358 (COD)

Proposal for a  
**REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**  
**on the establishment of European Business Wallets**

{SWD(2025) 837 final}

## **EXPLANATORY MEMORANDUM**

### **1. CONTEXT OF THE PROPOSAL**

#### **• Reasons for and objectives of the proposal**

This explanatory memorandum accompanies the proposal for a Regulation on the establishment of European Business Wallets. The legal instrument aims to provide a harmonised, trusted, and user-friendly digital framework for economic operators and public sector bodies to securely identify, authenticate and exchange data with full legal effect across EU borders.

Recent technological and societal developments require a new harmonised and digital approach to business-to-government and business-to-business interactions. AI, cloud computing and secure digital identity are moving at an unprecedented pace, affecting the way of doing business in Europe: processes have shifted from being document-based to automated and data-driven. For instance, 91% of scaleups consider digital technologies critical to their growth. These developments, combined with the EU's strategic priorities for competitiveness, digital sovereignty, simplification and digital-by-default public services, create the need for agile solutions that can support trusted cross-border business transactions at scale.

The Draghi and Letta reports have warned that persistence of administrative burdens, and fragmentation of the Single Market significantly weaken Europe's competitiveness, discourage EU firms from scaling up, and increase dependence on high-risk providers. Yet the digital infrastructure available to public sector bodies and economic operators remains fragmented and, compliance and reporting obligations complex: most stakeholders consulted, highlighted the lack of cross-border interoperability as a major source for red tape. Across the Union, public authorities still operate within heterogeneous digital environments that limit the full realisation of cross-border public services: the eGovernment Benchmark 2024 shows that while 88 % of public services are available online to national users, cross-border users can access only 56 % of those services digitally and interoperability barriers remain among the top obstacles to efficient e-government. For economic operators active in multiple Member States ensuring smooth transaction, such as tax registration, licensing or procurement applications, is key to remain competitive.

The practical consequences of the *status quo* are burdensome. Stakeholders reported for example, employing two full-time staff solely for sustainability reporting obligations, or incurring costs exceeding €100,000 for specialised consultancy in this area. Also, economic operators estimate that around 20% of staff time is absorbed by compliance-related activities. In cross-border contexts, this often requires manual or paper-based verification that delay transactions and multiply administrative costs. These costs are disproportionate especially for SMEs, where compliance obligations divert significant resources from strategic high-value activities: the European Investment Bank estimates that regulatory compliance consumes 1.8% of turnover for firms overall and 2.5% for smaller companies. Know-Your-Customer procedures in the financial sector alone can take 30 to 50 days per corporate client, with each dossier requiring dozens of hours of manual processing.

For public sector bodies, structural barriers prevent the full transition to modern, digital, and accessible services and the creation of a seamless EU administrative space. Although the digitalisation of public services is showing signs of increased maturity, it will not, at current rates, reach the target set in the Europe's Digital Decade Report of having 100% of public services online by 2030. This scenario limits scalability, raises administrative costs, and slows

down service delivery. Digitising interactions means more efficient administrative procedures, better service delivery and opportunities for requalification of public resources to more strategic tasks. Evidence shows that digitalisation in the public sector can make administrations more effective, either by expanding services without additional budget or by redeploying human resources towards higher-value activities.

The absence of a trusted, standardised channel for business-to-government and business-to-business interaction allowing to exchange attributes undermines traceability and security. Credentials are often shared via email or proprietary portals, which offer limited guarantees of authenticity, increasing exposure to fraudulent practices, such as invoice scams, which already generate over €26 million annually in illicit profits, according to Europol and EUIPO. Thus, while privacy and minimal disclosure are essential for natural persons, businesses require transparency and traceability of exchanges to support risk management, compliance and fraud prevention. The EU has already achieved a major milestone in its simplification agenda with the European Digital Identity Framework - a state-of-the-art, privacy-friendly and interoperable system for digital identification empowering citizens and legal entities to share data securely across borders. The European Business Wallets proposal aims at complementing the European Digital Identity Wallets by introducing a market-driven digital tool designed for the specific needs of business transactions.

The current drive for simplification and digitalisation is anchored in the Union's political agenda. The EU's Strategic Agenda 2024–2029, the European Council conclusions<sup>[50]</sup> and the Commission's Competitiveness Compass all underline the urgency of reducing administrative burdens, with explicit targets of a 25% reduction in overall burdens and 35% for SMEs. The Draghi and Letta reports identify fragmentation and administrative complexity as major obstacles to Europe's competitiveness, while President von der Leyen's 2025 State of the Union made clear that internal barriers continue to hinder economic operators more than external ones. In March and June 2025, the European Council reaffirmed the need for "simplicity by design," and in early 2025 the Commission explicitly identified the establishment of European Business Wallets as a cornerstone of a simpler and faster Europe.

Against this economic and political background, the European Business Wallets proposal delivers on the simplification demand by achieving the following specific objectives:

- Reduce administrative burdens, streamline compliance processes, and improve service delivery
- Ensure economic operators and public sector bodies have access to secure and trusted digital identification across borders, meeting user needs and demand
- **Consistency with existing policy provisions in the policy area**

The European Business Wallets proposal builds on and extends the ecosystem established under the European Digital Identity Framework (EUDI) - Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market, as amended by Regulation (EU) 2024/1183. The European Business Wallets aim to complement the EUDI Framework by offering functionalities tailored to the needs of public sector bodies and economic operators, including the digital management of representation rights and mandates, and a secure channel for exchanging official documents and attestations supported by a common directory. Full interoperability with the European Digital Identity Wallets will be guaranteed.

The proposal is complementary to the EU company law acquis and uses the existing European Unique Identifier which all limited liability companies and commercial partnerships (as well as the future 28th regime companies) have in accordance with EU company law. In addition, the proposal is compatible with the Business Registers Interconnection System (BRIS), developed in accordance with the codified Company Law Directive (EU) 2017/1132. Finally, the proposal is also in line with Beneficial Ownership Registers Interconnection System (BORIS), developed in accordance with the Anti-Money Laundering Directive (EU) 2015/849. These interconnections use the European Unique Identifier (EUID) to uniquely identify companies and other legal entities, and legal arrangements in the EU, but do not cover all economic operators or public sector bodies, such as sole traders, self-employed or public institutions. The European Business Wallets extend this ecosystem by offering a trusted and interoperable mean for all these entities.

- **Consistency with other Union policies**

This proposal is embedded in the Union's wider policy agenda to boost competitiveness, reduce administrative burdens and deliver a digitally integrated Single Market. It contributes directly to the goals set out in the Commission's Single Market Strategy which calls for more effective digitalisation in the EU to enable the optimal functioning of the Single Market as well as to the EU Strategic Agenda 2024–2029, the Competitiveness Compass, the SME Strategy for a sustainable and digital Europe, and the Digital Decade Policy Programme. All of which highlight the need for simplification, interoperability and digital-by-default public services. The European Business Wallets proposal deliver on these strategic priorities by offering a concrete instrument to make compliance and cross-border interactions simpler, faster and more reliable for economic operators and public sector bodies.

Furthermore, the proposal ensures complementarity with key legislative initiatives as follows:

- The Single Digital Gateway (SDG) and its Once-Only Technical System (OOTS) implement the “once-only” principle, requiring authorities to reuse data already held in another Member State without repeated submissions by businesses. The European Business Wallets proposal will complement the SDG and OOTS by providing trusted identification and authentication of economic operators and public administrations and a secure exchange layer that enables businesses and public sector bodies to share and reuse verified data and official attestations seamlessly across borders.
- The Digital Product Passport (DPP), central to the EU's circular economy agenda, depends on trusted access to conformity and sustainability data. The Business Wallets proposal can prove legal identity and any granted access rights, allow conformity declarations to be signed and sealed, and ensure product data is exchanged securely and verifiably across borders.
- The Interoperable Europe Act (IEA) establishes the framework for cross-border interoperability of public services. The Business Wallets proposal will complement this by serving as a trusted infrastructure that administrations can integrate into digital-by-default service delivery, reinforcing the removal of technical and organisational barriers.
- The upcoming proposal on the 28th Regime corporate legal framework will provide simple, flexible and fast procedures for companies to set up and operate and attract investment in the EU through digital solutions. It will ensure that digital tools such as the EU Company certificate and the EU digital Power of Attorney can be used in the European Business Wallets.

- The VAT in the Digital Age (ViDA) package modernises VAT reporting, introduces mandatory e-invoicing across borders and strengthens fraud prevention. The Business Wallets proposal will enable secure storage and verifiable exchange of VAT attestations and transaction data, thereby supporting real-time reporting and trusted invoicing.

## **2. LEGAL BASIS, SUBSIDIARITY AND PROPORTIONALITY**

### **• Legal basis**

The legal basis for the proposal is Article 114 of the Treaty on the Functioning of the European Union (TFEU), which provides for the adoption of measures at EU level to ensure the proper functioning of the internal market. Secure identification, trust services, and seamless exchange of verifiable electronic attestations are essential for economic operators and public sector bodies to participate effectively in the Single Market.

The functioning of the internal market relies on uniform and consistent rules applied across all relevant public sectors bodies performing equivalent functions or providing comparable services. European Union institutions, agencies, offices and bodies (Union entities) often carry out similar activities to national public sector bodies and have key supervisory and regulatory roles. Thus, their involvement in supporting the proper functioning of the Single Market is necessary. Excluding them would create regulatory gaps, fragmentation and uneven application of the rules, thereby undermining the Business Wallet's objective of safeguarding the integrity, stability and resilience of the internal market. In addition, simplification remains a key driver of the EU's commitment to building a bolder, simpler, and faster Union. A competitive and well-functioning Single Market requires active participation from both national and EU-level authorities, with the latter leading by example. Accordingly, Union entities should adopt and use the European Business Wallet, extending simplification and efficiency to their interactions with economic operators.

The current disparities in the way Member States identify economic operators, verify mandates and exchange official data and documentation in digital form may pose risks of obstacles to fundamental freedoms or cause significant distortions of competition. By providing a harmonised solution for secure business identification and data exchange, the European Business Wallets proposal aim to remove administrative barriers, prevent further divergences, and ensure that all economic operators can compete on a level playing field within the EU.

### **• Subsidiarity (for non-exclusive competence)**

Economic operators and public sector bodies across the Union should be able to rely on highly secure and trustworthy digital identity solutions, including the portability of electronic attestations of attributes that can be used across the Single Market in a user-friendly and efficient manner. These needs cannot be sufficiently met by Member States acting individually, as national solutions remain fragmented in scope, effect and technical design.

Hence, action at EU level is necessary to ensure that all public authorities, both national and European, recognise and apply the same interoperable solutions when interacting with economic operators. This guarantees a coherent regulatory environment and avoids parallel procedures or incompatible systems that would be contrary to the objectives of simplification and optimal functioning of the internal market. Obstacles to the freedom of establishment and

the freedom to provide services arise because credentials issued digitally in one Member State cannot always be reused or relied upon in another.

In addition, distortions of competition occur when operators face unequal conditions depending only on their place of establishment. In Member States where procedures are fully digitalised, companies can register for VAT or provide attestations within days at low cost, while in less digitalised domestic environments, the same process may require courier services, or lengthy manual checks, taking weeks and diverting staff from productive activities. The eGovernment Benchmark 2024 reveals substantial differences across Member States in the digital availability and usability of key public services: the average overall score of the 10 top-performers within the EU27 is 87 points, compared to 64 points for the 10 bottom-performers - a gap that highlights persistent disparities in the digitalisation of EU public services. These disparities translate into different compliance costs of digitalisation disproportionately harm SMEs and micro-enterprises, weakening their ability to compete in the Single Market and limiting their participation in economic opportunities such as public procurement.

EU-level intervention is the most efficient way to restore a level playing field: a common, harmonised framework ensures that all economic operators, regardless of size or location, can rely on a single tool to interact with public authorities and partners across the Union. By removing administrative barriers and creating uniform conditions, the European Business Wallets proposal strengthens legal certainty, trust and competitiveness.

Regarding added value, the European Business Wallets will eliminate duplication and lower compliance costs, enhance data quality and transparency, and provide public sector bodies with more reliable information, thereby improving service delivery. For economic operators, particularly SMEs, this means that the time and resources saved can be redirected to innovation, growth and international expansion. At the same time, EU-level harmonisation prevents dependency on high-risk providers, strengthens the resilience of critical infrastructures, and consolidates the Union's digital sovereignty. Beyond the internal market, the initiative can also enhance the Union's role as a global standard-setter for trusted digital infrastructures, supporting European competitiveness in international trade.

- **Proportionality**

This initiative is proportionate to the objectives sought, as it limits obligations to what is strictly necessary to ensure a secure, harmonised and interoperable framework for digital interactions between economic operators and public sector bodies. The European Business Wallets do not prescribe a single rigid business model or technical design but rather set a framework that combines interoperability with flexibility, fostering competition and innovation.

Furthermore, obligations for public sector bodies are balanced by transitional arrangements: flexible implementation periods allow public sector bodies sufficient time to adapt their administrative and IT systems and preventing disruption. The proposal does not create new administrative procedures that must be completed by economic operators or public sector bodies. It instead provides a common, trusted channel for fulfilling obligations that already exist under Union law. Being sector-agnostic in nature, the initiative does not touch upon the content of current obligations and simply provides a mean to simplify compliance with European and national existing rules, while helping overcoming fragmentation and treatment disparities across the Single Market.



The costs of adoption and maintenance will be sustained by economic operators and public sector bodies. In particular these relate to onboarding, training and IT adaptation. However, these costs are outweighed by efficiency gains from simplified processes, reduced duplication, and greater legal certainty. Moreover, training costs, that constitute the most substantial one-off costs, could be partly supported by existing Union initiatives for digital transformation and capacity-building, which can help alleviate training and adaptation costs.

The proposal is also proportionate in terms of its expected impact on economic operators. It also uses the existing European Unique Identifier (EUID) which avoids extra costs for 18 million companies. SMEs and micro-enterprises, which face the greatest relative burden from administrative complexity in terms of both costs and staff time, are expected to benefit the most from the simplification and efficiency gains deriving from the use of European Business Wallets. This is fully consistent with the EU's political priorities, including the EU Start-up and Scale-up Strategy, the upcoming 28<sup>th</sup> regime and the recommendations of the Draghi Report, which emphasise the need to reduce red tape and administrative barriers as a prerequisite for SMEs competitiveness and growth.

Notably, the proposal does not impose any obligation on economic operators. It requires public sector bodies to enable the use of European Business Wallets for specified functionalities, ensuring that economic operators like small and medium enterprises have the choice to adopt the Business Wallets and to benefit from simplified procedures. This approach aligns with the "Think Small First" principle by avoiding unnecessary regulatory pressure on SMEs. Self-employed individuals and sole traders may also rely on their European Digital Identity Wallets to access trust services offered for the European Business Wallets, including the secure communication channel or e-signatures, without the need to acquire a fully-fledged Business Wallet. This ensures proportionate treatment of smaller operators by preventing the imposition of an undue burden.

Finally, the initiative is also proportionate in its regulatory design, as it relies on ex post supervision by the specified supervisory bodies and a notification procedure rather than prior authorisation. This approach ensures effective oversight and accountability of providers without introducing unnecessary administrative delays or costs, while maintaining a high level of trust and security.

Taken together, these elements show that the proposal respects the principle of proportionality. By combining a clear common framework with flexibility for innovation, it delivers in the most efficient way on addressing pressing needs of both economic operators and public sector bodies.

- **Choice of the instrument**

The choice of a regulation as the legal instrument is justified by the need to ensure a uniform framework of application for the secure identification, authentication and the exchange of attestations by economic operators and public sector bodies across the Single Market. Only directly applicable rules can guarantee that the European Business Wallets operate seamlessly throughout the Single Market and that their legal effects are recognised and applied equally in all Member States, which is essential to safeguard the fundamental freedoms of establishment and the provision of services, currently weakened by divergent national solutions and fragmented procedures.

The direct applicability of a regulation, in accordance with Article 288 TFEU, will prevent further legal fragmentation and ensure that economic operators and public sector bodies can rely on a common instrument with the same legal certainty across the Union.

In addition, in order to guarantee the consistent application of all related instruments and taking into consideration that the EUDI Framework is itself established by a Regulation, the present proposal should likewise take the same legal form.

### **3. RESULTS OF EX-POST EVALUATIONS, STAKEHOLDER CONSULTATIONS AND IMPACT ASSESSMENTS**

#### **• Stakeholder consultations**

Targeted consultations were undertaken specifically for the European Business Wallets, reflecting their distinct focus on B2G and B2B interactions. A Call for Evidence ran between May and June 2025 and received nearly one hundred contributions from companies, business associations, registries, public authorities and citizens across 17 Member States and several third countries. The Commission also carried out surveys, in-depth interviews and a series of dedicated workshops with Member States, registries, SMEs, industry representatives and trust service providers. The feedback was complemented by input from conferences and ad hoc dialogues with stakeholders throughout 2025.

The consultation strategy focused on specific issues relevant to economic operators and public sector bodies, including operational requirements, technical integrations, workflow optimisations, and integration of reporting obligations, tailored to capture the technical and practical realities faced by professional users.

Stakeholders highlighted that existing digital tools and channels for administrative activities are highly fragmented, particularly for cross-border exchanges, leading to repetitive data submissions and administrative burdens. Several administrative activities were described as burdensome, particularly those involving document exchange, compliance, and verification across Member States. These activities are often time-consuming, repetitive, and prone to human error.

Respondents anticipated that the European Business Wallets could significantly reduce the cost and complexity of administrative tasks. Benefits cited included faster services, improved data accuracy, and enhanced cross-border operations. Many stakeholders expressed openness to adopting a cloud-based solution like the European Business Wallets, especially if it streamlines processes and reduces costs. However, concerns were raised about integration challenges and the need for clear guidance and support. In addition, stakeholders identified various use cases and cost-saving opportunities, including automating identity verification, streamlining compliance processes, and enabling secure cross-border transactions. The potential benefits were quantified in terms of time saved on administrative tasks and the reduction of manual processes.

The consultation results highlighted the need for a harmonised approach to business identity, representation, and regulatory compliance. Recommendations included the need for technological neutrality, ensuring the Wallets are technologically neutral, flexible, and future proof, relying on harmonised standards and protocols. Interoperability is crucial, with the Wallets integrated with existing frameworks, such as the EU Digital Identity Wallet, to ensure seamless cross-border operations. The Wallets should be based on sustainable, market-driven models, with clear guidelines and support for adoption. Special attention should be given to



SMEs, considering their challenges in adopting digital tools and the need for clear, actionable use cases.

The stakeholder consultation strategy provided valuable insights into the needs, challenges, and expectations of economic operators and public sector bodies regarding the European Business Wallets. The findings informed the development of the regulation, ensuring that it addresses the specific needs of professional users by: being technological neutral and future-proof; enabling the secure retrieval of data from business registries and other authentic sources, guaranteeing traceable interaction; allowing for a market-driven model and finally, making the acceptance of the Business Wallets mandatory for public sector bodies to ensure consistent and effective uptake across the EU.

The initiative also builds on the extensive public consultation carried out in 2021 in the context of the revision of the eIDAS Regulation, which gathered broad feedback on digital identity and trust services. The results of that consultation remain valid for understanding user expectations regarding interoperability, legal certainty, cross-border usability, and trust. Therefore, no open public consultation was held.

- **Collection and use of expertise**

In preparing this initiative, the Commission drew on external expertise. Beyond regular exchanges with Member State experts, business registries and industry representatives, the Commission contracted specialised consultancy firms to support the collection and analysis of evidence. These contractors conducted targeted interviews and surveys with stakeholders, gathered qualitative and quantitative feedback, and carried out a cost/benefit analysis for the Staff Working Document. Their work was complemented by the Commission's in-house expertise.

- **Staff Working Document**

For this proposal a derogation from an impact assessment was granted as the European Business Wallets build directly on the policy choice already assessed in 2021 for the European Digital Identity Framework and adapts it to the specific context and needs of economic operators and public sector bodies. The proposal therefore follows the 2021 preferred option, namely the establishment of a harmonised wallet framework with Union-wide legal effect, customising it to professional interactions. However, a Staff Working Document analysing in detail the expected costs and benefits of the proposal was prepared. The document provides the intervention logic (problems, drivers and objectives), describes the policy option, and quantifies economic impacts for both public sector bodies and economic operators on the basis of mixed-method research including quantitative and qualitative analysis of public sources, survey data and interview data combined with secondary sources (full details on the methodology are provided in the Staff Working Document).

To meet the objectives of simplification, administrative burden reduction and secure cross-border digital interactions, the initiative requires all public sector bodies in the EU to accept the European Business Wallets in their interaction with economic operators for the purpose of the core minimum functionalities (identification/authentication; signing/sealing; submission and receipt of documents and official notifications), which have legal effect equivalent to paper or in-person processes across the EU. The instrument is technology-neutral and market-driven: it does not prescribe a single design, leaves room for innovative features beyond the common layer, and ensures interoperability with eIDAS trust services and authentic sources.

The impacts of the policy option are outlined in detail in Annex 3 of the Staff Working Document. The costs benefits analysis indicates that there are annual direct costs both for economic operators and public sector bodies. They are divided in one-off costs for training and onboarding, activation and IT implementation, contracting/procurement costs, and in recurring costs for licensing fees and maintenance. Overall, when the Business Wallets reach their full potential and the adoption rate, for both public sector bodies and economic operators, would reach 100%, the total estimated costs and benefits could reach the following figures:

Stakeholder	No. in the EU	Year 1 (€bn)			Year 2 (€bn)		
		Benefits	Costs	<b>Net benefits</b>	Benefits	Costs	<b>Net benefits</b>
Public sector bodies	95,825	19.13	7.32	<b>11.81</b>	19.13	1.15	<b>17.98</b>
Economic operators	32,721,957	205.82	60.67	<b>145.15</b>	205.82	27.23	<b>178.59</b>
<b>Total</b>		<b>224.95</b>	<b>67.99</b>	<b>156.96</b>	<b>224.95</b>	<b>28.38</b>	<b>196.57</b>

Among micro-enterprises, self-employed individuals and sole traders could use their EU Digital Identity Wallets to access the newly introduced communication channel to interact with the Business Wallet ecosystem, without purchasing the full Business Wallet. Based on current market prices across the EU, the estimated annual recurring cost for this service is around €45, suggesting that these operators could connect to the ecosystem at a relatively low cost.

Importantly, the magnitude of the net benefits depends on the rate of usage of the European Business Wallets by economic operators, and SMEs in particular - which represent the largest share of economic operators. The higher the usage, the higher the resulting efficiency, simplification and cost savings across the internal market. Several scenarios are considered in the Staff Working Document: at lower adoption levels, the initiative already generates measurable efficiency gains for economic operators, with public authorities reaching positive returns shortly thereafter. As usage expands, both categories of stakeholders experience clear net benefits, particularly SMEs and micro-enterprises, as network effects begin to take hold. At higher rates of use, the European Business Wallets become a *de facto* standard for business-to-government exchanges, with growing spill-over effects in business-to-business contexts. (for a more detailed analysis, see Chapter 6 and, Annex 3 and 4 of the Staff Working Document).

In addition, beyond direct savings, the initiative generates substantial indirect benefits for the wider EU economy and society, articulated into three areas. The first area is economic opportunities and market competitiveness. Reduced time spent on compliance frees resources that can be redirected into innovation, and cross-border service expansion. By improving data quality and transparency, the initiative also facilitates fraud reduction and optimisation of internal processes. A second area is trust and resilience, where the European Business Wallets are expected to increase trust in digital transactions, and to strengthen the EU's cyber-resilience and operational continuity, including during crises. A third area is environmental sustainability, where gains are expected from the reduction of paper-based processes and the facilitation of more efficient sustainability reporting.

For public sector bodies, the European Business Wallets are expected to bring structural and lasting improvements in administrative efficiency and service quality. By automating verification, document handling and data exchange, the initiative reduces manual processing and the risk of human error, accelerating decision-making and enhancing the reliability of outcomes for citizens and companies. The consolidation of authentication and communication systems into a harmonised EU framework strengthens cybersecurity and digital sovereignty, allowing coordinated risk management and secure data flows. In parallel, the availability of a traceable, standardised channel for information exchange streamlines regulatory supervision, allowing authorities to rely on accurate, auditable data and to deploy innovative RegTech solutions that improve oversight and compliance monitoring.

Together, these indirect benefits reinforce the EU's competitiveness, strengthen trust in digital infrastructures, and support broader policy objectives such as the Green Deal and the Digital Decade.

- **Regulatory fitness and simplification**

This proposal establishes the European Business Wallets as a single, harmonised tool for economic operators to identify, sign, store, submit and receive documents in their interactions with public authorities. It will allow to replace fragmented national procedures with a secure and interoperable solution, thereby removing administrative complexity and reducing compliance costs.

For public sector bodies, it streamlines reporting and verification processes, enabling more efficient supervision and record-keeping. For economic operators, in particular SMEs, it eliminates duplicative procedures and disproportionate burdens. The latter stand to gain the most, as they are disproportionately burdened by fragmented and duplicative administrative procedures. Direct benefits are estimated at €4,000 per year at individual level for microenterprises and €42,250 per year for larger SMEs, but the impact goes beyond cost savings: simplified cross-border procedures will enable faster establishment abroad, easier access to finance, and stronger participation in procurement markets. By ensuring legal certainty and uniform application, the proposal promotes the free movement of goods and services, while at the same time fosters innovation, allowing market-driven features flourishing.

- **Fundamental rights**

While this legislative proposal primarily addresses legal persons, it indirectly supports the protection of several fundamental rights enshrined in the Charter of Fundamental Rights of the European Union. By providing a harmonised and trusted instrument for cross-border business interactions, the initiative strengthens the freedom to conduct a business (Article 16) by removing unnecessary barriers in the Single Market. It also facilitates the exercise of the freedom to choose an occupation and right to engage in work (Article 15), as businesses and professionals can expand their activities across borders more easily and at lower cost.

In their role as “gatekeepers” of administrative procedures within the Single Market, public sector bodies will be enabled to offer more transparent and efficient procedures, thereby indirectly reinforcing the right to good administration (Article 41). The European Business Wallets also contribute to ensuring a high level of protection of personal data (Article 8) in line with existing EU laws, in particular Regulation (EU) 2016/679. For example, the selective disclosure feature, inspired by the European Digital Identity Framework, also serves as a measure for the protection of personal data as users of the European Business Wallets are able

to control the type and amount of data communicated to other European Business Wallets owners and relying parties. In addition, when preparing the implementation of the European Digital Directory, the relevant data protection principles and obligations, such as data minimisation and data protection by design and by default, should be considered.

Finally, by increasing the accuracy and reliability of business credentials, the proposal indirectly strengthens consumer protection (Article 38) and contributes to overall trust and confidence in the Single Market dynamics.

#### **4. BUDGETARY IMPLICATIONS**

The inclusion of Union entities will have financial implications, which will be predominantly covered by the EU budget under the Multiannual Financial Framework (MFF) 2028-2034. These costs are mainly associated with the implementation and use of the European Business Wallets by Union entities and the establishment and maintenance of the European Digital Directory within the Commission.

A detailed overview of the costs involved is provided in the ‘financial statement’ linked to this proposal.

#### **5. OTHER ELEMENTS**

- **Implementation plans and monitoring, evaluation and reporting arrangements**

The impact of the proposed Regulation will be monitored and evaluated in accordance with the Better Regulation Guidelines, covering its implementation and application. The monitoring arrangement constitutes an important part of the proposal. The Commission will monitor its implementation with a view to generating the necessary and relevant information that will feed into a future evaluation and to provide solid evidence for policymaking. In particular the following aspects will be evaluated and monitored: 1) reduction of administrative burden of regulatory compliance and reporting requirements on businesses through demonstrable economic benefits; 2) improvement of public service delivery and 3) enhancement of competitiveness thanks to the Business Wallets’ introduction.

Given the horizontal reach of this regulation and considering the extensive uses-cases that the Business Wallets could support across various economic sectors, it will be important to ensure the efficient and collaborative coordination of its implementation. To this end, a cross-Commission interservice group chaired by DG CONNECT will be established.

On the application of the proposed instrument, the European Commission and the National Competent Authorities will assess also: 1) development of a market for secure digital identification and trust services between economic operators and public sector bodies; 2) trustability and security of available solutions and their compliance with all requirements to provide European Business Wallets and 3) adoption of the Business Wallets among different sectors.

Four years following the adoption of the Regulation, the Commission will carry out an evaluation to assess how effectively the European Business Wallets have met their objectives. The evaluation will look in particular at the usability of the wallets’ minimum core functionalities, the compliance level of wallets’ providers, the functioning of national supervision and penalties, performance of the qualified electronic registered delivery services and the use of Business Wallets and the qualified registered delivery service. Member States

will provide the Commission with the necessary data and evidence for this assessment (for an in-depth analysis of the monitoring and evaluation aspect, see Chapter 9 of Staff Working Document).

- **Detailed explanation of the specific provisions of the proposal**

Chapter I sets out the subject matter and scope of the proposal that applies to the provision and acceptance of European Business Wallets. It also sets out the definitions used throughout the instrument. The definition of the European Business Wallets is deliberately broad and technologically neutral to allow flexibility for varying market-driven solutions and future technological developments, a digital wallet that allows owners to store, manage, and share verified identification data and electronic attestations of attributes, as well as to issue and delegate mandates in a legally recognised manner.

Chapter II establishes the key components for the European Business Wallets framework. It sets out the principle of legal equivalence, serving as a provision which equates actions performed through a European Business Wallet to those carried out in person, on paper, or via any other means or processes: an essential element to remove administrative frictions in concerned exchanges. The principle of equivalence also applies to the use of the qualified electronic registered delivery service by self-employed persons and sole traders. In the same chapter, a minimum, interoperable set of core functionalities, together with qualified electronic registered delivery service as a standalone service to users of European Digital Identity Wallets, is defined alongside with technical requirements, further expanded in the Annex and envisioned to be complemented by implementing acts. Provisions of this chapter also address who can provide European Business Wallets, the relevant requirements that must be met by such legal persons and the process that an eligible entity must undergo at national level in order to be included in the trusted list of providers. To guarantee consistent cross-border recognition, the proposal relies on European Business Wallets' owners' identification data issued as electronic attestations of attributes by qualified trust service providers, national public sector bodies, or by the Commission for Union entities. Using these attestations ensures that every Business Wallet owner can be reliably identified on the basis of official and verifiable information. In addition, a unique identifier is attributed to each Business Wallet owner. Where a European Unique Identifier is assigned under Company Law Directive (EU) 2017/1132 or the Anti-Money Laundering Directive, the Business Wallets will use the European Unique Identifier as the unique identifier. In other cases, Member States designate existing national registers and corresponding registration numbers as the authentic source for generating an equivalent identifier. The structure and technical specifications of this identifier, ensuring Union-wide uniqueness and interoperability, will be defined by implementing acts.

To enable a straightforward communication through the Business Wallets, the proposal also establishes a European Digital Directory, which will be created and maintained by the Commission, will enable economic operators and public sector bodies to be easily contacted, while implementing adequate measures for the protection personal data. In this regard, the Commission will establish standards, technical specifications and the categories of information to be communicated to the Commission for the Directory through implementing acts.

Chapter II also establishes the governance and supervision mechanism. To minimise fragmentation and leverage existing expertise, the proposal names the existing eIDAS supervisory bodies to act as the supervisory authorities in each Member State for Business Wallets' providers established in the respective territories. These authorities also assist providers of Business Wallets in accessing the information needed for the issuance of owner



identification data by issuers of owner identification data based on information available from authentic sources, cooperate closely with the competent authorities for qualified trust service providers, and notify the Commission of the national registries holding data on economic operators and public sector bodies. In this regard, the Regulation provides for the role and tasks of such authorities. Given the Treaties' institutional balance, EU institutions, bodies and agencies (Union entity) are not subject to Member State supervision. The proposal rather provides a Union-level supervisory arrangement under the Commission.

In Chapter III the obligations placed on public sector bodies are set out. These provisions ensure that public sector bodies enable economic operators to use the European Business Wallets for the purposes of identifying, authenticating, signing or sealing, submitting documents, and sending or receiving notifications in administrative or reporting procedures. For the exchange of documents and notifications, public sector bodies must themselves hold a European Business Wallet and use the secure communication channel. The obligations have to be met by set time frames. Public sector bodies may also recognise the use of European Business Wallets and the communication channel (for sole traders and self-employed) as the sole means for submitting electronic documents and attestations when required under Union law. The Commission will review these obligations and their scope over time.

Chapter IV sets out the international dimension of the European Business Wallet framework, establishing the possibility for the recognition of systems developed in third countries that offer functionalities equivalent to the proposal where relevant conditions guarantee a comparable level of trust, security, and interoperability. This approach allows the EU to facilitate trusted global exchanges with non-EU partners while maintaining the Union's high standards for digital identity, authentication, and data integrity.

Chapter V contains the horizontal and closing provisions. It provides for the evaluation and review of the proposed regulation to assess the effectiveness of its implementation and the functioning of the supervisory framework.

Proposal for a

# **REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

## **on the establishment of European Business Wallets**

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 114 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee<sup>(1)</sup>,

Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) In its Communication of 29 January 2025 ‘A Competitiveness Compass for the EU’<sup>(2)</sup> the Commission announced that European Business Wallets, building on the European Digital Identity Framework, will constitute the cornerstone for conducting business in a simple and digital manner within the Union, providing companies with a seamless environment in which to interact with public administrations.
- (2) Regulation (EU) No 910/2014 of the European Parliament and of the Council<sup>(3)</sup> establishes the European Digital Identity Framework and introduces the European Digital Identity Wallets, enabling users to securely store and manage their digital identity and electronic attestations of attributes, and to access a wide range of online services. The European Digital Identity Framework features new trust services, including the issuance of electronic attestations of attributes, thereby enhancing the security and reliability of online transactions and interactions.
- (3) In order to foster a competitive and digital European economy, and to facilitate cross-border business, it is necessary to establish a seamless and secure environment for digital interaction between economic operators and public sector bodies in different configurations.
- (4) In order to ensure the interoperability and security of European Business Wallets, the technical specifications established in Regulation (EU) No 910/2014 and subsequent implementing regulations established pursuant to that Regulation as well as the technology and standards developments and the work carried out on the basis of

---

<sup>1</sup> OJ C 365, 23.9.2022, p. 18.

<sup>2</sup> Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions ‘A Competitiveness Compass for the EU’, COM(2025) 30 final.

<sup>3</sup> Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73, ELI: <http://data.europa.eu/eli/reg/2014/910/oj>).

Recommendation (EU) 2021/946, and in particular the Architecture and Reference Framework, should apply, with the specifications laid down in this Regulation taking precedence in the event of any inconsistency.

- (5) In order to enhance the functioning of the digital single market, ensure interoperability and reduce administrative burdens, it is essential to ensure compatibility between and European Business Wallets and existing systems and solutions at both Union and national level. As prescribed by the Interoperable Europe Act and to enhance secure and efficient data exchanges across the Union, the implementation of the European Business Wallets should, to the extent possible, where appropriate and following technical analysis, make use of existing EU digital infrastructures and building blocks, including those developed under the Once Only Technical System, the Business Registers Interconnection System and the European Digital Identity Wallet, thereby ensuring complementarity, interoperability, and efficient use of public resources.
- (6) The European Business Wallets are a digital tool for economic operators to interact with public sector bodies in the context of meeting reporting obligations and fulfilling administrative procedures. The use of the core functionalities of the European Business Wallets to identify and authenticate, sign or seal, submit documents and send or receive notifications should be without prejudice to procedural requirements that might be part of an administrative procedure and that cannot be fulfilled by the core functionalities of the European Business Wallets. These procedural requirements may include any additional safeguards or verifications, such as checks to ensure the awareness or understanding of the contents of a document or the implications of the signature of a contract, or specific actions that are required as part of an administrative procedure and are not supported by the core functionalities of the European Business Wallets. Public sector bodies should therefore ensure that all relevant procedural requirements are met, including any specific actions or processes which need to be fulfilled as part of an administrative procedure and which cannot be performed through the European Business Wallets.
- (7) Public sector bodies have the flexibility to decide how to ensure that they can accept European Business Wallets considering the diversity of their IT infrastructure and their needs for interoperability. This approach allows public sector bodies to maintain their existing operational frameworks, while benefiting from the advantages of the European Business Wallets.
- (8) This Regulation is without prejudice to the procedural autonomy, the constitutional requirements and the judicial independence that govern the organisation and functioning of national justice systems of the Member States, as well as to the framework, integrity and procedural safeguards of judicial proceedings.
- (9) This Regulation is without prejudice to the Member States' responsibility for safeguarding national security and their power to safeguard other essential State functions, including ensuring the territorial integrity of the State and maintaining law and order.
- (10) This Regulation should be without prejudice to the right of legal persons to submit only once information to public sector bodies as well as to the right of Member States to continue using other systems for the submission of documents and data between competent authorities as established under Union law, such as in Regulation

2018/1724<sup>(4)</sup> and Directive (EU) 2017/1132 establishing the Business Registers Interconnection System

- (11) In order to reduce administrative burden and improve competitiveness, all entities conducting economic activities, including companies, organisations, self-employed persons, sole traders and any other type of business, regardless of size, sector or legal form, should be able to use European Business Wallets. To ensure that legally valid notifications, and documents can be exchanged, and reporting obligations fulfilled by means of European Business Wallets, it is necessary to establish a reliable and secure communication channel that can be used by European Business Wallet owners across the Union. A qualified electronic registered delivery service ('QERDS') should therefore be integrated as a secure communication channel in the European Business Wallets, and should enable the secure and legally valid exchange of information between parties, as provided for in Article 43 of Regulation (EU) No 910/2014.
- (12) In order to provide a tailored solution for self-employed persons and sole traders, it is essential to ensure the seamless integration of European Digital Identity Wallets with European Business Wallets. That integration should enable those persons to authenticate using their European Digital Identity Wallet and access trust services offered for the European Business Wallets, including the QERDS established as a secure communication channel in this Regulation, using those Wallets, without the need to create a separate business identity. Providers of European Business Wallets should therefore be allowed to offer the secure communication channel as a standalone service to self-employed persons and sole traders that use European Digital Identity Wallets in a business capacity, with ensured interoperability to facilitate app switching, as well as trust services such as electronic signatures and qualified and non-qualified time stamping services. Such access to the secure communication channel for self-employed persons and sole traders, should be promoted by ensuring an offer, at reasonable and affordable prices, that reflects the usage needs and is accompanied by terms of use that do not impose an undue burden on those persons.
- (13) The European Business Wallets, in combination with Regulation (EU) 2018/1724, should support the forthcoming 28<sup>th</sup> Regime<sup>(5)</sup> by providing the digital infrastructure for fully digital procedures, enabling start-ups and scale-ups to conduct EU-wide operations in a rapid and efficient manner. The Business Wallets should provide the digital infrastructure for the 28th Regime's digital-first strategy, streamlining cross-border interactions and reducing administrative burden, such as facilitating the secure storing and signature of contracts and certificates or submitting, receiving and sharing electronic applications and documents. By providing this infrastructure, the Business Wallets should help make the "digital by default" principle a reality, facilitating the growth and development of EU companies and enhancing their competitiveness.
- (14) Given the objective of creating a unified digital ecosystem for electronic identification, authentication, and the exchange of electronic documents, notifications, and attestations of attributes, the inclusion of Union entities among public sector bodies covered this Regulation, is necessary. Such an inclusion should create a coherent

---

<sup>4</sup> Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (OJ L 295, 21.11.2018, pp. 1, ELI: <https://eur-lex.europa.eu/eli/reg/2018/1724/oj/eng>)

<sup>5</sup> European Commission, Call for Evidence: 28th regime – a single harmonized set of rules for innovative companies throughout the EU, 8<sup>th</sup> of July, available at [https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14674-28th-regime-a-single-harmonized-set-of-rules-for-innovative-companies-throughout-the-EU\\_en](https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14674-28th-regime-a-single-harmonized-set-of-rules-for-innovative-companies-throughout-the-EU_en)

framework for owners of European Business Wallets to engage with all levels of public administration thereby reducing administrative complexities and driving uptake of the European Business Wallets.

- (15) In order to ensure the proper issuance and integration of European Business Wallets throughout the operations and systems of Union entities, this Regulation should have due regard to the specific nature and structure of such institutions, bodies, offices and agencies. To ensure the respect of administrative autonomy and security of Union entities. They should be allowed to acquire European Business Wallets from already established providers of European Business Wallets, or develop their own European Business Wallets or act themselves as provider for Union entities. Where Union entities act as providers of European Business Wallets, they should also be subject to a supervisory framework. In such cases, the Commission should be tasked to the supervise the provision of European Business Wallets by Union entities.
- (16) Regulation (EU) No 910/2014 established a framework for electronic identification and trust services in the internal market. Building on the ecosystem established by Regulation (EU) No 910/2014, the European Business Wallets should offer economic operators and public sector bodies a secure and reliable solution for digital identification and authentication, data sharing, and the delivery of legally valid notifications. The trust framework for European Business Wallets, including the use of trusted lists, should build upon the structures established under Regulation (EU) No 910/2014.
- (17) The European Business Wallets should allow individuals granted the power to act on behalf of an entity in legal, financial, and administrative matters to exercise their functions by signing any attestations, declarations, or documents executed through a legally valid electronic signature within the meaning of Regulation (EU) 910/2014, which establishes that electronic signatures shall have the equivalent legal effect of a handwritten signature.
- (18) To support the delegation of powers and mandates within a professional context, the European Business Wallets should incorporate a mandate and role-based authorisation system that governs access to services and transactions within the European Business Wallet in such a way as to preserve the integrity of the identity of the owner of that Wallet. That system should enable economic operators and public sector bodies to assign rights to authorised representatives through clearly defined technical mandates allowing the owner of a specific European Business Wallet to grant full rights to generally use the solution and act on its behalf, and an administrative mandate, allowing the owner of a Business Wallet to assign roles and responsibilities to various users of the solution within their organisation. This authorisation system should ensure compatibility with the EU digital power of attorney, as established by Directive (EU) 2025/25 of the European Parliament and of the Council<sup>6</sup>. This authorisation system should be robust and scalable, to ensure that economic operators and public sector bodies, as the owners of European Business Wallets, can delegate authority to multiple users, including employees or other authorised natural or legal persons, thereby facilitating the efficient and secure management of internal activities and ensuring that access to European Business Wallets and their functions is controlled and auditable.

---

<sup>6</sup> 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 (OJ L, 2025/25, 10.1.2025, ELI: <http://data.europa.eu/eli/dir/2025/25/oj>).



This system should govern access to services and transactions within the European Business Wallet, preserving the integrity of the owners' identities.

- (19) In order to facilitate the conduct of cross-border business transactions, reduce administrative burdens, and promote economic growth, it is necessary to establish a clear and predictable legal framework that recognises the legal equivalence between the use of the European Business Wallets, or their core functionalities and the secure communication channel where the latter is used by self-employed persons and sole traders, and other accepted methods for economic operators to identify, authenticate, submit documents and receive notifications when interacting with public sector bodies in the Union. To that end, the use of the core functionalities of a European Business Wallet, or the secure communication channel where the latter is used by self-employed persons and sole traders, should have the same legal effect as if lawfully carried out in person, in paper form, or via any other means or process that would otherwise be deemed compliant with applicable legal, administrative, or procedural requirements.
- (20) To ensure a consistent user experience and to guarantee the utility, reliability, and interoperability of European Business Wallets across the Union, providers of European Business Wallets should implement a core set of functionalities. They should retain the freedom to offer additional features as part of their commercial offering, fostering innovation and responding to market needs. In order to ensure uniform conditions for the development and use of the core functionalities, implementing powers should be conferred on the Commission to set out requirements and technical specifications necessary to ensure interoperability and seamless functioning across the Union. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and the Council<sup>(7)</sup> and should include the powers to define the necessary standards and protocols for the secure communication channel, taking into account the latest technological developments.
- (21) European Business Wallets should simplify the complex interactions between economic operators and public sector bodies, and could also facilitate interactions among economic operators themselves, reducing administrative burden on economic operators in a broad range of economic sectors. In order to foster innovation and competitiveness, the European Business Wallets should enable sector-specific use cases and enhance operational efficiencies, while ensuring flexibility and adaptability to support the unique requirements of different sectors, including, but not limited to, agriculture, energy, environment, social security coordination.
- (22) The use of the European Business Wallets in such contexts can aid in the reduction of costs and promote a wide range of applications and use cases across the Union, such as the submission of declarations, applications for public funding, access to public services and facilitating secure data sharing and access within data spaces, such as the submission of A1 certificates concerning posted workers provided for under Regulation (EU) 883/2004.
- (23) The establishment of the European Business Wallets alongside the Once Only Technical System is expected to create powerful synergies that maximise efficiency and operational ease. In particular, economic operators should be able to use the

---

<sup>7</sup> Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers (OJ L 55, 28.2.2011, p. 13, ELI: <http://data.europa.eu/eli/reg/2011/182/oj>).

European Business Wallet to hold and transmit evidence retrieved from competent public authorities through the Once-Only Technical System. Where appropriate, economic operators should also be able to combine evidence held in the European Business Wallet with evidence retrieved via the Once Only Technical System in the context of public procedures. Consequently, by providing a secure digital platform for storing and exchanging business documents, the European Business Wallets should facilitate the exchange of such documents between public sector bodies through the mechanisms established under Once-Only Technical System.

- (24) In order to ensure coordination between the Union's ongoing digitalisation of judicial cooperation, the modernisation of secure cross-border information exchange, and the need to provide economic operators with efficient digital tools to interact with authorities, it is necessary to establish a coherent framework that enables smooth interaction between such relevant systems. Enhancing such coordination will reduce administrative burden, improve legal certainty, and strengthen the effectiveness of cross-border cooperation, by ensuring that communication channels used by economic operators function seamlessly within the European digital market. In that context, European Business Wallets should complement the systems set out in Regulation (EU) 2023/2844 and Regulation (EU) 2023/969, where a seamless interaction between these systems and the Business Wallets should be maintained through the Business Wallets gateway, enabling relevant authorities to maintain these systems whilst promoting simplification for European companies.
- (25) To facilitate a flexible and efficient exchange of information and services when using European Business Wallets, and to ensure seamless integration of European Business Wallets with existing digital identity solutions, it should be possible to use European Digital Identity Wallets and electronic attestations of attributes for onboarding to and access management of the European Business Wallets. This should enable users to leverage existing digital identities and electronic attestations of attributes to access European Business Wallets, thereby streamlining the onboarding process and enhancing the overall user experience. The use of electronic attestations of attributes in the context of the European Business Wallets should cater to the diverse needs of European Business Wallet owners and may be used to issue and enable the secure and trustworthy verification of key attributes, such as an owner's current address, VAT registration number, tax reference number, Legal Entity Identifier (LEI), Economic Operator Registration and Identification (EORI) number and excise number. European Business Wallets should support a wide range of use cases, from simple authentication and identification to more complex transactions and interactions.
- (26) In order to ensure the secure and trustworthy operation of European Business Wallets, providers of European Business Wallets should ensure that each European Business Wallet they provide is pre-configured to interact with certain trust services, which are required to enable the core functionalities of European Business Wallets, including the creation of qualified electronic signatures, the creation of qualified electronic seals, and the issuance and validation of qualified and non-qualified electronic attestations of attributes. To support these functionalities, European Business Wallets should allow for the sharing and storage of specific information and documents relating to the owner, such as messages and documents for the secure communication channel, signed and sealed documents, and sets of attributes for attestation-related services.
- (27) To allow for the legal recognition of electronic attestations of attributes presented via European Business Wallets, it is necessary to allow for the creation and validation of linked attestations, whereby one attestation is cryptographically linked to another in a

manner that allows the verification of the authenticity and integrity of each individual attestation, and of all linked attestations collectively. To that end, the European Business Wallet infrastructure should, through the use of the chain of attestations, enable the submission of a single instance of an attestation and facilitate its subsequent reuse across relevant procedures. Such functionality should allow European Business Wallet owners to transmit a reference to a document where appropriate with a cryptographic element, such as a hash key to a sealed attestation issued by a European Business Wallet, thereby attesting to the integrity and authenticity of the original submission.

- (28) In order to ensure that the standards and technical specifications for European Business Wallets ensure harmonisation across various solutions, it is necessary to define the standards and protocols for the core functionalities and technical requirements for European Business Wallets in an Annex to this Regulation. The Annex should set out the requirements for the implementation of European Business Wallets. To ensure the long-term viability and effectiveness of the European Business Wallets, implementing powers should be conferred on the Commission to establish and update the procedures and technical specifications on the implementation of core functionalities, thereby allowing for the integration of additional features and new technologies that would enable new use cases, such as agentic AI or the provision of a digital identity to an owner's asset, and enabling the European Business Wallets to continue to support the evolving needs of economic operators in a secure and trustworthy manner. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and the Council. To the extent possible, the standards and technical specifications of the European Business Wallet should take into account relevant technical solutions and standards used by existing ICT systems by economic operators, facilitating the alignment of these systems to be aligned to and made interoperable with the European Business Wallet.
- (29) To support the timely development of the market for European Business Wallets, the adoption of the implementing acts on core functionalities and the accompanying technical specifications should be prioritised. Where appropriate, these should build on the existing standards including those out in the Architecture and Reference Framework provided for in the context of Regulation (EU) No 910/2014, to support the re-use of familiar technical standards and uptake of the European Business Wallets.
- (30) To ensure the high level of trust, functionality, and security of European Business Wallets necessary to the cross-border provision of their services, and in particular to mitigate the risk of fraud, providers of European Business Wallets should be subject to clear and proportionate requirements and obligations without being subject to additional national requirements.
- (31) To ensure proper supervision in line with this Regulation, entities that would like to become providers of European Business Wallets should be required to notify their intention to provide such European Business Wallets to the supervisory bodies prior to offering their services. In order to safeguard the integrity and accountability of European Business Wallet providers and to ensure the security of data stored or exchanged in the European Business Wallets ecosystem, providers should be established within the Union. This should ensure that such providers fall under the jurisdiction and supervision of a competent body in a Member State, allowing for effective enforcement of this Regulation and the protection of users' rights and data.

Furthermore, providers of European Business Wallets should not present a risk to the security of the Union, namely by not being subject to control by a third country or by a third-country entity, to ensure that the Union's critical digital infrastructure remains secure and resilient. In line with the requirements set out in this Regulation, the Commission may adopt implementing acts to ensure cooperation and interoperability with solutions established or endorsed by like-minded partners of the Union.

- (32) The Union must protect its security interest against providers which could represent a persistent security risk due to the potential interference from third countries. To that end, it is necessary to reduce the risk of persisting dependency on high-risk suppliers in the internal market, including in the ICT supply chain, as they could have potentially serious negative impacts on the security of economic operators and public sector bodies across the Union and the Union's critical infrastructure, especially with regards to the integrity, confidentiality and availability of data and services. Any restrictions should be based on a proportionate risk assessment and corresponding mitigation measures as defined in Union policies and laws. Such limitations may apply, for example, to high-risk suppliers, as identified under Union law.
- (33) In order to establish the identity of economic operators in a secure and reliable manner, this Regulation should allow for the use of qualified electronic attestations of attributes to issue European Business Wallet owner identification data. Qualified electronic attestations of attributes can be easily updated or revoked. The use of qualified electronic attestations of attributes for establishing the identity of economic operators provides an efficient, and secure solution that is suited to the needs of the digital economy. Qualified trust service providers issuing these attestations are regulated under Regulation (EU) No 910/2014 and are subject to strict requirements and scrutiny, ensuring a high level of security and trust in the issuance process. The authentic sources used to verify the data contained in the qualified electronic attestations of attributes are business registers and other registers, and the use of the Business Registers Interconnection System ('BRIS') and the Beneficial Ownership Registers Interconnection System ('BORIS') should be promoted to facilitate the verification of this data, thereby ensuring the accuracy and reliability of the identification data.
- (34) This Regulation should not affect the functioning or the role of business registers as authentic sources and should not alter the way they operate or the data filed therein but rather build upon and complement the existing infrastructure. In this regard, where electronic attestations of attributes are issued by or on behalf of an authentic source, such as a business register, the register could directly issue the relevant data, further enhancing the security and reliability of the identification process.
- (35) Regulation (EU) No 910/2014 requires Member States to ensure that measures are taken to allow qualified trust service providers to verify by electronic means, at the request of the user, the authenticity of the attributes listed in Annex VI of Regulation (EU) No 910/2014, such as educational and professional qualifications, titles and licenses, powers and mandates to represent natural or legal persons, public permits and licenses and financial and company data. The European Business Wallets framework should build on this existing requirement that should cover all official data that is relevant for economic operators in the context of the European Business Wallets and enable the electronic verification of attributes to facilitate the issuance of European Business Wallet owner identification data and other electronic attestations of attributes.

- (36) As all economic operators and entities conducting economic activities should be able to use European Business Wallets, including self-employed persons and sole traders, European Business Wallet owner identification data should be provided in a manner that is specifically designed to verify their identity and attested attributes within a business context. To ensure consistency with existing Union frameworks and facilitate cross-border interoperability, the European Business Wallet framework should use the European Unique Identifier (EUID) provided by the codified Company Law Directive (EU) 2017/1132<sup>(8)</sup> and Commission Implementing Regulation (EU) 2021/369<sup>(9)</sup> as well as Regulation (EU) 2024/1624<sup>(10)</sup> and Commission Implementing Regulation (EU) 2021/369<sup>(11)</sup>. Companies and other legal entities as well as arrangements such as trusts are assigned a European Unique Identifier to enable their unequivocal identification in cross-border situations. The European Unique Identifier is currently made publicly accessible through BRIS and used by BORIS. Accordingly, the European Business Wallet framework should rely on the issuance and recording process of European Unique Identifiers as the means of verifying the identity of economic operators to which European Unique Identifiers are provided in accordance with Directive (EU) 2017/1132. The European Business Wallet framework should rely on the issuance and recording process of European Unique Identifiers for other economic operators falling under Directive (EU) 2015/849.
- (37) To ensure that all European Business Wallet owners can be reliably identified and their electronic attestation of attributes are associated with a unique entity, it is also necessary to assign a unique identifier to other economic operators and public sector bodies. To ensure uniform conditions for the implementation of unique identifiers, in particular their effectiveness and consistency, implementing powers should be conferred on the Commission to specify the detailed requirements for the unique identifiers. Those powers should be exercised in accordance with Regulation (EU) No 182/2011. Given the diverse approaches among Member States regarding the registration of some economic operators and public sector bodies, it is important to ensure transparency and accessibility for providers of European Business Wallet owner identification data. To this end, Member States should notify to the Commission the authentic sources that are relevant for the issuance of European Business Wallet owner identification data.
- (38) In order to ensure the efficient, secure, and transparent functioning of the European Business Wallet framework, it is necessary to establish a European Digital Directory, that includes personal data of economic operators. The Commission should be

---

<sup>8</sup> Directive (EU) 2017/1132 of the European Parliament and of the Council of 14 June 2017 relating to certain aspects of company law (codification) (OJ L 169, 30.6.2017, pp. 46–127, ELI: <http://data.europa.eu/eli/dir/2017/1132/oj>)

<sup>9</sup> Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (OJ L, 2024/1624, 19.6.2024, ELI: <http://data.europa.eu/eli/reg/2024/1624/oj>)

<sup>10</sup> Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money-laundering or terrorist financing, and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010 and (EU) No 1095/2010 (OJ L ..., 19.6.2024, ELI: <http://data.europa.eu/eli/reg/2024/1624/oj>)

<sup>11</sup> Commission Implementing Regulation (EU) 2021/369 of 1 March 2021 establishing the technical specifications and procedures required for the system of interconnection of central registers referred to in Directive (EU) 2015/849 of the European Parliament and of the Council (OJ L 71, 2.3.2021, pp. 11–17, ELI: [http://data.europa.eu/eli/reg\\_impl/2021/369/oj](http://data.europa.eu/eli/reg_impl/2021/369/oj))



empowered to set up and maintain this Directory, as a trusted source of information on economic operators and public sector bodies using European Business Wallets. The Directory should enable European Business Wallet owners to be easily contacted to promote legal certainty in relation to dealings between businesses and in relation to interactions with public sector bodies, particularly in the view of promoting trade between Member States. European Business Wallet Providers, liaising with the Commission, should submit the necessary information to support the functioning of the European Digital Directory and collaborate with the relevant qualified trust service providers to ensure that the data submitted remains accurate. Such actions shall not indirectly create a requirement for economic operators to update such information. In this regard the Digital Directory will rely on the information made available by business registers also through BRIS while ensuring that such information will not be duplicated.

- (39) Regulation (EU) 2016/679 of the European Parliament and of the Council applies to all personal data processing activities under this Regulation. Where the European Digital Directory includes the processing of personal data this will be carried out in accordance with the relevant data protection principles, such as the data minimisation and purpose limitation principle, obligations, such as data protection by design and by default, and include, where appropriate, features of pseudonymisation.
- (40) To avoid excessive regulatory burdens, ex post supervision of providers of European Business Wallets and monitoring of their activities should be provided for, rather than requiring prior compliance verification for every aspect of their operations. This approach should allow for a more flexible and efficient regulatory environment, while maintaining the necessary safeguards to protect users and ensure compliance with the requirements of the European Business Wallets framework. The notification process for providers of European Business Wallets should be streamlined and efficient, with clear requirements and timelines for applicants. Qualified trust service providers, which are already subject to a robust regulatory framework under Regulation (EU) No 910/2014, should benefit from a particularly light process to be able to provide European Business Wallets.
- (41) In order to ensure transparency and accountability in the European Business Wallet ecosystem, a publicly available list of notified providers of European Business Wallets should be established and maintained by the Commission. That list should include information transmitted by the national supervisory bodies concerning providers, including qualified trust service providers, that have completed the notification process. Making that information publicly available should enable users to verify the authenticity and trustworthiness of providers, thereby promoting a high level of security and trust in the European Business Wallet ecosystem.
- (42) Effective oversight by supervisory bodies, vested with sufficient powers and provided with adequate resources, is essential to ensure that European Business Wallets made available in the Union comply with the requirements laid down in this Regulation. To best ensure such oversight and relevant expertise, Member States should designate the same supervisory body or bodies as designated pursuant to Article 46a(1) and Article 46b(1) of Regulation (EU) No 910/2014.
- (43) Due consideration should be given to ensuring effective cooperation between supervisory bodies designated under this Regulation, Article 46b of Regulation (EU) No 910/2014 and the competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 of the European Parliament and of the

Council<sup>(12)</sup> Since the competent authorities are distinct entities, they should cooperate closely and in a timely manner, including by exchanging relevant information to ensure effective supervision and compliance of European Business Wallet providers with the applicable obligations under Regulation (EU) No 910/2014 and Directive (EU) 2022/2555.

- (44) To harmonise the enforcement of this Regulation, national supervisory bodies should be empowered to impose administrative fines. It is necessary to specify the upper limit of administrative fines and the criteria for their determination in order to promote equal treatment of providers of European Business Wallets across the Union regardless of their Member State of establishment. The competent supervisory authority should assess each case individually, taking into account all relevant circumstances, including the nature, gravity and duration of the infringement, its consequences and any measures taken to ensure compliance and mitigate harm. In this regard, Member States should notify the Commission of the rules laid down in national law allowing the supervisory body to impose penalties by [Publications Office, insert the date 12 months after the entry into force of this Regulation] and should notify the Commission without delay of any subsequent amendments to those rules.
- (45) In order to ensure the proper functioning of the internal market and to protect the rights of economic operators, it is necessary to establish a mechanism for the Commission to intervene in cases where a provider of European Business Wallets is found to be non-compliant with the requirements of this Regulation and no effective measures have been taken by the competent supervisory authority to remedy the situation. This mechanism should allow for the Commission to carry out an evaluation of compliance, consult with the Member States concerned and the provider, and adopt implementing acts to provide for corrective or restrictive measures. This should enable the Commission to take swift and effective action to address any non-compliance and to ensure that the European Business Wallets are used in a secure and trustworthy manner.
- (46) The Cooperation Group established pursuant to Regulation (EU) No 910/2014 should be given the additional responsibility for the coordination of national practices and policies related to this Regulation and facilitate discussions between competent authorities regarding the Regulation's application and enforcement, thereby delivering on the objectives of the Cooperations Group's establishment and retaining expertise for the benefit of implementing the European Business Wallet framework.
- (47) In order to support effective take-up and interoperability, all public sector bodies should be required to enable the use of the European Business Wallet in all relevant administrative procedures for the purposes of identification and authentication, signing or sealing documents, submitting documents and sending or receiving notifications. In this regard, public sector bodies should by [Publications Office, please insert the date 24 months after the entry into force of this Regulation] ensure that the use of European Business Wallets by economic operators is possible and that, where the receipt or communication of documents or notifications is concerned, they are able to access the

---

<sup>12</sup> 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 (OJ L 333, 27.12.2022, pp. 80–152, ELI: <http://data.europa.eu/eli/dir/2022/2555/oj>)

Business Wallets' secure communication channel. To ensure seamless and interoperable application of this Regulation in this regard, public sector bodies should own a European Business Wallet for the purposes of receiving or sending documents and notifications. The obligation for public sector bodies to accept European Business Wallets by economic operators should not affect systems used for the exchange or submission of documents or data between competent authorities.

- (48) In order to avoid disrupting existing interactions between economic operators and public sector bodies, it is necessary to enable a transition period until [Publications Office, please insert the date 36 months after the entry into force of this Regulation]. During such period public sector bodies may choose not to offer the European Business Wallets' secure communication channel and instead support alternative solutions already in place which enable economic operators to communicate with public sector bodies prior to offering the European Business Wallets' secure communication channel. In order to ensure an adequate level of security and interoperability, any alternative solution used during this transition period should comply with the requirements for Qualified Electronic Registered Delivery Services set out in Regulation (EU) No 910/2014 and offer a gateway to European Business Wallets. The gateway should enable users of European Business Wallets to access the alternative solutions used during the transition period. After this period, public sector bodies should support the secure communication channel of the European Business Wallets to ensure a harmonised and efficient means of communication across the Union, to the benefits of European businesses.
- (49) European Business Wallets contribute to the provision of a cross-border digital public service within the meaning of the Interoperable Europe Act (EU) 2024/903. The assessment required under that Regulation has been carried out, and the resulting report will be published on the Interoperable Europe Portal.
- (50) To ensure that the European Business Wallets ecosystem continues to meet the needs of economic operators and public sector bodies, it is necessary to assess its implementation and impact in light of the purpose of this Regulation. The evaluation should, in particular, take into account the risk of legal fragmentation within the internal market regarding the electronic submission of documents and attestations of attributes as well as the technological developments and progression of the market for European Business Wallets and associated trust services.
- (51) To avoid duplication and reduce administrative burden, public sector bodies should not require the same information or documents to be submitted again through physical or alternative digital means, or in the inverse, once these have been validly transmitted via the European Business Wallet in accordance with this Regulation. Accordingly, Member States should not adopt or maintain additional national requirements regarding matters falling within the scope of this Regulation, unless explicitly provided for herein, since this would affect its direct and uniform application.
- (52) In order to enable effective access to Union procedures and markets and facilitate the participation of economic operators established outside the Union in the European Business Wallet framework, it is necessary to enable providers of European Business Wallets to issue European Business Wallets to such operators, provided that their identity can be verified with a high level of certainty. To prevent duplicate registrations and safeguard the integrity of the internal market, such operators should not be allowed to obtain more than one set of European Business Wallet owner identification data and one unique identifier. Member States' should cooperate to

mitigate the risk of duplicate registrations and ensure the uniqueness of registrations of economic operators established outside of the Union.

- (53) The implementing act concerning the requirements and procedures for the unique identifier should encompass the conditions for their issuance to third country economic operators. In particular, it should set the conditions that promote coordination between providers of European Business Wallet owner identification data, ensuring that each third country economic operator is attributed only one unique identifier for the purpose of the European Business Wallet owner identification data. Prior to the provision of a European Business Wallet to an economic operator established outside the Union the relevant provider should confirm that the conditions for verifying the identity of the economic operator have been met. That should allow economic operators from third countries to use European Business Wallets, while preserving the security and trustworthiness of the ecosystem.
- (54) In order to ensure uniform conditions for the implementation of the recognition and interoperability of business wallets or similar systems and framework from third countries to support and promote partnerships and cooperation, implementing powers should be conferred on the Commission to set the conditions under which such similar systems or framework benefit from the provisions of this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council.
- (55) Regulation (EU) No 910/2014 offers a secure and convenient means for natural persons, such as citizens and residents, to identify themselves and access online services. It requires Member States to ensure that European Digital Identity Wallets are provided to legal persons, despite a lack of clarity on the specific technical implementation of European Digital Identity Wallets for legal persons. This uncertainty about the purpose and functioning of the European Digital Identity Wallets for legal persons increases legal and technical complexity for Member States. It is therefore necessary to amend Article 5a of Regulation (EU) No 910/2014 to ensure that the mandatory issuance of European Digital Identity Wallets relates only to natural persons.
- (56) The framework established by this Regulation should provide a secure, Union-wide digital infrastructure and should therefore constitute the principal instrument for such purposes. To fully realise the benefits of the European Business Wallet framework for both economic operators and public sector bodies, it is necessary to promote its use as the default tool for secure digital identification, authentication, and the exchange of electronic documents and attestations of attributes.
- (57) To ensure a coherent and horizontal application across sectors of Union legislation, reduce administrative cost on economic operators and to improve budgetary efficiency, Union law concerning electronic identification, authentication, or the exchange of electronic documents, notifications, or attestations of attributes, particularly where specific technical requirements, systems, or protocols are established, should be applied in a manner consistent with this Regulation. Accordingly, any future legislative or non-legislative initiatives in these fields should adhere to the Business-Wallet-by-Default principle and should be designed and developed to build upon and enable the use of European Business Wallets. Where such alignment is not possible, the Commission should provide a written justification through an Impact Assessment, accompanying the relevant initiative, setting out the reasons for not enabling the use of European Business Wallets. The Commission

should evaluate and review this Regulation by [Publications Office, please insert the date 3 years post adoption] and every four years thereafter and report to the European Parliament and the Council. This review is essential for assessing the continued relevance of the prescribed core functions and technical specifications, especially those associated with the QERDS as a secure communication channel, in the context of the latest technological advancements. Furthermore, the Commission should evaluate the notification procedures for providers of European Business Wallet, as well as the implementation and effectiveness of the rules on penalties established by Member States, to evaluate market developments and compliance levels.

- (58) The European Data Protection Supervisor was consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725 of the European Parliament and of the Council<sup>(13)</sup>, and delivered an opinion on [insert date].

HAVE ADOPTED THIS REGULATION:

## **Chapter I - Subject matter, scope and definitions**

### *Article 1*

#### **Subject matter**

This Regulation enables secure digital identification and authentication, data sharing and legally valid notifications, reduces administrative burdens and compliance costs, and supports cross-border business and competitiveness. In particular, it:

- (1) establishes a framework for the provision of European Business Wallets;
- (2) establishes the principle of equivalence, giving equivalent legal effect to actions and transactions carried out through a European Business Wallet as to actions and transactions lawfully carried out in person, in paper form, or via any other means or processes that would be deemed compliant with applicable legal, administrative, or procedural requirements;
- (3) establishes rules for the issuance of European Business Wallet owner identification data for the identification of economic operators and public sector bodies;
- (4) establishes the European Digital Directory;
- (5) designates the European unique identifier (EUID), as established and governed by Directive (EU) 2017/1132, as the unique identifier for European Business Wallet owners, and establishes a similar unique identifier for European Business Wallets owners to whom the European Unique Identifier is not available;
- (6) lays down the notification mechanism under which providers of European Business Wallets shall be established;
- (7) lays down obligations for public sector bodies concerning European Business Wallets;
- (8) provides a framework for the supervision of Union entities, where such public sector bodies provide European Business Wallets;

---

<sup>13</sup> Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39, ELI: <http://data.europa.eu/eli/reg/2018/1725/oj>).



- (9) provides a framework for the recognition of third-country systems similar to the European Business Wallets and the issuance of European Business Wallets to third country economic operators.

## *Article 2*

### **Scope**

1. This Regulation applies to the provision and acceptance of European Business Wallets and the issuance and acceptance of European Business Wallet owner identification data, and to the use of European Business Wallets by economic operators and public sector bodies.
2. This Regulation is without prejudice to the existing systems and procedures mandated by Union law governing the exchange of documents and data between competent authorities.

## *Article 3*

### **Definitions**

For the purposes of this Regulation, the following definitions apply:

- (1) ‘European Business Wallet’ means a digital solution that allows European Business Wallet owners to securely store, manage, and present European Business Wallet owner identification data and electronic attestations of attributes to Business Wallet-relying parties and other entities using European Business Wallets and European Digital Identity Wallets for the following purposes:
  - (a) to authenticate and provide the verified proofs required by a relying party;
  - (b) to access and use electronic attestations of attributes, electronic signatures, electronic seals, electronic registered delivery services, and electronic time stamps;
  - (c) to enable the creation, management and delegation of mandates to authorised representatives;and that may support additional functionalities in accordance with this Regulation;
- (2) ‘European Business Wallet owner identification data’ means a set of data that enables the establishment of the identity of a European Business Wallet owner and that is issued by a provider of European Business Wallet owner identification data;
- (3) ‘provider of European Business Wallet owner identification data’ means a qualified trust service provider or public sector body or the Commission issuing European Business Wallet owner identification data;
- (4) ‘economic operator’ means any natural or legal person, or a group of such persons, including temporary associations of undertakings, acting in a commercial or professional capacity for purposes related to their trade, business, craft or profession;

- (5) ‘public sector body’ means a Union entity, a national, state, regional or local authority, a body governed by public law or an association formed by one or several such entities or bodies , or a private entity mandated by at least one such entities, authorities, bodies or associations to provide public services, when acting under such a mandate;
- (6) ‘Union entity’ means a Union institution, body, office and agency set up by or pursuant to the Treaty on European Union, the Treaty on the Functioning of European Union or the Treaty establishing the European Atomic Energy Community;
- (7) ‘European Business Wallet owner’ means an economic operator or public sector body that owns or has a right of use of a European Business Wallet;
- (8) ‘trust service’ means trust service as defined in Article 3, point (16) of Regulation (EU) 910/2014;
- (9) ‘attribute’ means attribute as defined in Article 3, point (43) of Regulation (EU) 910/2014;
- (10) ‘electronic attestations of attributes’ means electronic attestations of attributes as defined in Article 3, point (44) of Regulation (EU) No 910/2014;
- (11) ‘qualified attestation of attributes’ means qualified attestation of attributes as defined in Article 3, point (45) of Regulation (EU) No 910/2014;
- (12) ‘European Digital Identity Wallet’ means European Digital Identity Wallet as defined in Article 3, point (42) of Regulation (EU) No 910/2014;
- (13) ‘electronic signature’ means an electronic signature as defined in Article 3, point (10) of Regulation (EU) No 910/2014;
- (14) ‘qualified electronic signature’ means a qualified electronic signature as defined in Article 3, point (12) of Regulation (EU) No 910/2014;
- (15) ‘electronic seal’ means an electronic seal as defined in Article 3, point (25) of Regulation (EU) No 910/2014;
- (16) ‘qualified electronic seal’ means qualified electronic seal as defined in Article 3, point (27) of Regulation (EU) No 910/2014;
- (17) ‘qualified electronic stamp’ means a qualified electronic stamp as defined in Article 3, point (34) of Regulation (EU) No 910/2014;
- (18) ‘authorised representative’ means a natural or legal person acting on behalf of the European Business Wallet owner in executing and operating functions of a designated European Business Wallet on the basis of an authorisation granted by a European Business Wallet owner;
- (19) ‘mandate’ means the authorisation granted by a European Business Wallet owner to an authorised representative, enabling that representative to act on behalf of the owner in executing and operating functions of a designated European Business Wallet;
- (20) ‘electronic document’ means an electronic document as defined in Article 3, point (35) of Regulation (EU) No 910/2014;
- (21) ‘qualified electronic registered delivery service’ means a qualified electronic registered delivery service as defined in Article 3, point (37) of Regulation (EU) No 910/2014;

- (22) ‘user’ means a natural or legal person, or a natural person representing another natural person or a legal person, that uses European Business Wallets or European Business Wallet electronic identification means provided in accordance with this Regulation;
- (23) ‘European Business Wallet-relying party’ means a natural person, an economic operator or public sector body that relies upon European Business Wallets;
- (24) ‘wallet unit attestation’ means a data object that describes the components of the European Business Wallet unit or allows authentication and validation of those components;
- (25) ‘European Business Wallet unit’ means a unique configuration of a European Business Wallet solution that includes European Business Wallet front-end and European Business Wallet back-end, wallet secure cryptographic applications and wallet secure cryptographic devices provided by a provider to a European Business Wallet to a specific European Business Wallet owner;
- (26) ‘European Business Wallet solution’ means a combination of software, hardware, services, settings, and configurations, including European Business Wallet front-end and back-end, one or more wallet secure cryptographic applications and one or more wallet secure cryptographic devices;
- (27) ‘critical assets’ means assets within or in relation to a European Business Wallet unit of such extraordinary importance that where their availability, confidentiality or integrity are compromised, that would have a very serious, debilitating effect on the ability to rely on the European Business Wallet unit;
- (28) ‘wallet secure cryptographic application’ means an application that manages critical assets by being linked to and using the cryptographic and non-cryptographic functions provided by the wallet secure cryptographic device;
- (29) ‘wallet secure cryptographic device’ means a tamper-resistant device that provides an environment that is linked to and used by the wallet secure cryptographic application to protect critical assets and provide cryptographic functions for the secure execution of critical operations;
- (30) ‘trust service provider’ means a trust service provider as defined in Article 3, point (19) of Regulation (EU) No 910/2014;
- (31) ‘qualified trust service provider’ means qualified trust service provider as defined in Article 3, point (20) of Regulation (EU) No 910/2014;
- (32) ‘electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source’; means a electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source as defined in Article 3, point (46) of Regulation (EU) No 910/2014;
- (33) ‘authentic source’ means authentic source as defined in Article 3, point (47) of Regulation (EU) No 910/2014;
- (34) ‘attestation scheme’ means a set of rules applicable to one or more types of electronic attestation of attributes;
- (35) ‘catalogue of schemes’ means a digital repository listing schemes for the attestation of attributes registered in accordance with this Regulation and that is maintained and published online by the Commission;

- (36) 'European unique identifier' means the European Unique Identifier referred to in Directive (EU) 2017/1132;
- (37) 'national register' means an official database or system established and maintained by or on behalf of a national government or its designated authority, which records, stores, and manages information pertaining to legal entities, including but not limited to companies, partnerships, foundations, associations as well as businesses as natural persons such as sole-traders and self-employed persons or other registrable persons or organisations;
- (38) 'API' or 'Application Programming Interface' means a set of definitions and protocols for building and integrating application software to share data;
- (39) 'submission' or 'submit' means any transmission of structured or unstructured data, files, forms, or records by between a public sector body and an economic operator or between economic operators or between public sector bodies, where such transmission is required, requested, or permitted under Union or national law, and is intended to support a legal, administrative, or procedural purpose;
- (40) 'notification' means any transmission of information, decisions, requests, or acknowledgements between a public sector body and an economic operator or between economic operators or between public sector bodies, which is required, requested, or permitted under Union or national law, and which is intended to produce legal effects or inform the recipient of rights, obligations, or procedural developments;
- (41) 'administrative procedure' means a sequence of actions, defined by Union or national law, that must be taken by economic operators or public sector bodies to comply with obligations, provide information, or obtain a decision, authorisation, or benefit from a public sector body in the exercise of administrative functions;
- (42) 'European Business Wallet front-end' means the user interface component, regardless of platform or form factor, that interacts with users acting on behalf of the owner, and is part of the European Business Wallet unit;
- (43) 'European Business Wallet back-end' means the server-side components, including software, services, and infrastructure, that provide the necessary functionality and support for the European Business Wallet Frontend, and form part of the European Business Wallet unit.

## **Chapter II – European Business Wallets**

### *Article 4*

#### **Principle of equivalence**

Where a European Business Wallet owner makes use of any of the core functionalities of a European Business Wallet referred to in Article 5(1), the resulting action shall have the same legal effect as if the action had been lawfully carried out in person, in paper form, or via any other means or processes that would be deemed compliant with applicable legal, administrative, or procedural requirements.

Where a self-employed person or a sole trader makes use of the qualified electronic registered delivery service in the circumstances set out in Article 5(3), the resulting action shall have the

same legal effect as if the action had been lawfully carried out in person, in paper form, or via any other means or processes that would be deemed compliant with applicable legal, administrative, or procedural requirements.

## *Article 5*

### **Core functionalities of European Business Wallets**

1. Providers of European Business Wallets shall ensure that the European Business Wallets they provide enable European Business Wallet owners to make use of the following core functionalities:
  - (a) securely issue, request, obtain, select, combine, store, delete, share and present electronic attestations of attributes;
  - (b) selectively disclose European Business Wallet owner identification data and attributes contained in electronic attestations of attributes, in the context of the functionalities listed in point a;
  - (c) request and share European Business Wallet owner identification data and electronic attestations of attributes in a secured way between European Business Wallets and European Digital Identity Wallets and with European Business Wallet-relying parties;
  - (d) sign by means of qualified electronic signatures and seal by means of qualified electronic seals, as applicable;
  - (e) bind data in electronic form to a particular time by means of qualified electronic time stamps;
  - (f) issue electronic attestations of attributes to European Business Wallets and European Digital Identity Wallets;
  - (g) issue electronic attestations of attributes through the European Business Wallet of the owner, allowing the issued attestation to be linked to other relevant attestations forming part of a chain;
  - (h) enable the use of qualified and non-qualified electronic attestations of attributes to allow European Business Wallet owners and their authorised representatives to authenticate themselves;
  - (i) transmit and receive electronic documents and data by means of a qualified electronic registered delivery service capable of supporting confidentiality and integrity;
  - (j) authorise multiple users to access and operate the European Business Wallet of the owner, and for the European Business Wallet owner to manage and revoke such authorisations;
  - (k) authorise European Business Wallet-relying parties to request electronic attestations of attributes issued to the European Business Wallet owner, and for the European Business Wallet owner to manage and revoke such authorisations;
  - (l) export their data, including issued European Business Wallet owner identification data, electronic attestations of attributes, communication logs, and interaction records, in a structured, commonly used and machine-readable



- format, at the request of the owner or in the event of termination of service or revocation of the notification of the provider of the European Business Wallet;
- (m) access a log of all transactions;
  - (n) access a common dashboard for accessing, storing and verifying communications exchanged through the qualified electronic registered delivery service referred to in point (i).
2. Providers of European Business Wallets may offer additional functionalities beyond those listed in paragraph 1 provided that such functionalities do not interfere with or compromise the confidentiality, availability, or integrity of the minimum core functionalities, and the reliability and interoperability of the European Business Wallets they provide.
  3. Providers of European Business Wallets shall enable the provision of the qualified electronic registered delivery service referred to in paragraph 1, point (i) as a standalone service to users of European Digital Identity Wallets.
  4. Providers of European Business Wallets shall implement the functionalities referred to in paragraph 1 in accordance with requirements set out in the Annex.
  5. The Commission shall, by means of implementing acts, establish a list of reference standards and where necessary, establish specifications and procedures for the core functionalities of European Business Wallets referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19.

## *Article 6*

### **Technical features for European Business Wallets**

1. Providers of European Business Wallets shall ensure that the European Business Wallets they provide support common protocols and interfaces:
  - (a) for the issuance of European Business Wallet owner identification data, qualified and non-qualified electronic attestations of attributes and qualified and non-qualified certificates to European Business Wallets;
  - (b) for European Business Wallet-relying parties to request and validate European Business Wallet owner identification data and electronic attestations of attributes;
  - (c) for the sharing and presenting to European Business Wallet-relying parties of European Business Wallet owner identification data, electronic attestation of attributes and of selectively disclosed data;
  - (d) to allow interaction with the European Business Wallets automatically without manual intervention or through direct user action;
  - (e) to securely onboard the European Business Wallet owner remotely via an authorised representative with an electronic identification means of that authorised representative which meets the requirements of Regulation (EU) No 910/2014 with regard to the assurance levels 'substantial' or 'high';
  - (f) for interaction between European Business Wallets, and between European Business Wallets and European Digital Identity Wallets for the purpose of

receiving, validating and sharing European Business Wallet owner identification data and electronic attestations of attributes in a secure manner;

- (g) for authenticating European Business Wallet-relying parties by implementing authentication mechanisms, where authentication is required;
- (h) for European Business Wallet-relying parties to verify the authenticity and validity of European Business Wallets, where the verification of the authenticity and validity is required;
- (i) for the provision of the qualified electronic registered delivery service referred to in Article 5(1), point (i), including an interface to the European Digital Directory established pursuant to Article 10;
- (j) for the assigning to each European Business Wallet owner, for the purposes of the qualified electronic registered delivery service referred to in Article 5(1), point (i) and the European Digital Directory referred to in Article 10, at least one unique digital address;
- (k) for the provision of wallet unit attestations to all European Business Wallet units, containing public keys and corresponding private keys protected by a wallet secure cryptographic device;
- (l) for the management of critical assets, for the use of at least one wallet secure cryptographic application and wallet secure cryptographic device and, where critical assets relate to performing electronic identification at assurance level substantial, for ensuring that such cryptographic operators or other operations processing critical assets are performed in accordance with the requirements for the characteristics and design of electronic identification means at assurance level substantial as set out in Commission Implementing Regulation (EU) 2015/1502.

2. Providers of European Business Wallets shall also:

- (a) ensure that the European Business Wallet owner identification data is digitally associated with the European Business Wallet of the owner;
- (b) ensure that, for the purposes of the functionality referred to in Article 5(1), point (j):
  - mappings between roles and attributes are verifiable, auditable, revocable and traceable to their legitimate issuers;
  - conflicts of roles, over-delegation, or expired authorisations are automatically detected and prevented in real time;
  - all authorisation logic is interoperable across Member States.
- (c) ensure security-by-design;
- (d) provide validation mechanisms, in order to ensure that the authenticity and validity of European Business Wallets can be verified;
- (e) provide a mechanism enabling European Business Wallet owners to easily request technical support and report technical problems or any other incidents having a negative impact on the use of European Business Wallets;
- (f) ensure that the validity of the European Business Wallets can be revoked in the following circumstances:

- upon the explicit request of the European Business Wallet owner;
  - where the security of the European Business Wallet has been compromised;
  - upon the permanent or temporary cessation of activity of the European Business Wallet owner;
  - where the provider of the European Business Wallet is not included in the list referred to in Article 12(5).
- (g) without undue delay, notify to the Commission:
- the mechanism allowing for the validation of the European Business Wallet owner identification data;
  - the mechanism by which to validate the authenticity and validity of European Business Wallets.
3. The Commission shall make available the information notified pursuant to paragraph 2, point (g) of this Article to the public through a secure channel, in electronically signed or sealed form suitable for automated processing.
  4. Providers of European Business Wallets shall implement the technical features provided for in paragraphs 1 and 2 in accordance with the requirements set out in the Annex.
  5. The Commission shall, by means of implementing acts, establish a list of reference standards and where necessary, establish specifications and procedures for the technical features of European Business Wallets provided for in paragraphs 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19.

## *Article 7*

### **Requirements and obligations for providers of European Business Wallets**

1. European Business Wallets shall be provided by providers of European Business Wallets that are included in the list established pursuant to Article 12(5).
2. Given the role of European Business Wallets in the Unions digital infrastructure, providers of European Business Wallets shall be established in the Union, have their principal place of business and main operations in the Union and not present a risk to the security of the Union. In particular they shall not be subject to control by a third country or by a third-country entity.
3. Providers of European Business Wallets shall comply with the requirements set out in Article 19a of Regulation (EU) 910/2014. That obligation shall not apply to providers of European Business Wallets that are qualified trust service providers.
4. Providers of European Business Wallets shall comply with the requirements set out in Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union.
5. Providers of European Business Wallets shall comply with applicable cybersecurity requirements laid down in Union and national law, including those relating to the identification of high-risk suppliers. Providers shall also ensure that their suppliers of software and security solutions comply with these requirements and conform to the relevant security standards and requirements.

6. Providers of European Business Wallets shall:
- (a) implement appropriate technical and organisational measures to ensure the confidentiality, integrity, authenticity, interoperability, and availability of the European Business Wallets they provide with other European Business Wallets and European Digital Identity Wallets;
  - (b) ensure that European Business Wallet owners are clearly informed, in a user-friendly, concise and accessible manner, about the terms and conditions of use of the European Business Wallet, including the scope and limitations of core and additional functionalities, cybersecurity standards, and the European Business Wallet owner's rights with regard to data portability, redress, and termination of service;
  - (c) ensure that authorised representatives of European Business Wallet owners are clearly informed, in a user-friendly, concise and accessible manner, about their rights and obligations in relation to their European Business Wallet unit, in particular, the right to request revocation of their wallet unit attestation, using the authentication mechanism provided in point 1 of the Annex;
  - (d) cooperate with the competent supervisory bodies referred to in Article 13(1), or with the Commission in the cases referred to in Article 13(10) and 14(1) and respond without undue delay to any request for information or documentation necessary to verify compliance with this Regulation;
  - (e) notify the relevant national supervisory bodies, or the Commission in the cases referred to in Article 14(1), of any substantive changes to their services or overall structure which may impact the compliance of the provider with this Regulation;
  - (f) notify European Business Wallet owners in the event of suspension, revocation or voluntary termination of the providers of European Business Wallet's services and of the removal of the provider of European Business Wallet from the list established pursuant to Article 12(5) and ensure the transfer or deletion of the European Business Wallet owner data in accordance with the European Business Wallet owners instructions, including European Business Wallet owner identification data;
  - (g) ensure that the information on European Business Wallet owners, pursuant to Article 10(2), is notified to the Commission and that the information initially submitted to the Commission is kept up to date and corroborated using the providers of the European Business Wallet owner identification data issuing the unique identifiers referred to in Article 8(5), point (b).

## *Article 8*

### **European Business Wallet owner identification data**

1. Providers of European Business Wallet owner identification data shall issue European Business Wallet owner identification data to European Business Wallets of European Business Wallet owners. Where European Business Wallet owners are Union entities, the Commission shall issue European Business Wallet owner identification data to the European Business Wallets of those Union entities.
2. Member States shall notify to the Commission the relevant authentic sources for the verification of the required attributes for the issuance of the European Business

Wallet owner identification data. On the basis of the information received pursuant to this paragraph, the Commission shall make available on the Commission's website, in a machine-readable format, a list of the notified relevant authentic sources.

3. European Business Wallet owner identification data shall be issued in a format compliant with one of the standards listed in Annex II of Commission Implementing Regulation (EU) 2024/2979 and as:
  - (a) qualified electronic attestations of attributes, when provided by qualified trust service providers;
  - (b) electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source, when provided by a public sector body so responsible;
  - (c) electronic attestations of attributes, when provided by the Commission.
4. European Business Wallet owner identification data issued by the Commission shall have the same legal effect as qualified electronic attestations of attributes and attestations of attributes issued by, or on behalf of, a public sector body responsible for an authentic source.
5. European Business Wallet owner identification data shall contain at least the following attributes:
  - (a) the official name of the economic operator or public sector body, as recorded in the relevant register or official record;
  - (b) the relevant unique identifier attributed in accordance with Article 9.
6. The Commission shall establish and maintain an attestation scheme for European Business Wallet owner identification data. That scheme shall be listed in the catalogue of schemes for the attestation of attributes referred to in Article 8 of Implementing Regulation (EU) 2025/1569.
7. The Commission may, by means of implementing acts, set out requirements for European Business Wallet owner identification data issued pursuant to this Article, including procedures for Member States to notify to the Commission the relevant authentic sources. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19.

## *Article 9*

### **Unique identifiers**

1. Where an economic operator has been attributed a European Unique Identifier, that identifier shall be used as the unique identifier referred to in Article 8(4), point (b) of this Regulation.
2. Where an economic operator or public sector body has not been attributed a European Unique Identifier, a unique identifier shall be created in accordance with the implementing act referred to in paragraph 4.
3. Where a public sector body is a Union entity, the Commission shall create and attribute a unique identifier to that Union entity in accordance with paragraph 4 of this Article.
4. The Commission shall, by means of implementing acts, establish specifications, requirements and procedures relating to the unique identifier referred to in paragraph



2 of this Article, including measures to ensure that European Business Wallet owners are not attributed more than one unique identifier. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19.

#### *Article 10*

##### **European Digital Directory**

1. The Commission shall establish, operate and maintain a European Digital Directory which shall act as the trusted source of information for European Business Wallet owners and shall take the form of a web application comprising of two interfaces:
  - (a) a machine-readable interface exposed through an API for automated system-to-system communication;
  - (b) a secure, web-based platform that provides access to authenticated and authorised users and system online portal for European Business Wallet users.
2. For the purpose of maintaining the European Digital Directory, providers of European Business Wallets shall, upon the provision of a European Business Wallet, provide to the Commission the categories of information set out in the implementing act referred to in paragraph 6
3. The Commission shall ensure that the relevant information shall be included in the European Digital Directory.
4. The Commission shall make the European Digital Directory only accessible to European Business Wallet owners and their authorised representatives and providers of European Business Wallets.
5. Any modification or revocation concerning the information referred to in paragraph 2 shall, without undue delay and in any event within one working day, be communicated by the providers of European Business Wallet directly to the Commission for the purpose of maintaining the European Digital Directory.
6. The Commission shall, by means of implementing acts, establish standards and technical specifications for the unique digital addresses and the categories of information to be communicated to the Commission for the purpose of the European Digital Directory. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19.

#### *Article 11*

##### **Notification of providers of European Business Wallets**

1. Entities that intend to provide European Business Wallets shall notify that intention together with the information listed in paragraph 2 to the competent supervisory body.
2. The notification referred to in paragraph 1 shall include the following information:
  - (a) the entity's legal name, any commercial names used, website URL, contact email, telephone number, and physical address;
  - (b) the entity's register number issued by a national register, where available

- (c) a description of how the core functionalities, set out in Article 5(1) shall be offered by the European Business Wallets the entity intends to provide;
  - (d) a description of any additional functionalities supported by the European Business Wallets the entity intends to provide;
  - (e) a declaration of conformity with the requirements of this Regulation.
- 3. Qualified trust service providers shall not be subject to the review and verification procedure set out in paragraphs 4 to 6. Upon submitting the information listed in paragraph 2, the competent supervisory body shall inform the Commission within two working days with a view to the addition of that provider to the list referred to in Article 12(5) and it may immediately offer European Business Wallets.
- 4. Upon receipt of a notification, the supervisory body shall have 30 days to review the information submitted.  
  
When that review leads the supervisory body to conclude that the information is complete and the description referred to in paragraph 2 point (c) appears to correspond to the requirements laid down in Article 5(1), it shall inform the Commission within two working days with a view to the addition of that provider to the list referred to in Article 12(5).
- 5. When that review leads the supervisory body to conclude that the information is not complete or the description referred to in paragraph 2 point (c) appears not to correspond to the requirements laid down in Article 5(1), it shall request additional information or explanations from the notifying entity and set a reasonable deadline, not exceeding 15 calendar days, for response. If that information or those explanations allow the supervisory body to conclude that the information is complete and the description referred to in paragraph 2 point (c) appears to correspond to the requirements laid down in Article 5(1), it shall inform the Commission within two working days with a view to the addition of that provider to the list referred to in Article 12(5). If not, or no response is received, the supervisory body shall inform the notifying entity that it will not be added to the list referred to in Article 12(5).
- 6. Where the supervisory body has not provided the notifying entity with a substantive response on the outcome of the review referred to in paragraph 4 within 30 calendar days of receiving the notification, the information shall be considered as complete and the description referred to in paragraph 2 point (c) shall be considered as appearing to correspond to the requirements laid down in Article 5(1), and the supervisory body shall inform the Commission within two working days with a view to the addition of that provider to the list referred to in Article 12(5)
- 7. Member States shall ensure that notifying entities have the right to an effective judicial remedy against a decision of the supervisory authority, without prejudice to any other administrative or non-judicial remedy, in cases where the supervisory authority refuses to list them as a provider of European Business Wallets or takes no decision within a reasonable timeframe.

## *Article 12*

### **List of notified providers of European Business Wallets**

1. Supervisory bodies shall inform the Commission of any changes to the information provided pursuant to Article 11, within 24 hours of having become aware of any changes.
2. The information provided by the supervisory bodies referred to in Article 11 and Article 12(1) shall include the following:
  - (a) the purpose of the submission, which may be one of the following:
    - the registration of a notified provider of European Business Wallets not previously present on the list referred to in paragraph 5;
    - a change to previously submitted information regarding providers of European Business Wallets currently present on the list referred to in paragraph 5;
    - a request to remove a provider of European Business Wallets from the list referred to in paragraph 5;
  - (b) name and, where applicable, the commercial name of the provider of European Business Wallets;
  - (c) the Member State in which the provider of European Business Wallets has its principal place of establishment;
  - (d) the name of the competent supervisory body;
  - (e) an indication whether the provider of European Business Wallets is a qualified trust service provider.
3. On the basis of the information received pursuant to this Article, the Commission shall establish and maintain on the Commission's website, in a machine-readable format, a list of providers of European Business Wallets.

## *Article 13*

### **Governance and supervision**

1. In each Member State, the supervisory bodies designated pursuant to Article 46a of Regulation (EU) No 910/2014 shall also be the supervisory bodies for the purposes of this Regulation.
2. Those supervisory bodies shall be responsible for supervisory tasks as regards providers of European Business Wallets having their principal place of establishment in that Member State.
3. Member States shall ensure that the supervisory bodies referred to in paragraph 1 have the necessary powers and adequate resources for the exercise of their tasks in an effective, efficient and independent manner.
4. The role of national supervisory bodies referred to in paragraph 1 shall be to:
  - (a) monitor compliance with the requirements laid down in this Regulation and take action, if necessary, in relation to providers of European Business Wallets, by means of ex post supervisory activities;

- (b) act as the main liaison office for providers of European Business Wallet owner identification data, facilitating access to information from relevant national authorities and registries, where necessary, for the issuance of European Business Wallet owner identification data and unique identifiers.
5. The tasks of the supervisory bodies referred to in paragraph 1 shall include the following:
- (a) review and assess the notifications submitted in accordance with Article 11;
  - (b) investigate substantiated claims, particularly those made by European Business Wallets owners, that a provider of European Business Wallets fails to comply with any of its obligations under this Regulation and to take action if necessary;
  - (c) verify the existence and correct application of termination plans where a provider of European Business Wallets ceases its activities, including how information is kept accessible;
  - (d) ensure that providers of European Business Wallets remedy any failure to fulfil the requirements laid down in this Regulation;
  - (e) impose penalties in accordance with paragraphs 6 to 9;
  - (f) inform the relevant competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 of the Member States concerned of any significant security breach or loss of integrity of which it becomes aware in the performance of its tasks and, in the case of a significant security breach or loss of integrity which concerns other Member States, to inform the single point of contact designated or established pursuant to Article 8(3) Directive (EU) 2022/2555 of the Member State concerned and the single points of contact designated pursuant to Article 46c(1) of Regulation (EU) No 910/2014 in the other Member States concerned, and to inform the public or require the provider of European Business Wallets to do so where the supervisory body determines that disclosure of the breach of security or loss of integrity would be in the public interest;
  - (g) cooperate with supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679, in particular, by informing them, without undue delay, where personal data protection rules appear to have been breached and about security breaches which appear to constitute personal data breaches;
  - (h) cooperate, as appropriate, with other national supervisory bodies;
  - (i) set up and ensure clear publicity of a complaint mechanism whereby complaints can be filed by providers of European Business Wallets in accordance with Article 11(7);
  - (j) report to the Commission on its main activities;
  - (k) revoke the inclusion in the list established pursuant to Article 12(5) of a provider of European Business Wallets if the supervisory body determines that the provider no longer meets the requirements laid down in this Regulation or that the provider has failed to comply with the obligations imposed by this Regulation;
  - (l) cooperate with the supervisory authorities designated pursuant to Article 46b of Regulation (EU) No 910/2014 by the Member States, in particular, to ensure

that economic operators established outside the Union are issued only one set of European Business Wallet owner identification data and European business Wallet unique identifier.

6. Member States shall lay down the rules allowing the supervisory body referred to in paragraph 1 of this Article to impose penalties applicable to infringements of this Regulation and shall take all measures necessary to ensure that they are implemented. Those penalties shall be effective, proportionate and dissuasive. Those rules shall not affect Article 31 of Directive (EU) 2022/2555 and Article 83 of Regulation (EU) 2016/679.
7. By [Publications Office, insert the date 12 months after the entry into force of this Regulation] Member States shall notify the Commission of the rules laid down by Member States in accordance with paragraph 6 and shall notify the Commission without delay of any subsequent amendments to the rules. The Commission shall regularly update and maintain an easily accessible public register of those rules.
8. Member States shall take into account the following non-exhaustive and indicative criteria for the imposition of penalties in accordance with paragraph 6:
  - (a) the nature, gravity, scale and duration of the infringement;
  - (b) any action taken by the infringing party to mitigate or remedy the damage caused by the infringement;
  - (c) any previous infringements by the infringing party;
  - (d) the financial benefits gained or losses avoided by the infringing party due to the infringement, insofar as such benefits or losses can be reliably established;
  - (e) any other aggravating or mitigating factor applicable to the circumstances of the case;
  - (f) the infringing party's total annual turnover in the preceding financial year in the Union.

Member States shall ensure that infringements of this Regulation committed by providers of European Business Wallets be subject to administrative fines of a maximum of 2% of the total worldwide annual turnover in the preceding financial year.

9. Where the legal system of a Member State does not provide for administrative fines being imposed by administrative authorities, fines initiated by the supervisory body and imposed by competent national courts, which have an equivalent effect to the administrative fines imposed by supervisory bodies, shall be considered to comply with the requirements laid down in paragraph 6. In any event, the fines imposed shall be effective, proportionate and dissuasive. That Member State shall notify to the Commission the provisions of the laws which it adopts pursuant to this paragraph by [Publications Office, insert the date 12 months after the entry into force of this Regulation] and, without delay, any subsequent amendment law or amendment affecting them.
10. In circumstances which justify an immediate intervention to preserve the proper functioning of the internal market and where the Commission has sufficient reason to consider that the European Business Wallets provided by a provider are non-compliant with the requirements laid down in this Regulation and no effective measures have been taken by the competent supervisory authority, the Commission



shall carry out an evaluation of compliance. The Commission shall inform the relevant authorities accordingly and the provider shall cooperate as necessary.

11. Based on the evaluation, the Commission may decide that a corrective or restrictive measure is necessary, and after consulting the Member States concerned and the provider, the Commission may determine the appropriate course of action. The Commission shall take into account the nature and severity of the non-compliance, as well as the potential impact on the internal market and the rights of economic operators.
12. On the basis of the consultation, the Commission may adopt implementing acts to provide for corrective or restrictive measures, including temporarily suspending the provider from the list of notified providers or requiring the provider to take specific actions to bring the European Business Wallets into compliance with the Regulation. Those implementing acts shall be adopted in accordance with the examination procedure.
13. The Commission shall immediately communicate the implementing acts to the provider and Member States shall implement those implementing acts without delay and inform the Commission accordingly. These measures shall be applicable for the duration of the exceptional situation that justified the Commission's intervention, provided that the European Business Wallets concerned are not brought into compliance with this Regulation.

#### *Article 14*

#### ***European Digital Identity Cooperation Group***

The European Digital Identity Cooperation Group established pursuant to Article 46e of Regulation (EU) No 910/2014 shall be responsible for facilitating cooperation and information sharing among Member States and the Commission on matters related to the European Business Wallets. This shall include sharing best practices, discussing technical and operational issues, and coordinating efforts to ensure the proper implementation and functioning of the European Business Wallets.

#### *Article 15*

#### **Governance and supervision of Union entities that are providers of European Business Wallets**

1. Where a Union entity is a provider of European Business Wallets the Commission shall be its supervisory body.
  2. The role of the Commission acting as a supervisory body in accordance with paragraph 1 shall be to monitor compliance with the requirements laid down in this Regulation and take action, if necessary, in relation to providers of European Business Wallets, by means of ex post supervisory activities.
  3. When acting as a supervisory body in accordance with paragraph 1, the Commission shall perform the tasks referred to in Article 13(5) points a, b, c, d, h and k.
- The Commission shall prepare a report on its main activities in this respect.

## Chapter III – Acceptance of the European Business Wallets

### Article 16

#### Obligations on public sector bodies

4. By [Publications Office, please insert the date 24 months after the entry into force of this Regulation] public sector bodies shall enable economic operators to take the following actions by using the core functionalities of European Business Wallets as set out in Article 5(1):

- (a) identify and authenticate;
- (b) sign or seal;
- (c) submit documents;
- (d) send or receive notifications.

The actions listed in points (a) to (d) of the first subparagraph shall take place for the purpose of meeting a reporting obligation or fulfilling an administrative procedure.

5. For the purposes of paragraph 1, points (c) and (d), public sector bodies shall have European Business Wallets, including the qualified electronic registered delivery service referred to in Article 5(1), point (i).

6. By way of derogation from paragraph 2 and until [Publications Office, insert the date 36 months after entry into force of this Regulation], public sector bodies may choose not to offer the qualified electronic registered delivery service referred to in Article 5(1), point (i), and support instead other existing alternative solutions which enable economic operators to take the actions listed in paragraph 1, points (c) and (d), provided those solutions:

- (a) comply with the requirements applicable to qualified electronic registered delivery services set out in Regulation (EU) No 910/2014;
- (b) offer a gateway that enables European Business Wallet owners to submit documents and send and receive notifications using the qualified electronic registered delivery service referred to in Article 5(1), point (i).

After the expiry of the derogation period laid down in this paragraph, public sector bodies may continue to support the alternative solutions referred to in that subparagraph but shall, in accordance with paragraph 2, have European Business Wallets, including the qualified electronic registered delivery service referred to in paragraph 1 of Article 5(1), point (i).

## Chapter IV - International aspects

### Article 17

#### Business wallets and other similar instruments and frameworks offered in third countries

1. The Commission may adopt implementing acts establishing that business wallets or systems offering similar functions that are issued by providers established in third countries are to be considered as offering assurances that are equivalent to European

Business Wallets issued in accordance with this Regulation, provided that such business wallets or systems are interoperable with the trust framework laid down in Regulation (EU) 910/2014 and allow for the support of at least an identification and authentication functionality and the exchange of electronic attestations of attributes. Such implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19.

2. The Commission may adopt implementing acts establishing that third country frameworks for systems offering similar functions as the European Business Wallets are to be considered as offering assurances that are equivalent to European Business Wallets issued in accordance with this Regulation, provided that the systems provided under that framework are interoperable with the trust framework laid down in Regulation (EU) 910/2014 and allow for the support of at least an identification and authentication functionality and the exchange of electronic attestations of attributes. Such implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19.
3. Prior to the adoption of the implementing acts referred to in paragraphs 1 and 2, the Commission shall assess whether the assurances can be considered as equivalent to the requirements under this Regulation.
4. The Commission shall, where available information reveals that those assurances can no longer be considered as equivalent to the requirements under this Regulation, to the extent necessary, repeal, amend or suspend the act referred to in paragraphs 1 and 2 by means of an implementing act.
5. The Commission shall publish on its website a list of frameworks, business wallets or systems offering similar functions that are issued by providers established in third countries in relation to which the Commission has adopted an implementing act pursuant to this Article.

#### *Article 18*

#### **Issuing of European Business Wallets to economic operators established outside the Union**

1. Providers of European Business Wallets may provide European Business Wallets to economic operators established in a third country under the condition that such economic operators have been issued European Business Wallet owner identification data and a unique identifier in accordance with this Article.
2. For the purposes of this Article, economic operators shall request only one set of European Business Wallet owner identification data from one provider of European Business Wallet owner identification data.
3. Where an economic operator established outside the Union requests a European Business Wallet, the provider of European Business Wallets shall notify this request to the supervisory body of the Member State in which the provider is notified.
4. Providers of European Business Wallets shall request European Business Wallet owner identification data from a provider of European Business Wallet owner identification data on behalf of the economic operator established in a third country.
5. Providers of European Business Wallet owner identification data may issue European Business Wallet owner identification data and unique identifiers pursuant

to Articles 8 and 9 to economic operators established outside the Union, provided that:

- (a) the identity proofing and verification of those economic operators fulfils one or, when needed, a combination, of the methods for verification of identity set out in Article 24 (1a) of Regulation (EU) No 910/2014;
  - (b) the economic operator has not been issued another set of European Business Wallet owner identification data.
6. Member States shall cooperate to ensure that providers of European Business Wallet owner identification data can verify that an economic operator established outside the Union has not yet been issued European Business Wallet owner identification data.

## Chapter V – Final provisions

### *Article 19*

#### **Committee procedure**

The Commission shall be assisted by the committee established by Article 48 of Regulation (EU) No 910/2014. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

### *Article 20*

#### **Amendment to Regulation (EU) No 910/2014**

In Regulation (EU) No 910/2014, Article 5a is amended as follows:

(1) paragraph 1 is replaced by the following:

‘1. For the purpose of ensuring that all natural persons in the Union have secure, trusted and seamless cross-border access to public and private services, while having full control over their data, each Member State shall provide at least one European Digital Identity Wallet within 24 months of the date of entry into force of the implementing acts referred to in paragraph 23 of this Article and in Article 5c(6).’

(2) in paragraph 5 point (f) is replaced by the following:

‘(f) ensure that the person identification data, which is available from the electronic identification scheme under which the European Digital Identity Wallet is provided, uniquely represents the natural person or the natural person representing the natural or legal person, and is associated with that European Digital Identity Wallet;’;

(3) in paragraph 9 point c) is replaced by the following:

‘(c) upon the death of the user.’;

(4) Paragraph 15 is replaced by the following:

‘15. The use of European Digital Identity Wallets shall be voluntary. Access to public and private services, access to the labour market and freedom to conduct business shall not in any way be restricted or made disadvantageous to natural persons that do not use European Digital Identity Wallets. It shall remain possible to access public and private services by other existing identification and authentication means.’.

## Article 21

### Evaluation and review

7. The Commission shall review the application of this Regulation and shall, by [Publications Office, insert the date – 3 years after entry into force], submit a report to the European Parliament and to the Council. The report shall evaluate the effectiveness of the provisions of this Regulation with regard to facilitating the submission of electronic documents and electronic attestations to public sector bodies, by the usage of the European Business Wallets, as well as technological, market, and legal developments. The report shall also assess whether it is necessary to modify the scope of this Regulation or its specific provisions to set out an obligation for the use of the European Business Wallets to address the risks of legal fragmentation.
8. The report referred to in paragraph 1 shall include the following aspects:
  - (a) the minimum core functionalities of European Business Wallets;
  - (b) the level of compliance of providers of European Business Wallets and the notification procedure and criteria established in Article 11;
  - (c) the application and functioning of the rules on penalties laid down by the Member States pursuant to Article 13;
  - (d) the detailed requirements and technical specifications for the qualified electronic registered delivery service referred to in Article 5(1) point I;

No later than one year before the report referred to in paragraph 1 is due, Member States shall provide the Commission with the information necessary for the preparation of the reports.

## Article 22

### Entry into force and application

This Regulation shall enter into force on the twentieth day following that of its publication in the *Official Journal of the European Union*.

It shall apply from [Publications Office, insert the date – 1 year after entry into force].

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at Brussels,

*For the European Parliament*  
*The President*

*For the Council*  
*The President*



## **LEGISLATIVE FINANCIAL AND DIGITAL STATEMENT**

1.	FRAMEWORK OF THE PROPOSAL/INITIATIVE .....	3
1.1.	Title of the proposal/initiative .....	3
1.2.	Policy area(s) concerned .....	3
1.3.	Objective(s) .....	3
1.3.1.	General objective(s) .....	3
1.3.2.	Specific objective(s) .....	3
1.3.3.	Expected result(s) and impact .....	3
1.3.4.	Indicators of performance .....	3
1.4.	The proposal/initiative relates to: .....	4
1.5.	Grounds for the proposal/initiative .....	4
1.5.1.	Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative .....	4
1.5.2.	Added value of EU involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this section 'added value of EU involvement' is the value resulting from EU action, that is additional to the value that would have been otherwise created by Member States alone. ....	4
1.5.3.	Lessons learned from similar experiences in the past .....	4
1.5.4.	Compatibility with the multiannual financial framework and possible synergies with other appropriate instruments .....	5
1.5.5.	Assessment of the different available financing options, including scope for redeployment .....	5
1.6.	Duration of the proposal/initiative and of its financial impact .....	6
1.7.	Method(s) of budget implementation planned .....	6
2.	MANAGEMENT MEASURES .....	8
2.1.	Monitoring and reporting rules .....	8
2.2.	Management and control system(s) .....	8
2.2.1.	Justification of the budget implementation method(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed .....	8
2.2.2.	Information concerning the risks identified and the internal control system(s) set up to mitigate them .....	8
2.2.3.	Estimation and justification of the cost-effectiveness of the controls (ratio between the control costs and the value of the related funds managed), and assessment of the expected levels of risk of error (at payment & at closure) .....	8
2.3.	Measures to prevent fraud and irregularities .....	9
3.	ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE .....	10
3.1.	Heading(s) of the multiannual financial framework and expenditure budget line(s) affected .....	10

3.2.	Estimated financial impact of the proposal on appropriations.....	12
3.2.1.	Summary of estimated impact on operational appropriations.....	12
3.2.1.1.	Appropriations from voted budget .....	12
3.2.1.2.	Appropriations from external assigned revenues .....	17
3.2.2.	Estimated output funded from operational appropriations.....	22
3.2.3.	Summary of estimated impact on administrative appropriations.....	24
3.2.3.1.	Appropriations from voted budget .....	24
3.2.3.2.	Appropriations from external assigned revenues .....	24
3.2.3.3.	Total appropriations .....	24
3.2.4.	Estimated requirements of human resources.....	25
3.2.4.1.	Financed from voted budget.....	25
3.2.4.2.	Financed from external assigned revenues .....	26
3.2.4.3.	Total requirements of human resources .....	26
3.2.5.	Overview of estimated impact on digital technology-related investments .....	28
3.2.6.	Compatibility with the current multiannual financial framework.....	28
3.2.7.	Third-party contributions .....	28
3.3.	Estimated impact on revenue .....	29
4.	DIGITAL DIMENSIONS .....	29
4.1.	Requirements of digital relevance.....	30
4.2.	Data .....	30
4.3.	Digital solutions .....	31
4.4.	Interoperability assessment .....	31
4.5.	Measures to support digital implementation .....	32

## 1. FRAMEWORK OF THE PROPOSAL/INITIATIVE

### 1.1. Title of the proposal/initiative

Regulation of the European Parliament and the Council on the establishment of the European Business Wallets

### 1.2. Policy area(s) concerned

Communications Networks, Content and Technology  
Internal Market

### 1.3. Objective(s)

#### 1.3.1. General objective(s)

The general objective of this initiative is to ensure the proper functioning of the internal market by meeting economic operators' and public sector bodies' specific needs in the area of digital identification and trust services and providing them with a harmonised, trusted, and user-friendly instrument for secure and legally valid identification, authentication and data exchange

#### 1.3.2. Specific objective(s)

##### Specific objective No 1

Reduce administrative burdens, streamline compliance processes, and improve service delivery.

##### Specific objective No 2

To ensure economic operators and public sector bodies have access to secure and trusted digital identification across borders, meeting user needs and market demand.

#### 1.3.3. Expected result(s) and impact

*Specify the effects which the proposal/initiative should have on the beneficiaries/groups targeted.*

Overall, the biggest main expected beneficiaries of the initiative are economic operators and public sector bodies. By establishing a harmonised and trusted digital framework for business identification, authentication, and document exchange and storage, the initiative will reduce administrative burdens and compliance costs both at national and EU level. The European Business Wallets will allow companies to interact seamlessly with public authorities and business partners across borders, eliminating repetitive submissions of data and accelerating key processes such as registration, licensing, and reporting. SMEs and micro-enterprises in particular will benefit from simplified, secure, and interoperable digital channels, freeing resources for innovation, growth, and cross-border expansion.

Public sector bodies will gain in efficiency, quality, and reliability of service delivery. The Business Wallets will streamline administrative procedures by enabling automation of verification and document handling, reducing manual intervention, duplication, and error rates. The secure communication channel will improve data quality and transparency, supporting better regulatory oversight and facilitating the use of innovative RegTech solutions.

#### 1.3.4. Indicators of performance

*Specify the indicators for monitoring progress and achievements.*

To ensure consistency and proportionality, the monitoring framework draws on the three-pillar structure referenced in the impact assessment for the revision of the eIDAS Regulation, implementation, application, and contextual indicators, and adapts it to the specific scope of the European Business Wallets. This ensures alignment while avoiding duplication of monitoring obligations and respecting Better Regulation principles, including proportionality and re-use of existing data streams. Additionally, a set of additional indicators, specifically linked to the Specific Objectives will be leveraged to assess the outcomes of the initiative via proxy-indicators. These broader macro-economic and administrative-burden trends remain contextual and will be interpreted alongside eIDAS data to support statistical inference rather than implying direct causality.

The new set of indicators linked to the Specific Objectives is reported underneath:

Monitoring and evaluation aspect and relevant objectives	Indicator(s)	Responsibility for collection	Source(s)
<b>SO1: Reduce administrative burdens, streamline compliance processes, and improve service delivery.</b>			
To reduce the administrative burden of regulatory compliance and reporting requirements on businesses through demonstrable economic benefits	Quantifiable reduction in the burden of government regulation indicator	European Commission	Single Market and Competitiveness Scoreboard <sup>14</sup>
To improve public service delivery	Measured improvements in Digital Public Services for Business indicators under the eGov benchmark, particularly in respect of online service delivery and interoperability signifiers (specific indicators: (cross-border) online availability; (cross-border) eID; pre-filled forms; OOTS)	European Commission	eGovernment benchmark study feeding the Digital Decade Policy Programme
To enhance European competitiveness	Measurable improvements in the exports of goods to other EU countries by SMEs in the industrial sector (% of SMEs)	European Commission	Single Market and Competitiveness Scoreboard
<b>SO2: To ensure economic operators and public sector bodies have access to secure and trusted digital identification across borders, meeting user needs and market demand.</b>			
To develop a market for secure digital identification and trust services between	Number of compliant and notified European Business Wallet providers, including Qualified Trust Service Providers	Supervisory bodies	Data reported to European Commission European Digital

<sup>14</sup> Plus any potential KPI on administrative burden reduction following the review of the Digital Decade Policy Programme

Monitoring and evaluation aspect and relevant objectives	Indicator(s)	Responsibility for collection	Source(s)
economic operators and public sector bodies			Directory
To ensure that available solutions are trusted and secure and comply with all requirements to provide European Business Wallets	<p>Number of withdrawn authorisations of notified European Business Wallet providers, excluding any providers who have voluntarily ceased their commercial provision of business wallets and related services</p> <p>Number and level of penalties imposed on European Business Wallet providers</p>	Supervisory bodies	Data reported to European Commission
To stimulate adoption of the European Business Wallet across all sectors of the economy	Number of European Business Wallets issued to economic operators and public sector bodies and registered in the European Digital Directory <sup>15</sup>	European Commission	European Digital Directory

#### 1.4. The proposal/initiative relates to:

- ☐ a new action
- ☐ a new action following a pilot project / preparatory action<sup>16</sup>
- ☒ the extension of an existing action
- ☐ a merger or redirection of one or more actions towards another/a new action

#### 1.5. Grounds for the proposal/initiative

##### 1.5.1. Requirement(s) to be met in the short or long term including a detailed timeline for roll-out of the implementation of the initiative

The Regulation will require public sector bodies to accept European Business Wallets for the purposes of identification and authentication, signing or sealing documents, submitting documents, and sending or receiving notifications. Public sector bodies have 24 months after entry into force of the Regulation to ensure they can accept Business Wallets for these purposes. For a transition period of up to 36 months after entry into force, public sector bodies may continue to support other existing communication solutions instead of implementing the Business Wallets' communication channel, provided that these solutions comply with applicable requirements set out in Regulation (EU) 910/2014 and offer a gateway between these existing solutions and the communication channel of the Business Wallets. After this

<sup>15</sup> The number of wallets is not necessarily equivalent to number of owners because one owner attributed with one unique identifier may have multiple wallets registered to them, but it will be a good approximation to determine the levels of usage

<sup>16</sup> As referred to in Article 58(2), point (a) or (b) of the Financial Regulation.



transition period, public sector bodies will have to support the Business Wallets' communication channel, either instead of or in addition to other eIDAS-compliant solutions.

*1.5.2. Added value of EU involvement (it may result from different factors, e.g. coordination gains, legal certainty, greater effectiveness or complementarities). For the purposes of this section 'added value of EU involvement' is the value resulting from EU action, that is additional to the value that would have been otherwise created by Member States alone.*

#### Reasons for action at EU level (ex-ante)

Divergent national digital identity solutions hinder the freedom of establishment and the freedom to provide services, undermining the optimal functioning of the Single Market. The current fragmentation creates duplication, delays, and additional costs for economic operators especially cross-border. Uneven levels of digitalisation of public sector bodies may also distort competition, giving economic operators in more advanced Member States a procedural advantage and weakening the level playing field in the Single Market.

The functioning of the internal market relies on uniform and consistent rules applied across all relevant public sector bodies performing equivalent functions or providing comparable services. The Commission often carry out similar activities to national public sector bodies and have key supervisory and regulatory roles. Thus, their involvement in supporting the proper functioning of the Single Market is necessary. Excluding them would create regulatory gaps, fragmentation and uneven application of the rules, thereby undermining the Business Wallet's objective of safeguarding the integrity, stability and resilience of the internal market. In addition, simplification remains a key driver of the EU's commitment to building a bolder, simpler, and faster Union, as outlined in the 2025 Work Programme. A competitive and well-functioning Single Market requires active participation from both national and EU-level authorities, with the latter leading by example. Accordingly, the Commission should adopt and use the European Business Wallet, extending simplification and efficiency to their interactions with economic operators.

#### Expected generated EU added value (ex-post)

The European Business Wallets will eliminate duplication and reduce compliance costs, while also improve transparency, data quality, and provide public sector bodies with more reliable information, enhancing service delivery. At the same time, EU-level harmonisation prevents dependency on high-risk providers, strengthens the resilience of critical infrastructures, and consolidates the Union's digital sovereignty. Beyond the internal market, the initiative can also enhance the Union's role as a global standard-setter for trusted digital infrastructures, supporting European competitiveness in international trade.

*1.5.3. Lessons learned from similar experiences in the past*

The European Business Wallets proposal builds on and extends the ecosystem of trust established under the European Digital Identity Framework - Regulation (EU) 910/2014, the legal reference in the EU on electronic identification and trust services for electronic transactions in the internal market, as amended by Regulation (EU) 2024/1183. This framework - a state-of-the-art, privacy-friendly and interoperable system for digital identification empowering citizens and legal entities to share data securely across borders - represents already a major milestone in the EU simplification agenda.

The European Business Wallets proposal aims at complementing the European Digital Identity Wallets by introducing a market-driven digital framework designed for the specific needs of businesses transactions, including traceability, the digital management of

representation rights and mandates, and a secure channel for exchanging official documents and attestations supported by a common directory. All this will be achieved while guaranteeing full interoperability with the European Digital Identity Wallets

Recent technological and societal developments require a new harmonised and digital approach to business-to-government and business-to-business interactions. AI, cloud computing and secure digital identity are moving at an unprecedented pace, affecting the way of doing business in Europe: processes have shifted from being document-based to automated and data-driven. For instance, 91% of scaleups consider digital technologies critical to their growth. These developments, combined with the EU's strategic priorities for competitiveness, digital sovereignty, simplification and digital-by-default public services, create the need for agile solutions that can support trusted cross-border business transactions at scale.

As a consequence, the demand for means to identify and exchange and store different business credentials, securely and with full legal effect across border has increased radically.

The Regulation also builds on the achievements of Directive (EU) 2025/25, which introduced the EU Company Certificate and digital EU power of attorney. These pioneering tools aim to ease administrative burdens in cross-border operations for Union companies by reducing fragmentation. This regulation takes the next step to offer a tool for enabling companies to seamlessly exchange EU Company Certificates and digital powers of attorneys via European Business Wallets.

#### *1.5.4. Compatibility with the multiannual financial framework and possible synergies with other appropriate instruments*

The initiative supports the EU's simplification and competitiveness goals by providing economic operators with tools such as the Business Wallets, enabling trusted, secure, and user-friendly compliance with administrative requirements through harmonised identification, authentication, and data exchange. Hence, it is fully in line with the objectives of the MFF.

The inclusion of the Commission will have financial implications, which will be predominantly covered by the EU budget under the Multiannual Financial Framework (MFF) 2028-2034. These costs are mainly associated with the implementation and use of the European Business Wallets, the establishment and maintenance of the European Digital Directory within the Commission, the integration of these with existing IT systems and the establishment of supervisory activities related to the European Business Wallets.

The estimated direct costs for the Commission as user amount to approximately €7 million during the first year due to expenditure for initial implementation (procurement process), licensing fee and maintenance costs for the European Business Wallet. As of the second year, the Commission will incur additional €5 million in recurring annual costs. For the European Digital Directory, the setup cost is estimated at just under €2 million, with annual maintenance costs projected at €1.7 million in the second year and €1.3 million in subsequent years.

In addition, potential costs for integrating the Business Wallets into all the relevant IT systems are estimated at €33.8 million for the first year and €7.5 million for the second year. As the systems are already in place, the costs are related to the first two years as it is an integration and not a development of a new system.

Synergies with other instruments are illustrated as follows:

- The Single Digital Gateway (SDG) and its Once-Only Technical System (OOTS) implement the “once-only” principle, requiring authorities to reuse data already held in another Member State without repeated submissions by businesses. The European Business Wallets will complement the SDG and OOTS by providing trusted identification and authentication of economic operators and public administrations and a secure exchange layer that enables businesses and public sector bodies to share and reuse verified data and official attestations seamlessly across borders.
- The Digital Product Passport (DPP), central to the EU’s circular economy agenda, depends on trusted access to conformity and sustainability data. The Business Wallets can prove legal identity and any granted access rights, allow conformity declarations to be signed and sealed, and ensure product data is exchanged securely and verifiably across borders.
- The Interoperable Europe Act (IEA) establishes the framework for cross-border interoperability of public services. The Business Wallets will complement this by serving as a trusted infrastructure that administrations can integrate into digital-by-default service delivery, reinforcing the removal of technical and organisational barriers.
- The upcoming proposal on the 28th Regime corporate legal framework will provide simple, flexible and fast procedures for companies to set up and operate and attract investment in the EU through digital solutions. It will ensure inter-operability with the business wallet and ensure that digital tools such as the EU Company certificate and the EU digital Power of Attorney are compatible with the Business Wallet so that companies can use these with their Business Wallet.
- The VAT in the Digital Age (ViDA) package modernises VAT reporting, introduces mandatory e-invoicing across borders and strengthens fraud prevention. The Business Wallets will enable secure storage and verifiable exchange of VAT attestations and transaction data, thereby supporting real-time reporting and trusted invoicing.

*1.5.5. Assessment of the different available financing options, including scope for redeployment*

The staff requested in the amount of 20 FTEs will be redeployed by existing allocations of the DG that is assigned to the management of the action or other Commission services.

**1.6. Duration of the proposal/initiative and of its financial impact**

☐ **limited duration**

- ☐ in effect from [DD/MM]YYYY to [DD/MM]YYYY
- ☐ financial impact from YYYY to YYYY for commitment appropriations and from YYYY to YYYY for payment appropriations.

☒ **unlimited duration**

- Implementation with a start-up period from 2028 to 2029,
- followed by full-scale operation.

**1.7. Method(s) of budget implementation planned**

☒ **Direct management** by the Commission

- ☒ by its departments, including by its staff in the Union delegations;
- ☒ by the executive agencies

☐ **Shared management** with the Member States

☐ **Indirect management** by entrusting budget implementation tasks to:

- ☐ third countries or the bodies they have designated
- ☐ international organisations and their agencies (to be specified)
- ☐ the European Investment Bank and the European Investment Fund
- ☐ bodies referred to in Articles 70 and 71 of the Financial Regulation
- ☐ public law bodies
- ☐ bodies governed by private law with a public service mission to the extent that they are provided with adequate financial guarantees
- ☐ bodies governed by the private law of a Member State that are entrusted with the implementation of a public-private partnership and that are provided with adequate financial guarantees
- ☐ bodies or persons entrusted with the implementation of specific actions in the common foreign and security policy pursuant to Title V of the Treaty on European Union, and identified in the relevant basic act
- ☐ bodies established in a Member State, governed by the private law of a Member State or Union law and eligible to be entrusted, in accordance with sector-specific rules, with the implementation of Union funds or budgetary guarantees, to the extent that such bodies are controlled by public law bodies or by bodies governed by private law with a public service mission, and are provided with adequate financial guarantees in the form of joint and several liability by the controlling bodies or equivalent financial guarantees and which may be, for each action, limited to the maximum amount of the Union support.

## **2. MANAGEMENT MEASURES**

### **2.1. Monitoring and reporting rules**

The Regulation will be reviewed three years after its full application. The Commission must report on the findings to the European Parliament and to the Council.

### **2.2. Management and control system(s)**

#### **2.2.1. *Justification of the budget implementation method(s), the funding implementation mechanism(s), the payment modalities and the control strategy proposed***

The Regulation establishes harmonised rules for the provision of eID and QERDS to economic operators and public sector bodies in the internal market while ensuring the respect of trust and users' control over their own data. These new rules require the development of technical specifications and standards, and supervision and coordination of the activities of European Union Institutions, Bodies, Offices and Agencies.

In addition, there is also a need to take into consideration the resources needed to communicate and coordinate with third countries on interoperability and equivalence of third country solutions.

In order to face these tasks, it is necessary to appropriately resource the Commission's services. The enforcement of the provisions of the new Regulation is estimated to require 20 FTEs.

#### **2.2.2. *Information concerning the risks identified and the internal control system(s) set up to mitigate them***

One of the main issues leading to shortcomings in the current legislative framework is the lack of harmonisation of national systems in the context of business-to-government interactions, which results in red tape and administrative burdens, particularly across borders. To mitigate this issue, the initiative builds on early engagement with potential providers and coordination with ongoing Large-Scale Pilots to ensure technological readiness and interoperability. In parallel, close cooperation with Member States and related EU initiatives will help prevent further fragmentation and foster a coherent, competitive, and trusted provider ecosystem within the Single Market.

#### **2.2.3. *Estimation and justification of the cost-effectiveness of the controls (ratio between the control costs and the value of the related funds managed), and assessment of the expected levels of risk of error (at payment & at closure)***

For the meeting expenditure of the expert group, given the low value per transaction (e.g. refunding travel costs for a delegate for a meeting if the meeting is physical), standard internal control procedures seem sufficient.

Also for pilot projects, DG CNECT standard procedures should be sufficient.

### **2.3. Measures to prevent fraud and irregularities**

The existing fraud prevention measures applicable to the Commission will cover the additional appropriations necessary for this Regulation.



### 3. ESTIMATED FINANCIAL IMPACT OF THE PROPOSAL/INITIATIVE

#### 3.1. Heading(s) of the multiannual financial framework and expenditure budget line(s) affected

- Existing budget lines

*In order of multiannual financial framework headings and budget lines.*

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff. <sup>17</sup>	from EFTA countries <sup>18</sup>	from candidate countries and potential candidates <sup>19</sup>	From other third countries	other assigned revenue
	MFF headings and budget lines to be determined <sup>20</sup>	Diff./Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO
	[XX.YY.YY.YY]	Diff./Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO
	[XX.YY.YY.YY]	Diff./Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO

- New budget lines requested

*In order of multiannual financial framework headings and budget lines.*

Heading of multiannual financial framework	Budget line	Type of expenditure	Contribution			
	Number	Diff./Non-diff.	from EFTA countries	from candidate countries and potential candidates	from other third countries	other assigned revenue
	[XX.YY.YY.YY]	Diff./Non-diff.	YES/NO	YES/NO	YES/NO	YES/NO

<sup>17</sup> Diff. = Differentiated appropriations / Non-diff. = Non-differentiated appropriations.

<sup>18</sup> EFTA: European Free Trade Association.

<sup>19</sup> Candidate countries and, where applicable, potential candidates from the Western Balkans.

<sup>20</sup> Budget lines for the new MFF are not yet known.

	[XX.YY.YY.YY]	Diff./Non -diff.	YES/NO	YES/NO	YES/NO	YES/NO
	[XX.YY.YY.YY]	Diff./Non -diff.	YES/NO	YES/NO	YES/NO	YES/NO

### 3.2. Estimated financial impact of the proposal on appropriations

#### 3.2.1. Summary of estimated impact on operational appropriations

- ☐ The proposal/initiative does not require the use of operational appropriations
- ☒ The proposal/initiative requires the use of operational appropriations, as explained below
- The amounts indicated are strictly indicative, pending the final outcome of the MFF negotiations 2028-2034.
- This initiative will be financed by redeployment within the operational programmes of the next MFF, and partially by administrative expenditure. At this stage, it is not possible to indicate accurately the contribution from each MFF heading and programme, while it is expected that a significant contribution will come from programmes under heading 2 of the 2028-2034 MFF (e.g. the European Competitiveness Fund).

–

#### 3.2.1.1. Appropriations from voted budget

EUR million (to three decimal places)

		First Year	Second Year	Following Years (yearly amount)
<b>TOTAL appropriations under HEADINGS 1 to 4</b>	<b>Commitments</b>	<b>45,442</b>	<b>16,867</b>	<b>8,929</b>
<b>of the multiannual financial framework</b>	<b>Payments</b>	<b>45,442</b>	<b>16,867</b>	<b>8,929</b>

The figures as shown in the table above are strictly indicative pending the outcome of the MFF negotiations.

		First Year	Second Year	Following Years (yearly amount)
<b>TOTAL appropriations under HEADINGS 1 to 4</b>	Commitments	<b>45.442</b>	<b>16.867</b>	<b>8.929</b>
of the multiannual financial framework	Payments	<b>45.442</b>	<b>16.867</b>	<b>8.929</b>

The figures as shown in the table above are strictly indicative pending the outcome of the MFF negotiations.

### 3.2.2. *Estimated output funded from operational appropriations (not to be completed for decentralised agencies)*

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs			Year 2028	Year 2029	Year 2030	Year 2031	Enter as many years as necessary to show the duration of the impact (see Section 1.6)	TOTAL
	OUTPUTS							

↓	Type <sup>21</sup>	Average cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	No	Cost	Total No	Total cost
SPECIFIC OBJECTIVE No 1 <sup>22</sup> ...																		
- Output																		
- Output																		
- Output																		
Subtotal for specific objective No 1																		
SPECIFIC OBJECTIVE No 2 ...																		
- Output																		
Subtotal for specific objective No 2																		
<b>TOTALS</b>																		

<sup>21</sup> Outputs are products and services to be supplied (e.g. number of student exchanges financed, number of km of roads built, etc.).

<sup>22</sup> As described in Section 1.3.2. 'Specific objective(s)'



### 3.2.3. Summary of estimated impact on administrative appropriations

- ☐ The proposal/initiative does not require the use of appropriations of an administrative nature
- ☒ The proposal/initiative requires the use of appropriations of an administrative nature, as explained below

#### 3.2.3.1. Appropriations from voted budget

EUR million (to three decimal places)

<b>VOTED APPROPRIATIONS</b>	First Year	Second Year	Following Years (yearly amount)
Human resources	2.629	2.629	2.629
Other administrative expenditure	pm	pm	pm
<b>TOTAL</b>	<b>2.629</b>	<b>2.629</b>	<b>2.629</b>

The figures in the table above are all strictly indicative pending the outcome of the MFF negotiations.

The appropriations required for human resources and other expenditure of an administrative nature will be met by appropriations from the DG that are already assigned to management of the action and/or have been redeployed within the DG, together, if necessary, with any additional allocation which may be granted to the managing DG under the annual allocation procedure and in the light of budgetary constraints.

#### 3.2.4. Estimated requirements of human resources

- ☐ The proposal/initiative does not require the use of human resources
- ☒ The proposal/initiative requires the use of human resources, as explained below

### 3.2.4.1. Financed from voted budget

Estimate to be expressed in full-time equivalent units (FTEs)

<b>VOTED APPROPRIATIONS</b>		<i>First Year</i>	<i>Second Year</i>	<i>Following Years</i>
<b>Y Establishment plan posts (officials and temporary staff)</b>				
20 01 02 01 (Headquarters and Commission's Representation Offices)		7	7	7
20 01 02 03 (EU Delegations)		0	0	0
(Indirect research)		0	0	0
(Direct research)		0	0	0
Other budget lines (specify)		0	0	0
<b>• External staff (inFTEs)</b>				
20 02 01 (AC, END from the 'global envelope')		13	13	13
20 02 03 (AC, AL, END and JPD in the EU Delegations)		0	0	0
Admin. Support line	- at Headquarters	0	0	0
[XX.01.YY.YY]	- in EU Delegations	0	0	0
(AC, END - Indirect research)		0	0	0
(AC, END - Direct research)		0	0	0
Other budget lines (specify) - Heading 4		0	0	0
Other budget lines (specify) - Outside Heading 4		0	0	0
<b>TOTAL</b>		<b>20</b>	<b>20</b>	<b>20</b>

Considering the overall strained situation in Heading 4, in terms of both staffing and the level of appropriations, the human resources required will be met by staff from the DG who are already assigned to the management of the action and/or have been redeployed within the DG or other Commission services.

The staff required to implement the proposal (in FTEs):

**To be covered by  
current staff  
available in the  
Commission  
services**

**Exceptional additional staff\***

**To be financed  
under Heading 4  
or Research**

**To be financed  
from BA line**

**To be financed  
from fees**

Establishment plan posts 7

N/A

External staff 13  
(CA, SNEs, INT)

Description of tasks to be carried out by:

Officials and temporary staff	The tasks to be carried out by the officials and temporary staff pertain the legal workstream, the technical workstream, the coordination and international outreach and the supervisory role.
External staff	The tasks to be carried out by the external staff pertain the legal workstream, the technical workstream, the coordination and international outreach and the supervisory role.

### 3.2.5. Overview of estimated impact on digital technology-related investments

Compulsory: the best estimate of the digital technology-related investments entailed by the proposal/initiative should be included in the table below.

This expenditure refers to the operational budget to be used to re-use/ buy/ develop IT platforms/ tools directly linked to the implementation of the initiative and their associated investments (e.g. licences, studies, data storage etc). The information provided in this table should be consistent with details presented under Section 4 “Digital dimensions”.

<b>TOTAL Digital and IT appropriations</b>	First Year	Second Year	Following Years
IT expenditure	42,813	14,238	6,300

### 3.2.6. Compatibility with the current multiannual financial framework

The proposal/initiative:

- ☒ can be fully financed through redeployment within the relevant heading of the proposed multiannual financial framework (MFF) 2028-2034
- ☐ requires use of the unallocated margin under the relevant heading of the MFF and/or use of the special instruments as defined in the MFF Regulation

- ☐ requires a revision of the MFF

### 3.2.7. Third-party contributions

The proposal/initiative:

- ☒ does not provide for co-financing by third parties
- ☐ provides for the co-financing by third parties estimated below:

Appropriations in EUR million (to three decimal places)

	Year 2024	Year 2025	Year 2026	Year 2027	Total
Specify the co-financing body					
TOTAL appropriations co-financed					

### 3.3. Estimated impact on revenue

- ☒ The proposal/initiative has no financial impact on revenue.
- ☐ The proposal/initiative has the following financial impact:
  - ☐ on own resources
  - ☐ on other revenue
  - ☐ please indicate, if the revenue is assigned to expenditure lines

EUR million (to three decimal places)

Budget revenue line:	Appropriations available for the current financial year	Impact of the proposal/initiative <sup>23</sup>			
		Year 2024	Year 2025	Year 2026	Year 2027
Article .....					

For assigned revenue, specify the budget expenditure line(s) affected.

Other remarks (e.g. method/formula used for calculating the impact on revenue or any other information).

<sup>23</sup> As regards traditional own resources (customs duties, sugar levies), the amounts indicated must be net amounts, i.e. gross amounts after deduction of 20% for collection costs.

9. 4. DIGITAL DIMENSIONS

**4.1. Requirements of digital relevance**

If the policy initiative is assessed as having no requirement of digital relevance:

*Justification of why digital means cannot be used to enhance policy implementation and why the ‘digital by default’ principle is not applicable*

N/A

Otherwise:

*High-level description of the requirements of digital relevance and related categories (data, process digitalisation & automation, digital solutions and/or digital public services)*

Reference to the requirement	Requirement description	Actors affected or concerned by the requirement	High-level Processes	Categories
<b>Article 4</b>	Principle of equivalence	European Business Wallet owners Self-employed persons Sole traders Union entities	Use of the EBW and the qualified electronic registered delivery service as digital solutions	Process digitalisation Digital solutions Digital public service
<b>Article 5(1),(2),(3),(4)</b>	European Business Wallet (EBW) functionalities	Providers of European Business Wallets European Business Wallet owners Authorised representatives of European Business Wallet owners Business Wallet-relying parties	IT development (core functionalities)	Digital solutions Digital public service Process digitalisation



<b>Article 6(1),(2),(4)</b>	Technical features for European Business Wallets	Providers of European Business Wallets European Business Wallet owners Business Wallet-relying parties	IT development (technical features)	Data Digital solutions Digital public service
<b>Article 6(3)</b>	Making available information notified	European Commission General Public	Publish validation mechanisms	Data Process automation Digital public service
<b>Article 6(5)</b>	Establish a set of reference standards and specifications	European Commission	Development of implementing acts	Digital public service
<b>Article 7</b>	Requirements and obligations for providers of European Business Wallets	Providers of European Business Wallets European Business Wallet owners Authorised representatives of European Business Wallet owners Competent supervisory bodies The European Commission	Establishing requirements and obligations for providers of European Business Wallets	Digital solutions Data Digital public service Process digitalisation
<b>Article 8</b>	European Business Wallet owner identification data	Providers of European Business Wallet identification data European Business Wallet owners EU entities	Management of owner identification data pertaining to EBW owners	Data Digital public service

		The European Commission		
<b>Article 9</b>	Unique identifiers for EBW owners	Providers of European Business Wallet owner identification data Economic operators Public sector bodies The European Commission	Allocation of unique identifiers for European Business Wallet owners	Data Digital solutions Digital public services
<b>Article 10</b>	European Digital Directory	The European Commission Providers of European Business Wallets European Business Wallet owners	Establishment, operation, and maintenance of the European Digital Directory	Digital solutions Data Digital public service
<b>Article 11</b>	Notification of providers of European Business Wallets	Providers of European Business Wallets Supervisory body in the Member State of establishment	Notification procedure for providers of EBW	Data Digital public service
<b>Article 12</b>	Notification of providers of European Business Wallets by the Member States to the European Commission	Member States The European Commission	Notification Publication	Digital solutions Digital public service Data
<b>Article 13</b>	Member State supervision	Supervisory bodies in each Member State The European Commission	Supervision of EBW providers Notification of	Data Digital public service

		Providers of European Business Wallets	relevant national registries	
<b>Article 14</b>	European Digital Identity Cooperation Group extension of support to EBW	European Digital Identity Cooperation Group The European Commission Member States	Information exchange and coordination	Digital public service
<b>Article 15</b>	Governance and supervision of Union entities that are providers of European Business Wallets (reports)			Data
<b>Article 16</b>	Obligations on public sector bodies to enable the use of the EBW and provide a Qualified Electronic Registered Delivery Service (QERDS)	Public sector bodies European Business Wallet owners Providers of European Business Wallets	Identification Authentication Signature and Seal Submission of documents Notification	Digital solutions Digital public service Process digitalisation
<b>Article 17</b>	List of Business Wallets and other similar instruments offered in third countries	The European Commission Non-EU countries	Publication of equivalent systems from third countries	Data Digital solutions Digital public service
<b>Article 18</b>	Issuing of European Business Wallets to economic operators established outside the Union	Providers of European Business Wallets Economic operators established in a third country Qualified trust service providers established in a	Issuance of European business wallets Identity proofing and verification	Data Digital solution Digital public service

		Member State Member States of the qualified trust service providers		
<b>Article 20</b>	Removal of legal persons from Regulation (EU) 910/2014, due to obsolescence with advent of EBW	Legal person Member states	Legal person identification, authentication and data sharing	Digital public service Digital solution Data

## 4.2. Data

*High-level description of the data in scope*

Type of data	Reference to the requirement(s)	Standard and/or specification (if applicable)
		//
EBW owner identification data	Article 8(1)	<p>EBW owner identification data shall be issued in a format according to one of the standards listed in Annex II of Commission Implementing Regulation (EU) 2024/2979 and as:</p> <ul style="list-style-type: none"> <li>- QEAA when provided by qualified trust service providers;</li> <li>- EAA when issued by or on behalf of a public sector body responsible for an authentic source, when provided by a public sector body;</li> <li>- EAA when provided by the Commission.</li> </ul>
EAA/QEAA (Electronic Attestations of Attributes / Qualified Electronic Attestations of Attributes)	Article 8(1)	<p>Issuer requirements: For QEAA, the issuer must be a Qualified Trust Service Provider, satisfying legal and technical requirements.</p> <p>Standards / formats: The attestations must follow the schemas / formats prescribed (within ARF / toolbox) for attribute attestations. The attributes themselves must be accurate, derived from authentic sources.</p> <p>Interoperability, trust / verification: Relying parties might be able to verify them, there must be revocation / suspension mechanics, and trust infrastructure must ensure their validity.</p> <p>Regulation (EU) 2024/1183 (eIDAS 2.0) - Annex V; ETSI TS 119 471; ETSI EN 319 412 (series); ETSI</p>

		TS 119 182-1; ETSI TS 119 102-1; ETSI TS 119 102-2; ETSI EN 319 401; ETSI EN 319 411-1 / 411-2; ETSI TS 119 461; ETSI TS 119 172-4; CEN/EN 319 521
EBW owner identification data elements	Article 8(6)	Must contain at least the following attributes: the official name of the economic operator or public sector body, as recorded in the relevant register or official record, the relevant unique identifier attributed in accordance with Article 9.
Unique identifiers for EBW owners (EUID)	Article 9(1)	EUID identifier must be used if an economic operator falls within the scope of Directive (EU) 2017/1132 or Directive (EU) 2015/849
Information for the purpose of maintaining the EDD	Article 10(3)(6)	Standards and technical specifications for the EDD to be established in the implementing acts to be adopted
Notification of providers of EBW	Article 11(2)	Lists elements to be included in the notification
List of notified providers of EBW	Article 12	Machine readable format
List of MS supervisory bodies	Article 13(3)	Data elements to be included: names and addresses
Information on national registries holding information on economic operators and public sector bodies	Article 13(5)(f)	Not specified
List of Business Wallets and other similar instruments offered in third countries	Article 17(4)	Not specified
EBW owner's data for portability purposes	Annex	Open format



**Alignment with the European Data Strategy**

*Explanation of how the requirement(s) are aligned with the European Data Strategy*

The proposal aligns with the European Data Strategy by implementing data-driven approach to innovation and enhancing the digital economy. It aims to reduce administrative burdens, streamline compliance processes, and improve service delivery through the provision of market-driven solutions, further enhancing competitiveness. The European Business Wallets facilitate seamless information exchange across borders in a transparent, trustworthy and secure way. The proposal promotes interoperability and compatibility with the existing systems.

**Alignment with the once-only principle**

*Explanation of how the once-only principle has been considered and how the possibility to reuse existing data has been explored*

The proposal promotes the once-only principle by requiring authorities to reuse data already held in another MS without need for the repeated submissions by businesses. The European Business Wallets will complement the SDG and OOTS by providing trusted identification and authentication of economic operators and public administrations and a secure exchange layer that enables businesses and public sector bodies to share, and reuse verified data and official attestations seamlessly across borders. Additionally, while the OOTS focuses on the interactions among Public Sector Bodies (G2G), the European Business Wallets is focusing the on the interactions between Public Sector Bodies and economic operators (B2G) and between economic operators (B2B).

*Explanation of how newly created data is findable, accessible, interoperable and reusable, and meets high-quality standards*

Newly created European Business Wallets data adheres to the FAIR principles by employing standards and specifications enhancing searchability and secure access. It is also designed to seamlessly integrate with a larger European Digital Identity Framework defined under eIDAS.

**Data flows**

*High-level description of the data flows*

Type of data	Reference(s) to the requirement(s)	Actors who provide the data	Actors who receive the data	Trigger for the data exchange	Frequency (if applicable)

Information on validation mechanisms	Article 6(2)(g)	Providers of EBW	The Commission	Without undue delay	//
Information on validation mechanisms	Article 6(3)	The Commission	General public	Notification from the provider of EBW	//
Notification about terms, conditions rights and obligations related to the EBW	Article 7(6)(b)(c)	Providers of EBW	EBW owners/ representatives of EBW owners	Use of EBW	//
Notification about substantive changes to the EBW service	Article 7(6)(e)	Providers of EBW	National supervisory body or the Commission	//	//
Notification about the suspension, revocation or voluntary termination of EBW service	Article 7(6)(f)	Providers of EBW	EBW owners	//	//
Information on EBW owners (and subsequent changes)	Article 7(6)(g)	Providers of EBW	The Commission	//	//
EBW owner identification data	Article 8(1)	Providers of EBW identification data	EBW owner	Request of the EBW owner	once
EAA/QEAA (Electronic Attestations of Attributes / Qualified Electronic Attestations of Attributes)	Article 8	(Q)EAA providers	EBW owner	Request of the EBW owner	Upon request
Notification on the national registers and associated registration numbers	Article 9(6)	MS	The Commission	No later than 3 months after the entry into force	//

Information for the purpose of maintaining the EDD	Article 10(3)(6)	Provider of EBW	The Commission	Upon issuance of the EBW (for the purpose of maintaining the EDD)	//
Notification on providers of EBW	Article 11(1)	Notifying entity	MS Supervisory body	//	//
Notification on providers of EBW	Article 11(4)(5)(6)	MS Supervisory bodies	Notifying entity	Notification sent by notifying entity – 30 days	//
List of notified providers of EBW	Article 12 (1)(2)(3)	MS	The Commission	24 hours 4 hours of the expiration of the 30-day period referred to in Article 11	//
List of MS supervisory bodies	Article 13(3)	MS	The Commission	//	//
List of MS supervisory bodies	Article 13(3)	The Commission	General public	//	//
Information on national registries	Article 13(5)(f)	MS Supervisory bodies	The Commission	//	//
Reporting obligations on the main activities	Article 13(5)(k)	MS Supervisory bodies	The Commission	//	//
List of Business Wallets and other similar instruments offered in third countries	Article 17(4)	The Commission	General public	//	//

### 4.3. Digital solutions

#### *High-level description of digital solutions*

Digital solution	Reference(s) to the requirement(s)	Main mandated functionalities	Responsible body	How is accessibility catered for?	How is reusability considered?	Use of AI technologies (if applicable)
European Business Wallet	Article 4 Article 5(1),(3),(5) Article 6(1),(2),(4) Article 7 Article 9 Article 16 Article 17(1),(3) Article 18 Annex	<p>Providers of European Business Wallets shall ensure that the European Business Wallets they provide enable European Business Wallet owners, at a minimum, to:</p> <p>(10) securely issue, request, obtain, select, combine, store, delete, share and present electronic attestations of attributes;</p> <p>(1) selectively disclose European Business Wallet owner identification data and attributes contained in electronic attestations of attributes, in the context of the functionalities listed under point a;</p> <p>(2) request and share European Business Wallet owner identification data and electronic attestations</p>	Providers of the European Business Wallet	The standards and specification that will be defined in the implementing acts will refer to accessibility requirements as it was the case for the EUDIW. However, it is important to consider that the solution providers will be the private sector and as such their will need to comply with the Accessibility	Emphasis on open standards, interoperability, and data portability ensures that the Wallets can be reused or integrated across various platforms and services without vendor lock-in. Additionally, the Business Wallet is reusing the EU Digital Identity Framework and compatibility with the EUDIW is prescribed.	N/A

		<p>of attributes in a secured way between European Business Wallets and European Digital Identity Wallets and with European Business Wallet-relying parties;</p> <p>(3) sign by means of qualified electronic signatures and seal by means of qualified electronic seals, as applicable;</p> <p>(4) bind data in electronic form to a particular time by means of qualified electronic time stamps;</p> <p>(5) issue electronic attestations of attributes to European Business Wallets and European Digital Identity Wallets;</p> <p>(6) issue electronic attestations of attributes through the European Business Wallet of the owner, allowing the issued attestation to be linked to other relevant</p>		Directive 2019/882.		
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	---------------------	--	--

		<p>attestations forming part of a chain.</p> <p>(7) enable the use of qualified and non-qualified attestations of attributes to allow European Business Wallet owners and their legal representatives to authenticate</p> <p>(8) transmit and receive electronic documents and data by means of a qualified electronic registered delivery service able to support confidentiality;</p> <p>(9) authorise multiple users to access and operate the European Business Wallet of the owner, and for the Business Wallet owner to manage and revoke such authorisations;</p> <p>(10) authorise European Business Wallet-relying parties to request electronic attestations of attributes issued to the owner of the European Business</p>				
--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--



		<p>Wallet, and for the Business Wallet owner to manage and revoke such authorisations;</p> <p>(11) exercise the European Business Wallet owner's right to data portability and export their data, including issued European Business Wallet owner identification data, electronic attestations of attributes, communication logs, and interaction records, in a structured, commonly used and machine-readable format, at the request of the owner or in the event of termination of service or revocation of the notification of the provider of the European Business Wallet;</p> <p>(12) access a log of all transactions;</p> <p>(13) access a common dashboard for accessing, storing and verifying</p>				
--	--	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--	--

		communications exchanged through the qualified electronic registered delivery service referred to in point (i).				
European Digital Directory	Article 10	<p>The Commission shall establish, operate and maintain a European Digital Directory as a web application comprising of two interfaces:</p> <ul style="list-style-type: none"> <li>• a machine-readable interface exposed through an API for automated system-to-system communication;</li> <li>• an online portal for European Business Wallets users, built on and communicating with the API, ensuring consistency between both interfaces.</li> </ul>	European Commission		-	N/A
Signature creation applications	Annex	<p>Signing or sealing data provided by European Business Wallets users.</p> <p>Signing or sealing data provided by relying parties.</p> <p>Creating signatures or seals in accordance with at least the mandatory format.</p> <p>Creating signatures or seals in accordance with the optional format.</p> <p>Informing Wallets users about the result of the signature or seal creation</p>	<p>European Business Wallets providers</p> <p>Providers of trust services</p> <p>Business-Wallet-relying parties</p>		-	-

		process.				
Qualified electronic registered delivery service	Annex	<p>In line with Article 5 of this Regulation, Business Wallets shall integrate and support the use of a specific qualified electronic registered delivery service in accordance with Articles 43 and 44 of Regulation (EU) No 910/2014.</p> <p>Interoperability between Business Wallets and the designated qualified electronic registered delivery service shall be mandatory. Providers of Business Wallets shall ensure technical integration in accordance with the implementing acts.</p>	European Commission		-	-

*For each digital solution, explanation of how the digital solution complies with applicable digital policies and legislative enactments*

### **European Business Wallet**

<b>Digital and/or sectorial policy (when these are applicable)</b>	<b>Explanation on how it aligns</b>
<i>AI Act</i>	N/A
<i>EU Cybersecurity framework</i>	<p>Providers of the European Business Wallets shall ensure integrity, authenticity, and confidentiality of the communication between the Business Wallet's back-end, front-end and secure cryptographic applications and device.</p> <p>Providers of the European Business wallets shall also comply with the requirements of Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union.</p>

<b><i>eIDAS</i></b>	<p>The European Business Wallet builds on the European Digital Identity Framework defined under eIDAS and it expands it to all economic operators and public sector bodies.</p> <p>Access to the European Business Wallets Unit shall be granted only after the European Business Wallets user has been successfully authenticated as detailed under annex I (1) (2).</p> <p>Interoperability between European Business Wallets and European Digital Identity Wallets: request and share European Business Wallet owner identification data and electronic attestations of attributes in a secured way between European Business Wallets and European Digital Identity Wallets.</p>
<b><i>Single Digital Gateway and IMI</i></b>	N/A
<b><i>Others</i></b>	N/A

### **European Digital Directory**

<b>Digital and/or sectorial policy (when these are applicable)</b>	<b>Explanation on how it aligns</b>
<b><i>AI Act</i></b>	N/A
<b><i>EU Cybersecurity framework</i></b>	<p>The Commission shall make the European Digital Directory only accessible to European Business Wallet owners and providers of European Business Wallets.</p> <p>The Commission shall implement the European Digital Directory in accordance with the relevant principles of data protection including, where appropriate, with the features of pseudonymisation.</p> <p>Alignment with Directive 2022/2555.</p>
<b><i>eIDAS</i></b>	
<b><i>Single Digital Gateway and IMI</i></b>	

<i>Others</i>	
---------------	--

#### Signature creation application

Digital and/or sectorial policy (when these are applicable)	Explanation on how it aligns
<i>AI Act</i>	N/A
<i>EU Cybersecurity framework</i>	-
<i>eIDAS</i>	Use of electronic signatures and seals.
<i>Single Digital Gateway and IMI</i>	-
<i>Others</i>	-

#### 4.4. Interoperability assessment

*High-level description of the digital public service(s) affected by the requirements*

Digital public service or category of digital public services	Description	Reference(s) to the requirement(s)	Interoperable Europe Solution(s) (NOT APPLICABLE)	Other interoperability solution(s)

<p><b>Digital identity verification and authorisation, European Business Wallets (COFOG 01.6 - BT.1 - General public services)</b></p>	<p>Public service facilitates secure cross-border transactions by providing a framework for digital identity and authentication for economic operators and public sector bodies.</p>	<p>Article 4; Article 5(1), (3), (5); Article 6(1),(2),(4); Article 6(3); Article 6(5); Article 7; Article 8; Article 9; Article 10; Article 11; Article 12; Article 13; Article 18(1),(3); Article 19; Article 21.</p>	<p>//</p>	<p>Business Registers Interconnection System ('BRIS') and the Beneficial Ownership Registers Interconnection System ('BORIS')</p> <p>SDG</p> <p>DPP Wallet</p> <p>EDD</p>
----------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------



Digital public services in Member States that are mandated to accept evidence through European Business Wallets	National digital public services impacted by the use of European Business Wallets in administrative procedures where public sector bodies are required to accept identification and authentication, eSignature or eSeal, submission of documents, the sending or receiving of notifications.	Article 16(1) (2)	//	
-----------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------	----	--

*Impact of the requirement(s) as per digital public service on cross-border interoperability*

**Digital public service #1: European Business Wallet**

Assessment	Measure(s)	Potential remaining barriers (if applicable)
<p><b>Alignment with existing digital and sectorial policies</b></p> <p><b>Please list the applicable digital and sectorial policies identified</b></p>	<p>The European Business Wallets will build on and extend the ecosystem of trust established under the European Digital Identity Framework, established by Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market, as amended by Regulation (EU) 2024/118318 (including adopted implementing acts).</p> <p>Providers of the European Business wallets must comply with the requirements of Directive (EU) 2022/2555 (NIS2) of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union. Likewise, the European Digital Directory shall be operated in alignment with the principles enshrined under NIS2.</p>	

	<p>Cryptographic operators or other operations processing critical assets shall be performed in accordance with the requirements for the characteristics and design of electronic identification means at assurance level substantial as set out in Commission Implementing Regulation (EU) 2015/1502.</p> <p>The European Data Protection Supervisor were consulted in accordance with Article 42(1) of Regulation (EU) 2018/1725.</p> <p>The proposal anticipates that the European Business Wallets should also enable the exchange of attestations for the purpose of delegating digital power of attorney, as established by Directive (EU) 2025/25, allowing economic operators and public sector bodies to exchange attestations with their Business Wallets to delegate authority to representatives.</p>	
<p><b>Organisational measures for a smooth cross-border digital public services delivery</b></p> <p><b>Please list the governance measures foreseen</b></p>	<p>In each Member State, the supervisory bodies designated pursuant to Article 46a of Regulation (EU) No 910/2014 shall also be the supervisory bodies for the purposes of this Regulation. The Regulation provides for the role and tasks of such authorities.</p> <p>Member States shall ensure that the supervisory bodies referred to in paragraph 1 possess the necessary powers and adequate resources for the exercise of their tasks in an effective, efficient, and independent manner.</p> <p>Where a Union entity is a provider of European Business Wallets the Commission shall be the responsible supervisory body.</p>	
<b>Measures taken to ensure a shared</b>	EBW owner identification data shall be issued in a	

<b>understanding of the data</b> <b>Please list such measures</b>	<p>format according to one of the standards listed in Annex II of Commission Implementing Regulation (EU) 2024/2979 and as QEAA or EAA depending on the issuing entity.</p> <p>The annexes define the high-level requirements that will be then instantiated in specifications and standards in the upcoming implementing act to ensure a shared understanding of the data.</p> <p>Business Wallets shall support the secure export and portability of an owner's European Business Wallet data in at least an open format.</p>	
<b>Use of commonly agreed open technical specifications and standards</b> <b>Please list such measures</b>	<p>Adopt implementing acts for the definition of reference standards and specifications.</p>	

**Digital public service #2: Digital public services in Member States that are mandated to receive evidence through European Business Wallets**

Assessment	Measure(s)	Potential remaining barriers (if applicable)
<b>Alignment with existing digital and sectorial policies</b> <b>Please list the applicable digital and sectorial policies identified</b>	<p>Alignment ensured for the European Business Wallets, as detailed above.</p>	
<b>Organisational measures for a smooth cross-border digital public services delivery</b>	<p>Article 15 mandates Member States to enable economic operators to exchange information with public sector bodies via the European Business Wallet.</p>	

<b>Please list the governance measures foreseen</b>		
<b>Measures taken to ensure a shared understanding of the data</b> <b>Please list such measures</b>		
<b>Use of commonly agreed open technical specifications and standards</b> <b>Please list such measures</b>		

#### 4.5. Measures to support digital implementation

*High-level description of measures supporting digital implementation*

<b>Description of the measure</b>	<b>Reference(s) to the requirement(s)</b>	<b>Commission role (if applicable)</b>	<b>Actors to be involved (if applicable)</b>	<b>Expected timeline (if applicable)</b>
List of reference standards and, where necessary, specifications and procedures for the core functionalities of European Business Wallets	Article 5(3)(5)	Adopt implementing acts	//	//
List of reference standards and, where necessary, specifications and procedures for the technical features of the European Business Wallets	Article 6 (5)	Adopt implementing acts	//	//
Requirements for European Business wallet	Article 8 (6)	Adopt implementing acts	//	//

owner identification data issuance				
Specifications and detailed requirements for the unique identifier	Article 9 (4)	Adopt implementing acts	//	//
Standards and technical specifications for the European Digital Directory	Article 10(6)	Adopt implementing acts	//	//
Acts establishing that Business Wallets or systems offering similar functions that are issued by providers established in third countries are to be considered as equivalent to European Business Wallets	Article 18(1)	Adopt implementing acts	//	//









EUROPEAN  
COMMISSION

Brussels, 19.11.2025  
COM(2025) 838 final

ANNEX

**ANNEX**

**to the**

**Proposal for a Regulation of the European Parliament and of the Council  
on the establishment of European Business Wallets**

{SWD(2025) 837 final}

## **ANNEX**

### **Requirements for minimum functionalities and technical requirements of European Business Wallets**

#### **1. EUROPEAN BUSINESS WALLETS UNIT AUTHENTICATION**

Access to the European Business Wallets Unit shall be granted only after the European Business Wallets user has been successfully authenticated by means of either:

- (1) a notified electronic identification (eID) means in accordance with Article 6 of Regulation (EU) No 910/2014, fulfilling at least the requirements for a substantial level of assurance as defined in Article 8 of that Regulation and further specified in Commission Implementing Regulation (EU) 2015/1502; or
- (2) an alternative authentication mechanism recognised as equivalent and fulfilling at least the requirements for a substantial level of assurance as defined in Article 8 of Regulation (EU) No 910/2014 and further specified in Commission Implementing Regulation (EU) 2015/1502.

Until such authentication has been completed, no functionality of the European Business Wallets Unit or of any other functionalities shall be made accessible to the Wallets user.

#### **2. EUROPEAN BUSINESS WALLETS UNIT INTEGRITY**

Providers of European Business Wallets shall, for each European Business Wallet unit, generate and sign a European Business Wallet unit attestation in accordance with the requirements laid down in point 5. The certificate used to sign or seal the Business Wallet unit attestation shall be issued under a certificate listed in the trusted list referred to in Commission Implementing Regulation (EU) 2024/2980.

#### **3. EUROPEAN BUSINESS WALLETS SECURE COMMUNICATION AND CRITICAL ASSET MANAGEMENT**

- (1) European Business Wallet back-end shall use at least one Wallet secure cryptographic application and Wallets secure cryptographic device to manage critical assets.
- (2) Providers of the European Business Wallets shall ensure integrity, authenticity and confidentiality of the communication between the Business Wallet's back-end, front-end and secure cryptographic applications and device.
- (3) Where critical assets relate to performing electronic identification at assurance level substantial, the European Business Wallets cryptographic operations or other operations processing critical assets shall be performed in accordance with the requirements for the characteristics and design of electronic identification means at assurance level substantial, as set out in Commission Implementing Regulation (EU) 2015/1502.

#### **4. WALLETS SECURE CRYPTOGRAPHIC APPLICATIONS**

- (1) Providers of European Business Wallets shall ensure that European Business Wallets secure cryptographic applications and devices:

- (a) perform the wallet's cryptographic operations involving critical assets other than those needed for the Wallets unit to authenticate the Wallets owner only in cases where those applications have successfully authenticated Wallets users;
- (b) where they authenticate the European Business Wallet owner in the context of performing electronic identification at assurance level substantial as set out in Implementing Regulation (EU) 2015/1502;
- (c) are able to securely generate new cryptographic keys;
- (d) are able to perform secure erasure of critical assets;
- (e) are able to generate a proof of possession of private keys;
- (f) protect the private keys generated by these Wallets secure cryptographic applications and devices during the existence of the keys;
- (g) comply with the requirements for the characteristics and design of electronic identification means at assurance level substantial, as set out in Implementing Regulation (EU) 2015/1502.

## **5. WALLETS UNIT AUTHENTICITY AND VALIDITY**

- (1) Providers of European Business Wallets shall ensure that the European Business Wallets unit attestations referred to in point 1 contain public keys and that the corresponding private keys are protected by a Wallets secure cryptographic device.
- (2) Providers of European Business Wallets shall provide mechanisms, independent of Wallets units, for the secure identification and authentication of Wallets users.

## **6. REVOCATION OF WALLETS UNIT ATTESTATIONS**

- (1) Providers of European Business Wallets shall establish a publicly available policy specifying the conditions and the timeframe for the revocation of Wallets unit attestations.
- (2) In line with Article 6, where the providers of European Business Wallets revoke European Business Wallets unit attestations, they shall inform the affected European Business Wallets users without undue delay and no later than 24 hours from the revocation of their European Business Wallets units, including the reason for the revocation and the consequences for the European Business Wallets user. This information shall be provided in a manner that is concise, easily accessible and using clear and plain language.
- (3) Where European Business Wallets providers have revoked a European Business Wallet's unit attestation, they shall make publicly available the validity status of the European Business Wallet unit attestation and describe the location of that information in the Business Wallet's unit attestation.

## **7. TRANSACTION LOGS**

- (1) The providers of European Business Wallets shall provide an appropriate logging policy that shall include, at a minimum, electronic signing, electronic

sealing, and notifications of all transactions with Business-Wallet-relying parties, other European Business Wallets units, and European Digital Identity Wallets units, irrespective of whether the transaction is successfully completed.

- (2) The logged information shall at least contain:
  - (a) the time and date of the transaction;
  - (b) the name, contact details, and unique identifier of the corresponding Business-Wallet-relying party and the Member State in which that Business-Wallet-relying party is established, or in case of other Wallets units, relevant information from the Wallets unit attestation;
  - (c) the type or types of data requested and presented in the transaction;
  - (d) in the case of non-completed transactions, the reason for such non-completion.
- (3) Providers of European Business Wallets shall ensure integrity, authenticity and confidentiality of the logged information.
- (4) European Business Wallets back-end shall log reports sent by the Wallets user to the competent authorities via the Wallets unit, including interactions related to notifications, regulatory compliance, data sharing, or audit requests.
- (5) The logs referred to in subpoints 1 and 2 shall be accessible to the European Business Wallets provider, where it is necessary for the provision of Wallets services.
- (6) The logs referred to in subpoints 1 and 2 shall remain accessible for as long as required to be accessible by Union law or national law.

## **8. QUALIFIED ELECTRONIC SIGNATURES AND SEALS**

- (1) In line with Article 6, providers of European Business Wallets shall ensure that Wallets users are able to receive qualified certificates for qualified electronic signatures or seals which are linked to qualified signature or seal creation devices that are either local, external, or remote in relation to the Wallet's unit.
- (2) Providers of European Business Wallets shall ensure that European Business Wallets solutions can securely interface with one of the following types of qualified signature or seal creation devices: local, external, or remotely managed qualified signature or seal creation devices for the purposes of using the qualified certificates referred to in subpoint 1.

## **9. SIGNATURE CREATION APPLICATIONS**

- (1) The signature creation applications used by European Business Wallets units may be provided either by European Business Wallets providers, by providers of trust services or by Business-Wallet-relying parties.
- (2) Signature creation applications shall have the following functions:
  - (a) signing or sealing data provided by European Business Wallets users;
  - (b) signing or sealing data provided by relying parties;
  - (c) creating signatures or seals in accordance with at least the mandatory format;

- creating signatures or seals in accordance with the optional format;
- informing Wallets users about the result of the signature or seal creation process.

To ensure uniform conditions for the implementation of this Regulation, the Commission is empowered to adopt implementing acts in accordance with Article 6 that specify the technical standards referred to in subpoint 2, letters (c) and (c)(ii).

- (3) The signature creation applications may either be integrated into or be external to European Business Wallets back-end. Where signature creation applications rely on remote qualified signature creation devices and where they are integrated into European Business Wallets back-end, they shall support the application programming interface set out in the implementing acts, which the Commission is empowered to adopt in accordance with Article 5 in order to ensure uniform conditions for the implementation of this Regulation.

## **10. DATA EXPORT AND PORTABILITY**

Business Wallets shall support the secure export and portability of an owner's European Business Wallet data in at least an open format. This shall enable the owner to migrate their data to another Business Wallets solution while ensuring a level of assurance of at least "substantial", as defined in Implementing Regulation (EU) 2015/1502.

## **11. SECURE LEGAL COMMUNICATION CHANNEL FOR THE BUSINESS WALLET**

- (1) In line with Article 5 of this Regulation, Business Wallets shall integrate and support the use of a specific qualified electronic registered delivery service in accordance with Articles 43 and 44 of Regulation (EU) No 910/2014.
- (2) The Commission shall, by means of implementing acts:
  - (a) designate one qualified electronic registered delivery service that shall serve as the mandatory secure legal communication channel for European Business Wallets;
  - (b) define the minimum technical and interoperability requirements that such qualified electronic registered delivery service must fulfil, including alignment with the reference standards, specifications and procedures established under Articles 43 and 44 of Regulation (EU) No 910/2014;
  - (c) ensure that the chosen qualified electronic registered delivery service is based on open, publicly available and royalty-free standards to guarantee interoperability and prevent vendor lock-in;
  - (d) ensure that the chosen qualified electronic registered delivery service provides end-to-end encryption to guarantee confidentiality;
  - (e) establish procedures for ensuring continuous availability, redundancy and fallback mechanisms in case of service failure.
- (3) Interoperability between Business Wallets and the designated qualified electronic registered delivery service shall be mandatory. Providers of Business Wallets shall ensure technical integration in accordance with the implementing acts referred to in subpoint 2.

## **12. EUROPEAN BUSINESS WALLETS ACCESS CONTROL MECHANISM**

- (1) Providers of European Business Wallets shall ensure that authorisation decisions under the access control mechanism are based on one or more of the following criteria, as appropriate to the specific access request:
  - (a) the electronic attestation of attributes of the acting subject;
  - (b) the formal role of the acting subjects within a recognised organisational structure or economic operator;
  - (c) the scope, validity and constraints of any mandate, delegation, or power of attorney;
  - (d) contextual information or policies and rules adopted at Union or national level for sector-specific compliance.
- (2) Providers of European Business Wallets shall ensure the access control mechanism enables fine-grained and auditable authorisation outcomes, ensuring that:
  - (a) visibility of credentials and attestations is selective and conditioned on access rights;
  - (b) access to business processes, digital procedures or submission interfaces is controlled by real-time validation of roles and mandates;
  - (c) all access and execution events are logged, timestamped, and bound to cryptographically verifiable proofs of authorisation, suitable for audit and legal proceedings.
- (3) Providers of the European Business Wallets shall ensure that:
  - (a) mappings between roles and attributes are verifiable, auditable, revocable and traceable to their legitimate issuers;
  - (b) conflicts of roles, over-delegation, or expired authorisations are automatically detected and prevented in real time;
  - (c) all authorisation logic is interoperable across Member States.
- (4) The list of reference standards, technical specifications and procedures to be applied for the implementation of the access control mechanism shall be defined in the implementing acts, which the Commission is empowered to adopt in accordance with Article 5 in order to ensure uniform conditions for the implementation of this Regulation. These shall cover in particular:
  - (a) the formats for the representation of roles and attributes;
  - (b) interoperability mechanisms for mandates and delegations across wallets;
  - (c) protocols, policy language and constraint enforcement;
  - (d) requirements for secure logging, timestamping and auditability of authorisation events.
- (5) Compliance with the requirements laid down in this Article shall be presumed where the standards, specifications and procedures referred to in subpoint 1 are met.



### **13. GENERAL PROVISIONS FOR PROTOCOLS AND INTERFACES**

In line with Article 6 of this Regulation, providers of European Business Wallets shall ensure that European Business Wallets units:

- (1) authorise requests and, where applicable, authenticate those made through relying-party access certificates or Wallet unit attestations. Authentication of the relying party shall be required where attestations are intended for a restricted audience; in all other cases, attestations may be presented by any requesting party;
- (2) display to Wallet users' information contained in the Business-Wallet-relying party access certificates or in the Wallets unit attestations where applicable;
- (3) display to Wallets users, where applicable, the attributes that Wallets users are requested to present;
- (4) present Wallet unit attestations of the Wallet unit to Business-Wallet-relying parties or Wallets units that request it.

### **14. ISSUANCE OF ELECTRONIC ATTESTATIONS OF ATTRIBUTES TO WALLETS UNITS**

- (1) In line with Article 5 of this Regulation, providers of European Business Wallets shall ensure that Business Wallet units requesting issuance of, electronic attestations of attributes are able to authenticate relying parties.
- (2) In relation to the issuance of electronic attestations of attributes to a Wallet unit, Wallet providers shall ensure that the following requirements are complied with:
  - (a) where European Business Wallets owners, through their Business Wallet unit, request from the provider of the European Business Wallet the issuance of Business Wallets owner identification data or of electronic attestations of attributes from providers of Business Wallets owner identification data or providers of electronic attestations of attributes that enable issuance of Business Wallets owner identification data or electronic attestations in more than one format, the Wallets unit shall request it in all formats referred to in Article 8 to this Regulation laying down rules for the application of the Business Wallets Regulation as regards the integrity and core functionalities of Business Wallets;
  - (b) where Business Wallet owners use their Business Wallets unit to interact with competent national authorities and providers of electronic attestations of attributes, Wallet units shall enable authentication and validation of the Wallet unit components by presenting the Wallet unit attestations to those competent national authorities and providers upon their request;
  - (c) Wallet solutions shall support mechanisms that enable providers of Business Wallets Owner Identification Data to verify issuance, delivery and activation in compliance with assurance level substantial requirements set out in Commission Implementing Regulation (EU) 2015/1502 (11);
  - (d) Wallet units shall verify the authenticity and validity of Business Wallets owner identification data and electronic attestations of attributes.

**15. PRESENTATION OF ATTRIBUTES TO EUROPEAN BUSINESS WALLET RELYING PARTIES**

In line with point (d) and (k) of paragraph 1 of Article 5, European Business Wallet providers shall ensure that:

- (1) European Business Wallet solutions support protocols and interfaces for the presentation of attributes to Business-Wallet-relying parties in accordance with the standards defined in the implementing acts;
- (2) At the request of users, European Business Wallet units respond to successfully authenticated and validated requests from Business-Wallet-relying parties in accordance with the standards defined in the implementing acts;
- (3) European Business Wallet units support proving the possession of private keys corresponding to public keys used in cryptographic bindings.

**16. ISSUANCE OF EUROPEAN BUSINESS WALLET OWNER IDENTIFICATION DATA TO WALLETS UNITS**

- (1) Competent authorities shall ensure that Business Wallets owner identification data issued to Business Wallets units comply with the technical specifications set out in the implementing acts, in line with Article 8 of this Regulation.
- (2) Competent national authorities shall ensure that Business Wallets owner identification data that they issue is cryptographically bound to the Wallets unit to which it is issued.

**17. ISSUANCE OF ELECTRONIC ATTESTATIONS OF ATTRIBUTES TO WALLETS UNITS**

- (1) Electronic attestations of attributes issued to European Business Wallets units shall comply with at least one of the standards in the list set out in the implementing acts, in line with Article 5 of this Regulation.
- (2) Providers of electronic attestations of attributes shall identify themselves to European Business Wallets units using their wallet-relying party access certificate.
- (3) Providers of electronic attestations of attributes shall ensure that electronic attestations of attributes issued to European Business Wallets units contain the information necessary for authentication and validation of those electronic attestations of attributes.