Council of the European Union

Brussels, 2 June 2026
(OR. en)

9684/26

Interinstitutional File: 2025/0358 (COD)

TELECOM 265
COMPET 623
MI 526
DATAPROTECT 172
JAI 660
CODEC 999

NOTE

From:	General Secretariat of the Council
To:	Council
Subject:	Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of European Business Wallets - General approach

I. BACKGROUND

1. The Commission adopted the proposal for a Regulation on the establishment of European Business Wallets (EBW) on 19 November 2025.

2. The proposal builds on the ecosystem established under the European Digital Identity Framework (EUDI) Regulation[1] and aims to complement said framework by helping reduce administrative burdens and by offering functionalities such as the access to secure and trusted digital identification across borders, the digital management of representation rights and authorisations, and a secure channel for exchanging official documents and attestations supported by a common directory.

[1] Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market, amended by Regulation (EU) 2024/1183 (EUR-Lex - 02014R0910-20241018 - EN - EUR-Lex).

II. WORK IN OTHER INSTITUTIONS AND BODIES

3. In the European Parliament, the proposal was referred to the Committee on Industry, Research and Energy (ITRE), with two committees giving an opinion, namely the Committee on the Internal Market and Consumer Protection (IMCO) and the Committee on Legal Affairs (JURI). The rapporteur is Eero Heinäluoma (S&D, Finland), who published his draft report on 20 March 2026.

4. On 19 January 2026 the European Economic and Social Committee was invited to give its opinion on the proposal, which was subsequently delivered on 18 March 2026.

5. The European Data Protection Supervisor published formal comments on the proposal on 20 January 2026.

III. WORK IN THE COUNCIL

6. With the **first compromise proposal** (10 February) the Cyprus Presidency intervened on: definitions; EBW functionalities; obligations for, and supervision of, EBW providers; the extension of timelines and their tying to the availability of implementing acts.

7. The **second compromise proposal** (10 March) encompassed: clarifications on the application of national laws in relation to the exchange of documents; revised definitions; management and revocation of roles; interoperability of all authorisation logic between EBWs; streamlining of references to eIDAS2 and cybersecurity rules; clear references to owner identification data; enhancement of ex-ante obligations for providers; a stronger supervision mechanism; full flexibility for public sector bodies regarding the adoption of EBWs; further elaboration on the Commission's assessment of third-country solutions.

8. In the **third compromise proposal** (14 April) the Cyprus Presidency included: an exemption for public security purposes and defence; limitations to the principle of equivalence and a clarification that national administrative and procedural requirements still apply; a deadline for the Commission to adopt implementing acts; the incorporation of public sector bodies that are not EBW owners in the European Digital Directory; an obligation for the Commission to issue guidance on how to determine whether providers of European Business Wallets present risks for the security of the Union; a higher threshold for applicants aspiring to become EBW providers – even if the latter are Qualified Trust Service Providers – and longer deadlines for reviews by supervisory bodies; stronger involvement of the supervisory body and provider concerned in case of non-compliance; the supervision by the Commission of Union entities other than Union institutions; streamlining and grouping of all timelines in the proposal.

9. After presenting the third compromise proposal, the Cyprus Presidency made a few **further amendments to address Member States' remaining concerns**, including with regard to: national requirements; the principle of equivalence; exemptions for any power of attorney and legal mandates provided under national or Union law; accessibility for persons with disabilities; the exchange of data on authorisations with national registers; implementing acts on the assessment of the risks potentially posed by EBW providers; flexibility on the imposition of administrative fines on national public authorities and bodies.

10. On 27 May Coreper examined the text presented and **agreed to submit it to the TTE (Telecommunications) Council**, without any changes, **with a view to reaching a general approach** at its meeting of 9 June 2026.

VI. CONCLUSION

11. In light of the above the Council, at its meeting on 9 June 2026, is invited to:

– examine the compromise text set out in the Annex to this note;

– confirm a general approach on the proposal for a Regulation on the establishment of European Business Wallets.

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([2]),

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) In its Communication of 29 January 2025 'A Competitiveness Compass for the EU'([3]) 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 and perform business transactions.

---

[2] OJ C 365, 23.9.2022, p. 18.

[3] 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.

(2) Regulation (EU) No 910/2014 of the European Parliament and of the Council([4]) establishes the European Digital Identity Framework and introduces the European Digital Identity Wallets, enabling European Business Wallet 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 among economic operators as well as between those and public sector bodies in different configurations.

(4) In order to ensure the interoperability, trustworthiness 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 Recommendation (EU) 2021/946, and in particular the Architecture and Reference Framework, should apply, where appropriate, with the specifications laid down in this Regulation taking precedence in the event of any inconsistency.

---

[4] 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).

(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 European Business Wallets and existing systems and solutions at both Union and national level. This work should be supported by the European Digital Identity Cooperation Group. 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, 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 as well as enabling the reuse of the same trusted functionalities in business-to-business settings. The principle of legal equivalence established in this Regulation should apply horizontally across the entirety of the Regulation. In this respect, the principle should only apply to actions resulting from the use of the core functionalities of the European Business Wallets that are functionally equivalent to those carried out in person, in paper form, or through other means and that service the same purpose as their traditional counterparts. This includes, for example, the use of qualified electronic signatures, seals, and electronic attestations of attributes that have the same legal value as their manual or physical equivalents. The use of the core functionalities of the European Business Wallets to identify and authenticate, sign or seal, request or share electronic attestations of attributes, 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. To that effect, this Regulation should also be understood to be without prejudice to legal, administrative or procedural requirements which oblige economic operators to fulfil an administrative requirement or submit documents in a particular electronic form. The principle of legal equivalence ensures that actions carried out via the core functionalities of the European Business Wallets have the same legal effect and validity as equivalent actions, while remaining subject to applicable legal, administrative, or procedural requirements. Such requirements should not be applied in a manner that has the effect of excluding the use of the core functionalities of the European Business Wallets solely on the basis of their digital nature. 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, existing interfaces, and their needs for interoperability. This approach allows public sector bodies to maintain their existing operational frameworks, including where administrative procedures are currently fulfilled electronically by other existing digital tools and services. This approach should also allow public sector bodies to maintain existing interfaces while benefiting from the advantages of the European Business Wallets. However, this flexibility should be exercised with due regard to the principle of proportionality and the need to avoid imposing disproportionate technical or administrative burdens, especially on micro-enterprises and small and medium enterprises.

(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 and crime prevention.

(10) This Regulation should be without prejudice to the right of legal persons to submit information only once 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([5]) and Directive (EU) 2017/1132 establishing the Business Registers Interconnection System**.**

---

[5] 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)

(11) In order to reduce administrative burden and improve competitiveness, all entities conducting economic activities, for purposes related to their trade, business, craft or profession, and regardless of their method of financing or legal form, such as 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. Such economic operators can become European Business Wallet owners through various methods, for example through ownership, license, subscription or any other agreement granting a right of use of such a European Business Wallet.

(11a) 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 28th Regime([6]) 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 European 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 European 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 under this Regulation, is necessary. Such an inclusion should create a coherent 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. In such cases, the Commission should be tasked to supervise the provision of European Business Wallets by Union entities other than Union institutions.

---

[6] European Commission, Call for Evidence: *28th regime – a single harmonized set of rules for innovative companies throughout the EU*, 8th 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

(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. The identification and authentication within the European Business Wallets framework should rely on electronic attestations, issued by trusted entities, which attest to the identity, attributes or specific roles of a natural or legal person using these solutions and enable their verification in accordance with the requirements of this Regulation.

(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) No 910/2014, which establishes that qualified electronic signatures shall have the equivalent legal effect of a handwritten signature.

(18) To support the delegation of powers within a professional context, the European Business Wallets should incorporate an authorisation and role-based 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 European Business Wallet. That system should enable economic operators and public sector bodies to assign rights to European Business Wallet users through clearly defined technical authorisations 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 authorisation, allowing the owner of a European Business Wallet to assign roles and responsibilities to various European Business Wallet users 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**7**. 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 European Business Wallet 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. This system should govern access to services and transactions within the European Business Wallet, preserving the integrity of the owners' identities. Such authorisations granted through the systems should be understood to be of a technical nature and to not create, limit, or otherwise affect any power of attorney or legal mandate provided under applicable national or Union law and procedures.

---

7 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).

(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 European Business Wallet 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. Providers of European Business Wallets should also provide accessibility for persons with disabilities, including in accordance with Annex I of Directive (EU) 2019/882, to the extent relevant. 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([8]) and should include the powers to define the necessary standards and protocols for the secure communication channel, taking into account the latest technological developments.

---

[8] 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: https://eur-lex.europa.eu/eli/reg/2011/182/oj).

(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 European Business Wallets to hold and transmit evidence retrieved from competent public authorities using components of the Once-Only Technical System. Where appropriate, economic operators should also be able to combine evidence held in the European Business Wallets 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 between public sector bodies of such documents retrieved through the 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 European Business Wallets should be maintained through the European 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, notified electronic identification means and electronic attestations of attributes for onboarding to and access management of the European Business Wallets. This should enable European Business Wallet 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 European Business Wallet 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, storage and verification 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 interoperability and security 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. Providers are encouraged to release the source code of the application software of European Business Wallets under an open source license.

(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 set 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. Such implementing acts should act as guidance for the appropriate organisational and technical measures that Member States should take in order to enable the use of the core functionalities of European Business Wallets and meet their obligations under this Regulation.

(30) To ensure the appropriate level of trust, functionality, and security of European Business Wallets for the cross-border provision of their services, including 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. To that end, the European Commission should be empowered to adopt implementing acts in order to establish a list of reference standards and, where necessary, specifications and procedures for providers of European Business Wallets. Those implementing acts should cover, in particular, the implementation of European Business Wallets, the management of direct or indirect risks related to the provision of European Business Wallets, registration and onboarding procedures for European Business Wallets. To ensure that risks are assessed consistently across the Union and that providers take tailored measures based on the sector, use case, interface security and service availability of their European Business Wallets, the Commission should be empowered to adopt implementing acts setting common procedures, a risk register and criteria for risk assessments and self-assessments. In order to avoid unnecessary duplication and administrative burden, applicants should be able to rely on certifications, self-assessments and documentation already carried out under other applicable Union law, such as Regulation (EU) No 910/2014 and Regulation (EU) 2024/2847, where those cover requirements or risks that correspond to the requirements set out in this Regulation. Applicants should take into account the practical context in which the European Business Wallets will be used, including any relevant security requirements that apply under national law for the specific service or procedure concerned.

(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 submit an application for authorisation 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 and have their principal place of business and main operations in 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 European Business Wallet 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 or acute security risk due to the potential interference from third countries. To that end, it is necessary to reduce the risk of strategic dependencies 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 issuing 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 European Business Wallet 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([9]) and Commission Implementing Regulation (EU)2021/369([10]) as well as Regulation (EU) 2024/1624([11]) and Commission Implementing Regulation (EU) 2021/369([12]). 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.

---

[9] 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: https://eur-lex.europa.eu/eli/dir/2017/1132/oj

[10] 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: https://eur-lex.europa.eu/eli/reg/2024/1624/oj)

[11] 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: https://eur-lex.europa.eu/eli/reg/2024/1624/oj

[12] 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: https://eur-lex.europa.eu/eli/reg_impl/2021/369/oj

(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 empowered to set up and maintain this European Digital Directory, as a trusted source of information on economic operators and public sector bodies using European Business Wallets. The European Digital 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. Providers of European Business Wallets, 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, providers of electronic attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source, and authentic sources, to ensure that the data submitted remains accurate. Such actions should not indirectly create a requirement for economic operators to update such information. In this regard the European Digital Directory will rely on the information made available by business registers including but not limited to those accessible through BRIS while ensuring that such information will not be duplicated. In order to ensure that public sector bodies can enable the use of European Business Wallets and meet their obligations under this Regulation, they are required to be identified and be contacted by economic operators using core functions of the European Business Wallet ecosystem. To that effect, public sector bodies that are not owners of European Business Wallets should be issued a unique identifier, a digital address and be listed in the European Digital Directory.

(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 operation of 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 balance regulatory burdens and security, supervision of providers of European Business Wallets and monitoring of their activities should be provided for, while requiring prior assessment of their operations. This approach should allow for a more flexible and efficient regulatory environment, while maintaining the necessary safeguards to protect European Business Wallet users and ensure compliance with the requirements of the European Business Wallets framework. The authorisation process for providers of European Business Wallets should be streamlined and efficient, with clear requirements and timelines for applicants. As part of this authorisation process, applicants that intend to provide European Business Wallets should demonstrate compliance with the requirements set out in Articles 5, 6, and 7 through a self-assessment report and supervisory bodies should assess whether the requirements of this Regulation are met. The Commission should provide guidance on the self-assessment report to ensure consistency and facilitate the assessment of the application by supervisors. 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 authorised 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 authorisation process. Making that information publicly available should enable European Business Wallet 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, and in order to ensure the application and enforcement of this Regulation to providers of European Business Wallets other than Union entities, Member States should designate a competent authority to act as the supervisory body for the application and enforcement of this Regulation. In this regard, Member States may establish new authorities or rely on existing authorities established in their territory or designate, upon mutual agreement with another Member State, a supervisory body established in that other Member State.

(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([13]). 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.

[13] 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: https://eur-lex.europa.eu/eli/dir/2022/2555/oj)

(44) To ensure 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 24 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 European Business Wallet owners, it is necessary to establish a mechanism enabling the Commission to intervene in cases where a provider of European Business Wallets is systematically non-compliant with the requirements of this Regulation and where the relevant competent authorities have failed to take effective, timely and proportionate remedial measures. In such circumstances, and where the nature or persistence of the non-compliance may adversely affect the internal market, an intervention at Union level should be justified in order to ensure uniform and effective application of this Regulation. To that end, the Commission should be empowered to carry out an evaluation of compliance in cooperation with the relevant national authorities and the provider concerned. That evaluation should take due account of the nature, gravity and duration of the non-compliance, its actual and potential impact on the internal market as well as the rights of the affected European Business Wallet owners, in accordance with the principles of proportionality and due process. Where the evaluation confirms that the conditions for Union intervention are met, the Commission should, following consultation with the Member States and the provider and following the opportunity for the provider to remedy the non-compliance, be able to adopt a decision to temporarily suspend the provider from the list of trusted providers established under Article 12. On the basis of such a decision, the relevant supervisory authorities should take the necessary measures to ensure that the provider complies with this Regulation and they should report in a timely manner to the Commission on the measures taken and their outcome. Where remedial actions are proven to be effective, the Commission should end the suspension of the provider from the list within two working days of receiving the proof of compliance.

(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 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 Business Wallets' secure communication channel. To ensure seamless and interoperable application of this Regulation in this regard, public sector bodies should enable the use of 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) *deleted*

(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[14].

(55) Regulation (EU) No 910/2014 offers a secure and convenient means for Union citizens and residents in the Union as defined by national law, 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 amendment 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.

---

[14] 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).

(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 5 years after entry into force of this Regulation] 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 Wallets, as well as the implementation and effectiveness of the rules on penalties established by Member States, to evaluate market developments and compliance levels.

(58) Since the objectives of this Regulation cannot be sufficiently achieved by the Member States but can rather, by reason of the scale or effects of the action, be better achieved at Union level, the Union may adopt measures, in accordance with the principle of subsidiarity as set out in Article 5 of the Treaty on European Union. In accordance with the principle of proportionality as set out in that Article, this Regulation does not go beyond what is necessary in order to achieve those objectives.

(59) 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([15]), and delivered an opinion on 20 January 2026.

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, providing for the legal effect of actions and transactions carried out through a European Business Wallet to be equivalent 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 Wallet owners to whom the European Unique Identifier is not available;

[15] 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: https://eur-lex.europa.eu/eli/reg/2018/1725/oj).

(6) lays down the authorisation mechanism under which providers of European Business Wallets shall be allowed to offer such wallets;

(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 to other Union entities;

(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 or national law governing the exchange of documents and data between competent authorities.

2a. This Regulation is without prejudice to actions taken by Member States for public order and public security purposes and defence.

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 receive, store, manage, combine and present European Business Wallet owner identification data and electronic attestations of attributes to European Business Wallet-relying parties for the following purposes:

(a) to authenticate and provide the European Business Wallet owner identification data required by a European Business Wallet 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 create, manage and delegate authorisations to European Business Wallet users;

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 issuing European Business Wallet owner identification data;

(4) ‘economic operator’ means any natural or legal person, including but not limited to companies, partnerships, foundations, associations as well as sole-traders and self-employed persons or a group of such persons, acting in a commercial or professional capacity;

(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 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 a European Business Wallet;

(8) ‘trust service’ means trust service as defined in Article 3, point (16) of Regulation (EU) No 910/2014;

(9) ‘attribute’ means attribute as defined in Article 3, point (43) of Regulation (EU) No 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 electronic attestation of attributes’ means qualified electronic 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 a qualified electronic seal as defined in Article 3, point (27) of Regulation (EU) No 910/2014;

(17) ‘qualified electronic time stamp’ means a qualified electronic time stamp as defined in Article 3, point (34) of Regulation (EU) No 910/2014;

(18) *deleted*

(19) ‘authorisation’ means the granting or recognition of a right or permission by a European Business Wallet owner to a European Business Wallet user to perform specified actions on specified resources or functionalities, and the corresponding access-control decision that permits each concrete request in accordance with applicable access-control policy and any required conditions 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) ‘European Business Wallet user’ means a natural or legal person, or a natural person representing another natural person or a legal person, that uses European Business Wallets 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) ‘European Business 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 provided by a provider of European Business Wallets 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;

(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) *deleted*

(29) *deleted*

(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 an 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;

(33a) ‘significant incident’ means an incident within the meaning of Article 23(3) of Directive (EU) 2022/2555;

(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 electronic attestations 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 public sector bodies and economic operators;

(38) ‘API’ or ‘Application Programming Interface’ means a set of definitions and protocols for building and integrating application software to share data;

(39) ‘submission’ means any transmission of structured or unstructured data, files, forms, or records between a public sector body and an economic operator, 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, 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, an authorisation, a service or a benefit from a public sector body in the exercise of administrative functions;

(42) ‘European Business Wallet front-end’ means the European Business Wallet user interface component, regardless of platform or form factor, that interacts with European Business Wallet users 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 front-end, 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 or authorised European Business Wallet user makes use of any of the qualified trust services forming part of 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.

Where existing EU or national law includes requirements relating to electronic formats as part of an administrative procedure, such requirements remain applicable and shall be observed.

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 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) securely request and share European Business Wallet owner identification data and electronic attestations of attributes between European Business Wallets, 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) have electronic attestations of attributes securely issued by the provider on behalf of the European Business Wallet owner. Such attributes shall relate to data for which the European Business Wallet owner is the primary source to European Business Wallets and European Digital Identity Wallets;

(g) link electronic attestations of attributes issued pursuant to point (f) to other electronic attestations of attributes 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 European Business Wallet users to authenticate themselves;

(i) transmit and receive electronic documents and data by means of the qualified electronic registered delivery service set out in the Annex;

(j) authorise multiple European Business Wallet users to access and operate the European Business Wallet of the owner, and for the European Business Wallet owner to manage and revoke authorisations, including authorisations associated to roles for the purposes of access to and operation of the European Business Wallet and without prejudice to any power of attorney or legal mandate;

(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 transaction records, in a structured, commonly used and machine-readable format, in the event of termination of service or revocation of the notification of the provider of the European Business Wallet;

(la) import their data as listed under point (l) to benefit from data portability across European Business Wallet providers;

(m) access a log of all communications and transactions;

(n) access a 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 the requirements set out in the Annex.

5. By [Publications Office, insert the date – 1 year after entry into force of this Regulation] 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, including those critical for interoperability and security and those relevant for Member States' compliance with Article 16, 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, electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source 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 European Business Wallet user action;

   (e) to securely onboard the European Business Wallet owner remotely via a legal representative or other persons that are lawfully empowered to carry out the onboarding process with an electronic identification means, as defined in Article 3, point (2) of Regulation (EU) No 910/2014, and that meets the requirements of Regulation (EU) No 910/2014 with regard to the assurance level ‘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 verification of the authenticity and validity of the European Business Wallets;

(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 European Business Wallet unit attestations to all European Business Wallet units;

1a. Providers of European Business Wallets shall provide, as a standalone service, to requesting public sector bodies that are not owners of European Business Wallets, a unique digital address for the purposes of being listed in the European Digital Directory and of enabling the qualified electronic registered delivery service referred to in Article 5(1), point (i).

2. Providers of European Business Wallets shall also:

(a) ensure that the European Business Wallet owner identification data is cryptographically bound 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 between European Business Wallets.

(c) ensure security-by-design;

(d) provide a mechanism enabling European Business Wallet owners to easily request technical support and report technical problems having a negative impact on the use of European Business Wallets;

(e) provide validation mechanisms, in order to ensure that the authenticity and validity of European Business Wallets can be verified;

(ea) make the European Business Wallets they provide accessible for use, by persons with disabilities, on an equal basis with other users.

(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(3).

(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 and the relevant implementing acts as set forth in this Regulation.

5. By [Publications Office, insert the date – 1 year after entry into force of this Regulation] 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, including those critical for interoperability and security, such as for the exchange of data on authorisations with national registers, and those relevant for Member States' compliance with Article 16, 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(3).

2. 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.

2a. By [Publications Office, insert date 8 months after entry into force of this Regulation] the Commission shall, by means of implementing act, specify the tools, indicators and assessment frameworks suitable for determining whether providers of European Business Wallets present risks to the security of the Union within the meaning of this Article, including for the purpose of assessing whether such providers are subject to control by a third country or by a third-country entity. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19.

3. Providers of European Business Wallets shall comply with the requirements set out in Article 19a of Regulation (EU) 910/2014.

4. *deleted*

5. Providers of European Business Wallets shall comply with [applicable cybersecurity requirements / Cybersecurity Act] 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 and availability of the European Business Wallets they provide as well as their interoperability 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 European Business Wallet owners and their authorised European Business Wallet users 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 European Business Wallet unit attestation, using the authentication mechanism provided for 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 Articles 13(10) and 15(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 15(1), of any substantive changes to their services, including the intention to cease the activities, 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 services offered by the providers of European Business Wallets and of the removal of the providers of European Business Wallets from the list established pursuant to Article 12(3) and ensure the transfer or deletion of the European Business Wallet owner data in accordance with the European Business Wallet owner's 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 by the providers of the European Business Wallet owner identification data through the issuance of the unique identifiers referred to in Article 8(5), point (b);

6a. Providers of European Business Wallets shall maintain a documented and up-to-date version of the risk-assessment referred to in Article 11(2a), following the procedures and criteria set out in the implementing acts referred to in Article 11(2c).

6b. Providers of European Business Wallets shall update, following the procedures and criteria set out in the implementing acts referred to in Article 11(2c), the self-assessment referred to in Article 11(2aa) every 24 months or immediately where:

(a) a significant incident has occurred;

(b) a substantial change is made to the architecture, security functions, cryptographic components, critical suppliers or core functionalities of the European Business Wallet;

(c) a function affecting the security, validity, authenticity or portability of the European Business Wallet is suspended, revoked or materially modified;

(d) the risk assessment referred to in paragraph 6a identifies a new risk.

6c. By [Publications Office, insert the date – 1 year after entry into force of this Regulation] the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for paragraph 3. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19.

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.

1a. 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 or the intermediary platform acting on behalf of them, 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 electronic 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. By [Publications Office, insert the date – 1 year after entry into force of this Regulation] the Commission shall, 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(5), 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 for the purposes of European Business Wallet owner identification data shall, upon request from the economic operator or public sector body or upon the provision of a European Business Wallet to this entity, be created in accordance with paragraph 4.

3. Where a public sector body is a Union entity, the Commission shall create and attribute a unique identifier for the purposes of European Business Wallet owner identification data to that Union entity in accordance with paragraph 4.

4. By [Publications Office, insert the date – 1 year after entry into force of this Regulation] the Commission shall, by means of implementing acts, establish specifications, requirements and procedures relating to the unique identifier referred to in paragraph 2 and 3 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 European Business Wallet users through an 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 paragraph 3a and the implementing acts referred to in paragraph 6.

3. The Commission shall ensure that the relevant information shall be included in the European Digital Directory.

3a. Providers of European Business Wallets shall provide at least the following information to the Commission upon the issuance of a European Business Wallet to a European Business Wallet owner:

   (a) the official name of the European Business Wallet owner as stated in the national register of the owner's country of establishment or habitual residence;

   (b) the unique identifier referred to in Article 9;

(c) the unique digital address or addresses referred to in point (j) of paragraph 1 of Article 6;

(d) the European Business Wallet owner's country of establishment.

3b. To ensure compliance with the obligations laid down in Article 16, where a public sector body is not a European Business Wallet owner it shall provide to the Commission the following information for the purpose of its inclusion in the European Digital Directory:

(a) the official name of the public sector body;

(b) the unique identifier referred to in Article 9;

(c) the unique digital address or addresses referred to in paragraph 1a of Article 6;

(d) the public sector body's country of establishment.

4. The Commission shall make the European Digital Directory accessible to European Business Wallet owners, their authorised European Business Wallet users, providers of European Business Wallets and Member State authorities.

4a. European Business Wallet providers shall, at least once every 72 hours, verify the European Business Wallet owner information referred to in paragraph 3a, where applicable using verification mechanisms or notifications made available by the relevant authentic sources.

5. Any modification or revocation concerning the information referred to in paragraph 2 shall be communicated by the providers of the European Business Wallet directly to the Commission for the purpose of maintaining the European Digital Directory, without undue delay and, in any event, one working day following receipt of such information pursuant to paragraph 4a.

6. By [Publications Office, insert the date – 1 year after entry into force of this Regulation] 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

Authorisation of providers of European Business Wallets

1. Entities that intend to provide European Business Wallets shall submit an application for authorisation together with the information listed in paragraph 2 to the competent supervisory body.

2. The application 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) the self-assessment report including referred to in paragaph 2aa, which shall include:

(i) a description of termination plans in cases where a provider of European Business Wallets ceases its activities, including of how information is kept accessible;

(ii) the policies and corresponding measures to manage risks to the provision of European Business Wallets as referred to in Article 7(3).

(iii) the policies and corresponding measures implemented to address the risks identified in the risk assessment referred to in paragraph 2a;

2a. Applicants shall, following the procedures and criteria set out in the implementing acts referred to in paragraph 2c of this Article, perform a risk assessment covering the European Business Wallet solution they intend to provide as a whole, including risks arising from its design, development, deployment, operation, maintenance, interoperability, dependencies and termination. Where applicants have carried out risk assessments pursuant to other applicable Union law covering risks corresponding to those referred to in this Regulation or the implementing acts referred to in Article 11, they shall not be required to carry out a further risk assessment to the same effect and may submit that risk assessment as part of the self-assessment report.

2aa. Applicants shall demonstrate conformity with the requirements in Article 5, 6, 7 and the Annex through a self-assessment report resulting from a self-assessment of conformity with those requirements, including, where applicable, a self-assessment report provided by third parties from which the applicant sources the services falling under Articles 5, 6, 7 and the Annex and which the applicant does not itself provide directly with the requirements that apply to them.

2b. Where applicants or a third party from which the applicant sources the relevant qualified trust services, already demonstrate compliance with requirements for qualified trust services established pursuant to Regulation (EU) No 910/2014 corresponding to those listed in Articles 5, 6, 7 and the Annex of this Regulation, and have a valid conformity assessment report or certificate from a conformity assessment body pursuant to Regulation (EU) No 910/2014, applicants shall submit those conformity assessment reports or certificates as part of the self-assessment report. In respect of those corresponding requirements, applicants shall not be required to carry out a further self-assessment to the same effect.

2c. The Commission shall by [Publication Office, insert the date 1 year from the date of application of this Regulation], by means of implementing acts, specify the procedures, assessment criteria and a risk register for the risk assessment and the self-assessment report referred to in paragraph 2, including how to take into account differences in use cases or sectors, test specifications for interfaces, and service availability requirements. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 19.

3. *deleted*

4. Upon receipt of an application for authorisation, the supervisory body shall have 60 days to review the information submitted.

When that application for authorisation leads the supervisory body to conclude that the information is complete and the requirements of this Regulation are met, 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(3).

5. When that application for authorisation leads the supervisory body to conclude that the information is not complete or the requirements of this Regulation are not met, it shall request additional information or explanations from the applicant 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 requirements of this Regulation are met, it shall inform the Commission within ten working days with a view to the addition of that provider to the list referred to in Article 12(3). If not, or no response is received, the supervisory body shall inform the applicant that it will not be added to the list referred to in Article 12(3).

6. Where the supervisory body has not provided the applicant with a substantive response on the outcome of the application for authorisation referred to in paragraph 4 within 60 calendar days of receiving the application for authorisation, the supervisory body shall, without undue delay, inform the applicant of the reasons for the delay and the period within which the review is to be concluded, which shall not exceed 20 calendar days. Following this period, the supervisory body shall come to a conclusion as to the application and inform the applicant to that effect without undue delay.

7. Member States shall ensure that applicants have the right to an effective judicial remedy against a decision of the supervisory authority, or lack thereof, 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 authorised providers of European Business Wallets

1. Supervisory bodies shall inform the Commission of any changes to the information provided pursuant to Article 11, within 3 working days 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 authorised provider of European Business Wallets not previously present on the list referred to in paragraph 3;

   – a change to previously submitted information regarding providers of European Business Wallets currently present on the list referred to in paragraph 3;

   – a request to remove a provider of European Business Wallets from the list referred to in paragraph 3;

   (b) the 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 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. Upon receiving the information from the supervisory bodies pursuant to Article 11(4)(5)(6) with a view to the addition of a provider to the list, the Commission shall include the provider in the list within two working days. Further to the notification under Article 13(5)(k), the Commission shall revoke the inclusion of the non-compliant provider in the list within two working days.

Article 13

Supervision and penalties

1. Each Member State shall designate a competent authority to act as the supervisory body for the application and enforcement of this Regulation. Member States may establish new authorities or rely on existing authorities established in their territory or designate, upon mutual agreement with another Member State, a supervisory body established in that other Member State.

2. *deleted*

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 supervisory bodies referred to in 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 other than Union entities in line with paragraph (5);

5. The tasks of the supervisory bodies referred to in paragraph 1 and their role pursuant to paragraph (4) shall include the following:

(a) review and assess the applications 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 incident of which it becomes aware in the performance of its tasks and, in the case of a significant incident 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) *deleted*

(k) notify the Commission if the supervisory body determines that a provider of European Business Wallets 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 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 24 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 if imposing 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. Member States may lay down the rules on whether and to what extent administrative fines may be imposed on national public authorities and bodies established in that Member State.

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 24 months after the entry into force of this Regulation] and, without delay, any subsequent amendment law or amendment affecting them.

10. Where a provider of European Business Wallets other than Union entities is systematically non-compliant with the requirements of this Regulation and no effective measures have been taken by the supervisory bodies, and such circumstances justify an immediate intervention to preserve the proper functioning of the internal market, the Commission shall carry out an evaluation of compliance in cooperation with the supervisory body. The Commission shall inform the provider accordingly and the provider shall cooperate as necessary.

11. Based on the evaluation, taking into account the nature and severity of the non-compliance, as well as its potential impact on the internal market and the rights of affected European Business Wallet owners, the Commission, by means of a Commission decision, after consulting the Member States concerned and the provider, may temporarily suspend the provider from the list referred to in Article 12. Before adopting the decision, the Commission shall consult the Member States concerned and the provider, and shall afford the provider the opportunity to remedy the non-compliance.

11a. Based on this decision, the supervisory body concerned shall take measures to ensure that the provider complies with the Regulation and it shall report to the Commission in relation to such measures. Where remedial actions are proven to be effective, the Commission shall end the suspension of the provider from the list within two working days of receiving the proof of compliance.

12. *deleted*

13. *deleted*

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, it shall comply with the requirements laid down in this Regulation.

1a. The Commission shall be the supervisory body for Union entities other than Union institutions. It shall act with complete independence in performing its tasks in accordance with this Regulation.

2. The role of the Commission acting as a supervisory body in accordance with paragraph 1a 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 1a, the Commission shall perform the tasks referred to in Article 13(5) points a, b, c, d, h.

   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

1. 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.

1a. For the purpose of paragraph 1, Member States shall take appropriate organisational and technical measures that enable the use of the core functionalities of European Business Wallets.

2. *deleted*

3. *deleted*

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 solutions offering an equivalent level of security and similar functions to the European Business Wallets 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 solutions are interoperable with the trust framework laid down in Regulation (EU) No 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 an equivalent level of security and 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) No 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 carry out an assessment of the third-country solution, system or framework, taking into account, at least, data protection standards, compliance with cybersecurity requirements and the independence of the third-country system and its providers from the control of high-risk governments. Such assessment shall be used to determine 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

Provision 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 from a provider of European Business Wallets, that provider shall notify this request to the supervisory body of the Member State in which it is authorised.

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 and their representative empowered to carry out the onboarding process 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. National supervisory bodies 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. National supervisory bodies may make use of the European Digital Directory for that purpose.

6a. The Commission shall establish standards and technical specifications for issuing of European Business Wallet owner identification data, including unique identifiers, to economic operators established outside the Union as part of the implementing acts referred to in Articles 8(9) and 9(4).

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. Where reference is made to this paragraph, Article 5 of Regulation (EU) 182/2011 shall apply.

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

1. The Commission shall review the application of this Regulation and shall, by [Publications Office, insert the date – 5 years after entry into force of this Regulation], 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 including, where available, information on time and cost savings, as well as uptake by all economic actors, including a specific assessment of the impact of this Regulation on micro-enterprises and small and medium-sized enterprises. 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.

2. 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 authorisation 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

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

1a. Articles 5(5), 6(5), 7(6c), 8(7), 9(4), 10(6), 11(2c), 13, 19, 20 and 21 shall apply from [Publications Office, insert the date of entry into force].

1b. Chapter I, II, III, IV and V, with the exception of Articles 5(5), 6(5), 7(6c) 8(7), 9(4), 10(3b), 10(6), 11(2c), 13, 16, 19 and 20 shall apply from [Publications Office, insert the date – 1 year after the date of application of the last implementing act referred to in articles 5(5), 6(5), 7(6c), 8(7), 9(4), 10(6), 11(2c)].

1c. Articles 10(3b) and 16 shall apply from [Publications Office, insert the date – 2 years after the date of application of the last implementing acts referred to in articles 5(5), 6(5), 7(6c), 8(7), 9(4), 10(6), 11(2c)].

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

Done at Brussels,

For the European Parliament	*For the Council*
The President	*The President*

ANNEX

Requirements for core 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 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 any other functionalities shall be made accessible to the **European Business Wallet** 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 European 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) *deleted*

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 European Business Wallet's cryptographic operations involving critical assets other than those needed for the European Business Wallets unit to authenticate the European Business Wallet owner only in cases where those applications have successfully authenticated European Business Wallet users;

(b) *deleted*

(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) *deleted*

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 European Business Wallet 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 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 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 European 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 European Business Wallet-relying party and the Member State in which that European Business Wallet-relying party is established, if available, or in case of other Wallets units, relevant information from the European Business 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**,** availability and confidentiality of the logged information.

(4) European Business Wallets back-end shall log reports sent by the European Business Wallet user to the competent authorities via the European Business 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 European Business 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 European Business Wallet 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 European Business Wallet unit.

(2) Providers of European Business Wallets shall ensure that European Business Wallet 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 providers of European Business Wallets, by providers of trust services or by European Business Wallet-relying parties.

(2) Signature creation applications shall have the following functions:

(a) signing or sealing data provided by European Business Wallet 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 European Business Wallet 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, IMPORT AND PORTABILITY

European Business Wallets shall support the secure export, import and portability of an owner's European Business Wallet data in at least an open format, while ensuring European Business Wallet users have been successfully authenticated as per point 1 of this Annex. This shall enable the owner to migrate their data to another European Business Wallet solution.

11. SECURE LEGAL COMMUNICATION CHANNEL FOR THE EUROPEAN BUSINESS WALLET

(1) In line with Article 5 of this Regulation, European 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 the protocol and set out standards and specifications for compliant implementations of the specific 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 European Business Wallets and the designated qualified electronic registered delivery service shall be mandatory. Providers of European 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 **e**nables 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 between European Business Wallets.

(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 European Digital Identity Wallets relying-party access certificates or European Digital Identity 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 European Business Wallet users' information contained in the European Digital Identity Wallets relying party access certificates or in the European Digital Identity Wallets unit attestations where applicable;

(3) display to European Business Wallet users, where applicable, the attributes that European Business Wallet users are requested to present;

(4) present European Business Wallet unit attestations of the European Business Wallet unit to European Business Wallet relying parties or European Business Wallet units that request it.

14. ISSUANCE OF ELECTRONIC ATTESTATIONS OF ATTRIBUTES TO EUROPEAN BUSINESS WALLET UNITS

(1) In line with Article 5 of this Regulation, providers of European Business Wallets shall ensure that European 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 European Business Wallet unit, providers of European Business Wallets shall ensure that the following requirements are complied with:

(a) where European Business Wallets owners, through their European Business Wallet unit, request from the provider of the European Business Wallet the issuance of European Business Wallets owner identification data or of electronic attestations of attributes from providers of European Business Wallets owner identification data or providers of electronic attestations of attributes that enable issuance of European Business Wallets owner identification data or electronic attestations in more than one format, the European Business Wallet unit shall request it in all formats referred to in Article 8 to this Regulation laying down rules for the application of the European Business Wallets Regulation as regards the integrity and core functionalities of European Business Wallets;

(b) where European Business Wallet owners use their European Business Wallet unit to interact with competent national authorities and providers of electronic attestations of attributes, European Business Wallet units shall enable authentication and validation of the European Business Wallet unit components by presenting the European Business Wallet unit attestations to those competent national authorities and providers upon their request;

(c) European Business Wallet solutions shall support mechanisms that enable providers of European Business Wallets Owner Identification Data to verify issuance, delivery and activation in compliance with assurance level high requirements set out in Commission Implementing Regulation (EU) 2015/1502 (2.2);

(d) European Business Wallet units shall verify the authenticity and validity of European Business Wallet 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, providers of European Business Wallets shall ensure that:

(1) European Business Wallet solutions support protocols and interfaces for the presentation of attributes to European Business Wallet-relying parties in accordance with the standards defined in the implementing acts;

(2) At the request of European Business Wallet users, European Business Wallet units respond to successfully authenticated and validated requests from European 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 EUROPEAN BUSINESS WALLET UNITS

(1) providers of European Business Wallets shall ensure that Business Wallet 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) providers of European Business Wallets shall ensure that European Business Wallet owner identification data that they issue is cryptographically bound to the European Business Wallet unit to which it is issued.

17. ISSUANCE OF ELECTRONIC ATTESTATIONS OF ATTRIBUTES TO EUROPEAN BUSINESS WALLET UNITS

(1) Electronic attestations of attributes issued to European Business Wallet 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 Wallet units.

(3) Providers of electronic attestations of attributes shall ensure that electronic attestations of attributes issued to European Business Wallet units contain the information necessary for authentication and validation of those electronic attestations of attributes.