EUROPEAN UNION

THE EUROPEAN PARLIAMENT **THE COUNCIL**

Brussels, 13 March 2024
(OR. en)

2021/0136 (COD) **PE-CONS 68/23**

TELECOM 351
COMPET 1163
MI 1028
DATAPROTECT 329
JAI 1550
CODEC 2237

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject:	REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

REGULATION (EU) 2024/…
OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of …

amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework

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[1],

Having regard to the opinion of the Committee of the Regions[2],

Acting in accordance with the ordinary legislative procedure[3],

---

1 OJ C 105, 4.3.2022, p. 81.
2 OJ C 61, 4.2.2022, p. 42.
3 Position of the European Parliament of 29 February 2024 (not yet published in the Official Journal) and decision of the Council of ...

Whereas:

(1) The Commission Communication of 19 February 2020 entitled ‘Shaping Europe’s Digital Future’ announces a revision of Regulation (EU) No 910/2014 of the European Parliament and of the Council[4] to improve its effectiveness, extend its benefits to the private sector and promote trusted digital identities for all Europeans.

(2) In its conclusions of 1-2 October 2020, the European Council called on the Commission to propose the development of a Union-wide framework for secure public electronic identification, including interoperable digital signatures, to provide people with control over their online identity and data as well as to enable access to public, private and cross-border digital services.

(3) The Digital Decade Policy Programme 2030, established by Decision (EU) 2022/2481 of the European Parliament and of the Council[5], sets the objectives and digital targets of a Union framework which, by 2030, are intended to lead to wide deployment of a trusted, voluntary, user-controlled digital identity that is recognised throughout the Union and allows every user to control their data in online interactions.

---

[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).

[5] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030 (OJ L 323, 19.12.2022, p. 4).

(4) The ‘European Declaration on Digital Rights and Principles for the Digital Decade’ proclaimed by the European Parliament, the Council and the Commission[6] (the ‘Declaration’), underlines everyone’s right to access digital technologies, products and services that are safe, secure, and privacy-protective by design. This includes ensuring that all people living in the Union are offered an accessible, secure and trusted digital identity that enables access to a broad range of online and offline services, protected against cybersecurity risks and cybercrime including data breaches and identity theft or manipulation. The Declaration also states that everyone has the right to the protection of their personal data. That right encompasses the control on how the data is used and with whom it is shared.

(5) Union citizens and residents in the Union should have the right to a digital identity that is under their sole control and that enables them to exercise their rights in the digital environment and to participate in the digital economy. To achieve that aim, a European digital identity framework should be established allowing Union citizens and residents in the Union to access public and private online and offline services throughout the Union.

(6) A harmonised digital identity framework should contribute to the creation of a more digitally integrated Union by reducing digital barriers between Member States and by empowering Union citizens and residents in the Union to enjoy the benefits of digitalisation, while increasing transparency and the protection of their rights.

---

6 OJ C 23, 23.1.2023, p. 1.

(7) A more harmonised approach to electronic identification should reduce the risks and costs of the current fragmentation due to the use of divergent national solutions or, in some Member States, the absence of such electronic identification solutions. Such an approach should strengthen the internal market by allowing Union citizens, residents in the Union, as defined by national law, and businesses to identify themselves and to provide authentication of their identity online and offline in a safe, trustworthy, user-friendly, convenient, accessible and harmonised way, across the Union. The European Digital Identity Wallet should provide natural and legal persons across the Union with a harmonised electronic identification means enabling authentication and the sharing of data linked to their identity. Everyone should be able to access public and private services securely, relying on an improved ecosystem for trust services and on verified proofs of identity and electronic attestations of attributes, such as academic qualifications, including university degrees, or other educational or professional entitlements. The European Digital Identity Framework is intended to achieve a shift from the reliance on national digital identity solutions only, to the provision of electronic attestations of attributes valid and legally recognised across the Union. Providers of electronic attestations of attributes should benefit from a clear and uniform set of rules, while public administrations should be able to rely on electronic documents in a given format.

(8) Several Member States have implemented and use electronic identification means that are accepted by service providers in the Union. Additionally, investments have been made in both national and cross-border solutions on the basis of Regulation (EU) No 910/2014, including the interoperability of notified electronic identification schemes pursuant to that Regulation. In order to ensure the complementarity and fast adoption of European Digital Identity Wallets by current users of notified electronic identification means and to minimise the impact on existing service providers, European Digital Identity Wallets are expected to benefit from building on the experience gained with existing electronic identification means and from the infrastructure of notified electronic identification schemes deployed at Union and national level.

(9) Regulation (EU) 2016/679 of the European Parliament and of the Council[7] and, where relevant, Directive 2002/58/EC of the European Parliament and of the Council[8] apply to all personal data processing activities under Regulation (EU) No 910/2014. The solutions under the interoperability framework provided in this Regulation also comply with those rules. Union data protection law provides for data protection principles, such as the data minimisation and purpose limitation principle and obligations, such as data protection by design and by default.

---

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).

8 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, p. 37).

(10) To support the competitiveness of Union businesses, both online and offline service providers should be able to rely on digital identity solutions recognised across the Union, irrespective of the Member State in which those solutions are provided, thus benefiting from a harmonised Union approach to trust, security and interoperability. Both users and service providers should be able to benefit from the same legal value provided to electronic attestations of attributes across the Union. A harmonised digital identity framework is intended to create economic value by providing easier access to goods and services and by significantly reducing operational costs linked to electronic identification and authentication procedures, for instance during the onboarding of new customers, by reducing the potential for cybercrime, such as identity theft, data theft and online fraud, thus promoting efficiency gains and the secure digital transformation of the Union's micro, small and medium-sized enterprises (SMEs).

(11) European Digital Identity Wallets should facilitate the application of the 'once only' principle, thus reducing the administrative burden on and supporting cross-border mobility of Union citizens and residents in the Union and businesses across the Union and fostering the development of interoperable e-government services across the Union.

(12) Regulation (EU) 2016/679, Regulation (EU) 2018/1725 of the European Parliament and of the Council[9] and Directive 2002/58/EC apply to the processing of personal data in the implementation of this Regulation. Therefore, this Regulation should lay down specific safeguards to prevent providers of electronic identification means and electronic attestation of attributes from combining personal data obtained when providing other services with the personal data processed to provide the services falling within the scope of this Regulation. Personal data related to the provision of European Digital Identity Wallets should be kept logically separate from any other data held by the provider of the European Digital Identity Wallet. This Regulation should not prevent providers of European Digital Identity Wallets from applying additional technical measures that contribute to the protection of personal data, such as physical separation of personal data related to the provision of European Digital Identity Wallets from any other data held by the provider. Without prejudice to Regulation (EU) 2016/679, this Regulation further specifies the application of principles of purpose limitation, data minimisation, and data protection by design and by default.

[9] 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).

(13) European Digital Identity Wallets should have the function of a common dashboard embedded into the design, in order to ensure a higher degree of transparency, privacy and control of the users over their personal data. That function should provide an easy, user-friendly interface with an overview of all relying parties with whom the user shares data, including attributes, and the type of data shared with each relying party. It should allow users to track all transactions executed through the European Digital Identity Wallet with at least the following data: the time and date of the transaction, the counterpart identification, the personal data requested and the data shared. That information should be stored even if the transaction was not concluded. It should not be possible to repudiate the authenticity of the information contained in the transaction history. Such a function should be active by default. It should allow users easily to request the immediate erasure by a relying party of personal data pursuant Article 17 of Regulation (EU) 2016/679 and easily to report the relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for personal data is received, directly via the European Digital Identity Wallet.

(14) Member States should integrate different privacy-preserving technologies, such as zero knowledge proof, into the European Digital Identity Wallet. Those cryptographic methods should allow a relying party to validate whether a given statement based on the person’s identification data and attestation of attributes is true, without revealing any data on which that statement is based, thereby preserving the privacy of the user.

(15) This Regulation sets out the harmonised conditions for the establishment of a framework for European Digital Identity Wallets to be provided by Member States. All Union citizens, and residents in the Union as defined by national law, should be empowered to securely request, select, combine, store, delete, share and present data related to their identity and request the erasure of their personal data in a user friendly and convenient way, under the sole control of the user, while enabling selective disclosure of personal data. This Regulation reflects shared European values and respects fundamental rights, legal safeguards and liability, thus protecting democratic societies, Union citizens and residents in the Union. Technologies used to achieve those objectives should be developed aiming towards the highest level of security, privacy, user convenience, accessibility, wide usability and seamless interoperability. Member States should ensure equal access to electronic identification to all their citizens and residents. Member States should not, directly or indirectly, limit access to public or private services to natural or legal persons not opting to use European Digital Identity Wallets and should make available appropriate alternative solutions.

(16) Member States should rely on the possibilities offered by this Regulation to provide, under their responsibility, European Digital Identity Wallets for use by the natural and legal persons residing on their territory. To offer Member States flexibility and leverage the state-of-the-art technology, this Regulation should enable provision of European Digital Identity Wallets directly by a Member State, under a mandate from a Member State, or independently of a Member State, but recognised by that Member State.

(17) For the purposes of registration, relying parties should provide the information necessary to allow for their electronic identification and authentication towards European Digital Identity Wallets. When declaring their intended use of the European Digital Identity Wallet, relying parties should provide information regarding the data that they will request, if any, in order to provide their services and the reason for the request. Relying party registration facilitates the verification by Member States with regard to the lawfulness of the activities of the relying parties in accordance with Union law. The obligation to register provided for in this Regulation should be without prejudice to obligations laid down in other Union or national law, such as the information to be provided to the data subjects pursuant to the Regulation (EU) 2016/679. Relying parties should comply with the safeguards offered by Articles 35 and 36 of that Regulation, in particular by performing data protection impact assessments and by consulting the competent data protection authorities prior to data processing where data protection impact assessments indicate that the processing would result in a high risk. Such safeguards should support the lawful processing of personal data by relying parties, in particular with regard to special categories of data, such as health data. The registration of relying parties is intended to enhance transparency and trust in the use of European Digital Identity Wallets. Registration should be cost-effective and proportionate to the related risks in order to ensure uptake by service providers. In that context, registration should provide for the use of automated procedures, including the reliance on and the use of existing registers by Member States, and should not entail a pre-authorisation process. The registration process should enable a variety of use-cases that can differ in terms of mode of operation, whether online or in offline mode, or in terms of the requirement to authenticate devices for the purposes of interfacing with the European Digital Identity Wallet. Registration should apply exclusively to relying parties providing services by means of digital interaction.

(18) Safeguarding Union citizens and residents in the Union against the unauthorised or fraudulent use of European Digital Identity Wallets is of high importance for ensuring trust in and for the wide uptake of European Digital Identity Wallets. Users should be provided with effective protection against such misuse. In particular, when facts that form the basis for fraudulent or otherwise illegal use of a European Digital Identity Wallet are established by a national judicial authority in the context of another procedure, supervisory bodies that are responsible for European Digital Identity Wallet issuers should, upon notification, take the necessary measures to ensure that the registration of the relying party and the inclusion of relying parties in the authentication mechanism are withdrawn or suspended until the notifying authority confirms that the irregularities identified have been remedied.

(19) All European Digital Identity Wallets should enable users to electronically identify themselves and authenticate online and in offline mode across borders to access a wide range of public and private services. Without prejudice to Member States' prerogatives as regards the identification of their citizens and residents, European Digital Identity Wallets can also serve the institutional needs of public administrations, international organisations and the Union's institutions, bodies, offices and agencies. Authentication in offline mode would be important in many sectors, including in the health sector where services are often provided through face-to-face interaction and ePrescriptions should be able to rely on QR-codes or similar technologies to verify authenticity. Relying on the assurance level high with regard to electronic identification schemes European Digital Identity Wallets should benefit from the potential offered by tamper-proof solutions such as secure elements, to comply with the security requirements under this Regulation. European Digital Identity Wallets should also allow users to create and use qualified electronic signatures and seals which are accepted across the Union. Once on-boarded to a European Digital Identity Wallet, natural persons should be able to use it to sign with qualified electronic signatures, by default and free of charge, without having to go through any additional administrative procedures. Users should be able to sign or seal self-claimed assertions or attributes.To achieve simplification and cost-reduction benefits for persons and businesses across the Union, including by enabling powers of representation and e-mandates, Member States should provide European Digital Identity Wallets that rely on common standards and technical specifications to ensure seamless interoperability and to adequately increase IT security, strengthen robustness against cyber-attacks and thus significantly reduce the potential risks of ongoing digitalisation for Union citizens, residents in the Union and undertakings.

Only Member States' competent authorities can provide a high level of confidence in establishing the identity of a person and therefore provide assurance that the person claiming or asserting a particular identity is in fact the person he or she claims to be. It is therefore necessary for the provision of European Digital Identity Wallets to rely on the legal identity of Union citizens, residents in the Union or legal persons. Reliance on the legal identity should not hinder European Digital Identity Wallet users to access services under a pseudonym, where there is no legal requirement for legal identity for authentication. Trust in European Digital Identity Wallets would be enhanced if issuing and managing parties are required to implement appropriate technical and organisational measures to ensure the highest level of security that is commensurate to the risks raised for the rights and freedoms of the natural persons, in accordance with Regulation (EU) 2016/679.

(20) The use of a qualified electronic signature should be free of charge to all natural persons for non-professional purposes. It should be possible for Member States to provide for measures to prevent the use of qualified electronic signatures for professional purposes by natural persons free-of-charge, while ensuring that any such measures are proportionate to identified risks and are justified.

(21) It is beneficial to facilitate the uptake and use of European Digital Identity Wallets by seamlessly integrating them with the ecosystem of public and private digital services already implemented at national, local or regional level. To achieve that goal, it should be possible for Member States to provide for legal and organisational measures in order to increase flexibility for providers of European Digital Identity Wallets and to allow for additional functionalities of European Digital Identity Wallets to those provided for in this Regulation, including by enhanced interoperability with existing national electronic identification means. Such additional functionalities should by no means be to the detriment of providing core functions of European Digital Identity Wallets provided for in this Regulation or promote existing national solutions over European Digital Identity Wallets. Since they go beyond this Regulation, such additional functionalities do not benefit from the provisions on cross-border reliance on European Digital Identity Wallets set out in this Regulation.

(22) European Digital Identity Wallets should include a functionality to generate user chosen and managed pseudonyms, to authenticate when accessing online services.

(23) In order to achieve a high level of security and trustworthiness, this Regulation establishes the requirements for European Digital Identity Wallets. The conformity of European Digital Identity Wallets with those requirements should be certified by accredited conformity assessment bodies designated by Member States.

(24) In order to avoid divergent approaches and harmonise the implementation of the requirements laid down by this Regulation, the Commission should, for the purpose of certifying European Digital Identity Wallets, adopt implementing acts to establish a list of reference standards and, where necessary, to establish specifications and procedures for the purpose of expressing detailed technical specifications of those requirements. To the extent that the certification of the conformity of European Digital Identity Wallets with relevant cybersecurity requirements is not covered by existing cybersecurity certification schemes that are referred to in this Regulation, and as regards non-cybersecurity requirements relevant to European Digital Identity Wallets, Member States should establish national certification schemes pursuant to the harmonised requirements set out in and adopted pursuant to this Regulation. Member States should transmit their draft national certification schemes to the European Digital Identity Cooperation Group, which should be able to issue opinions and recommendations.

(25) Certification of conformity with the cybersecurity requirements established in this Regulation should, where available, rely on the relevant European cybersecurity certifications schemes established pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council[10], which establishes a voluntary European cybersecurity certification framework for ICT products, processes and services.

---

[10] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

(26) In order to continuously assess and mitigate risks linked to security, certified European Digital Identity Wallets should be subject to regular vulnerability assessments aiming to detect any vulnerability in the certified product-related components, certified process-related components and certified service-related components of the European Digital Identity Wallet.

(27) By protecting users and companies from cybersecurity risks, the essential cybersecurity requirements laid down in this Regulation also contribute to enhancing the protection of personal data and privacy of individuals. Synergies on both standardisation and certification on cybersecurity aspects should be considered through the cooperation between the Commission, the European Standardisation Organizations, the European Union Agency for Cybersecurity (ENISA), the European Data Protection Board established by Regulation (EU) 2016/679 and the national data protection supervisory authorities.

(28) The onboarding of Union citizens and residents in the Union to the European Digital Identity Wallet should be facilitated by relying on electronic identification means issued at assurance level high. Electronic identification means issued at assurance level substantial should be relied upon only where harmonised technical specifications and procedures using electronic identification means issued at assurance level substantial in combination with supplementary means of identity verification will allow the fulfilment of the requirements set out in this Regulation as regards assurance level high. Such supplementary means should be reliable and easy to use and could be built on the possibility to use remote onboarding procedures, qualified certificates supported by qualified electronic signatures, qualified electronic attestation of attributes or a combination thereof. To ensure sufficient uptake of European Digital Identity Wallets, harmonised technical specifications and procedures for the onboarding of users by using electronic identification means, including those issued at assurance level substantial, should be set out in implementing acts.

(29) The objective of this Regulation is to provide the user with a fully mobile, secure and user-friendly European Digital Identity Wallet. As a transitional measure until the availability of certified tamper-proof solutions, such as secure elements within the users' devices, European Digital Identity Wallets should be able to rely upon certified external secure elements for the protection of the cryptographic material and other sensitive data or upon notified electronic identification means at assurance level high in order to demonstrate compliance with the relevant requirements of this Regulation as regards the assurance level of the European Digital Identity Wallet. This Regulation should be without prejudice to national conditions with regard to the issuance and use of a certified external secure element where the transitional measure is dependent on it.

(30) European Digital Identity Wallets should ensure the highest level of data protection and security for the purposes of electronic identification and authentication to facilitate access to public and private services, irrespective of whether such data is stored locally or on cloud-based solutions, taking due account of the different levels of risk.

(31) European Digital Identity Wallets should be secure-by-design and should implement advanced security features to protect against identity and other data theft, denial of service and any other cyber threat. Such security should include state-of-the-art encryption and storage methods that are accessible only to, and decryptable only by, the user and that rely on end-to-end encrypted communication with other European Digital Identity Wallets and relying parties. Additionally, European Digital Identity Wallets should require secure, explicit and active user confirmation for the operations performed via European Digital Identity Wallets.

(32) The use, free of charge, of European Digital Identity Wallets should not result in the processing of data beyond data that is necessary for the provision of European Digital Identity Wallet services. This Regulation should not allow the processing of personal data stored in or resulting from the use of the European Digital Identity Wallet by the provider of the European Digital Identity Wallet for purposes other than the provision of European Digital Identity Wallet services. To ensure privacy, European Digital Identity Wallet providers should ensure unobservability by not collecting data and not having insight into the transactions of the users of the European Digital Identity Wallet. Such unobservability means that the providers are not able to see the details of the transactions made by the user. However, in specific cases, on the basis of explicit prior consent by the user in each of those specific cases, and fully in accordance with Regulation (EU) 2016/679, providers of European Digital Identity Wallets could be granted access to the information necessary for the provision of a particular service related to European Digital Identity Wallets.

(33) The transparency of European Digital Identity Wallets and the accountability of their providers are key elements to creating social trust and trigger acceptance of the framework. The functioning of European Digital Identity Wallets should therefore be transparent and, in particular, allow for verifiable processing of personal data. To achieve this, Member States should disclose the source code of the user application software components of European Digital Identity Wallets, including those that are related to processing of personal data and data of legal persons. The publication of this source code under an open-source licence should enable society, including users and developers, to understand its operation, audit and review the code. This would increase users' trust in the ecosystem and contribute to the security of European Digital Identity Wallets by enabling anyone to report vulnerabilities and errors in the code. Overall, this should provide suppliers with an incentive to deliver and maintain a highly secure product. However, in certain cases, the disclosure of the source code for the libraries used, communication channel or other elements that are not hosted on the user device, could be limited by Member States, for duly justified reasons, especially for the purpose of public security.

(34) The use of European Digital Identity Wallets as well as the discontinuation of their use should be the exclusive right and choice of users. Member States should develop simple and secure procedures for the users to request immediate revocation of validity of European Digital Identity Wallets, including in the case of loss or theft. Upon the death of the user or the cessation of activity by a legal person, a mechanism should be established to enable the authority responsible for settling the succession of the natural person or assets of the legal person to request the immediate revocation of European Digital Identity Wallets.

(35) In order to promote the uptake of European Digital Identity Wallets and the wider use of digital identities, Member States should not only promote the benefits of the relevant services, but should also, in cooperation with the private sector, researchers and academia, develop training programmes aiming to strengthen the digital skills of their citizens and residents, in particular for vulnerable groups such as persons with disabilities and older persons. Member States should also raise awareness of the benefits and risks of European Digital Identity Wallets by means of communication campaigns.

(36) To ensure that the European Digital Identity Framework is open to innovation, technological development and future-proof, Member States are encouraged, jointly, to set up sandboxes to test innovative solutions in a controlled and secure environment in particular to improve the functionality, protection of personal data, security and interoperability of the solutions and to inform future updates of technical references and legal requirements. That environment should foster the inclusion of SMEs, start-ups and individual innovators and researchers, as well as relevant industry stakeholders. Such initiatives should contribute to and strengthen the regulatory compliance and technical robustness of European Digital Identity Wallets to be provided to Union citizens and residents in the Union, thus preventing the development of solutions that do not comply with Union law on data protection or that are open to security vulnerabilities.

(37) Regulation (EU) 2019/1157 of the European Parliament and of the Council[11] strengthens the security of identity cards with enhanced security features by August 2021. Member States should consider the feasibility of notifying them under electronic identification schemes to extend the cross-border availability of electronic identification means.

(38) The process of notification of electronic identification schemes should be simplified and accelerated to promote access to convenient, trusted, secure and innovative authentication and identification solutions and, where relevant, to encourage private identity providers to offer electronic identification schemes to Member State's authorities for notification as national electronic identification schemes under Regulation (EU) No 910/2014.

(39) Streamlining of the current notification and peer-review procedures will prevent heterogeneous approaches to the assessment of various notified electronic identification schemes and facilitate trust-building between Member States. New, simplified, mechanisms are intended to foster Member States' cooperation on the security and interoperability of their notified electronic identification schemes.

(40) Member States should benefit from new, flexible tools to ensure compliance with the requirements of this Regulation and of the relevant implementing acts adopted pursuant thereto. This Regulation should allow Member States to use reports and assessments, performed by accredited conformity assessment bodies, as provided for in the context of certification schemes to be established at Union level under Regulation (EU) 2019/881, to support their claims on the alignment of the schemes or of parts thereof with Regulation (EU) No 910/2014.

---

[11] Regulation (EU) 2019/1157 of the European Parliament and of the Council of 20 June 2019 on strengthening the security of identity cards of Union citizens and of residence documents issued to Union citizens and their family members exercising their right of free movement (OJ L 188, 12.7.2019, p. 67).

(41) Public service providers use the person identification data available from electronic identification means pursuant to Regulation (EU) No 910/2014 to match the electronic identity of the users from other Member States with the person identification data provided to those users in the Member State performing the cross-border identity matching process. However, in many cases, despite the use of the minimum data set provided under the notified electronic identification schemes, ensuring accurate identity matching when Member States act as relying parties requires additional information about the user and specific complementary unique identification procedures to be performed at national level. To further support the usability of electronic identification means, provide better online public services and increase legal certainty in relation to the electronic identity of the users, Regulation (EU) No 910/2014 should require Member States to take specific online measures to ensure unequivocal identity matching when users intend to access online cross-border public services.

(42) When developing European Digital Identity Wallets, it is essential to take into consideration the needs of users. Meaningful use cases and online services relying on European Digital Identity Wallets should be available. For the convenience of users and in order to ensure cross-border availability of such services, it is important to undertake actions in order to facilitate a similar approach to design, development and implementation of online services in all Member States. Non-binding guidelines on how to design, develop and implement online services relying on European Digital Identity Wallets have the potential of becoming a useful tool to achieve that goal. Such guidelines should be prepared taking into account the interoperability framework of the Union. Member States should have a leading role when it comes to adopting those guidelines.

(43) In accordance with Directive (EU) 2019/882 of the European Parliament and of the Council[12], persons with disabilities should be able to use European Digital Identity Wallets, trust services and end-user products used in the provision of those services on an equal basis with other users.

(44) In order to ensure effective enforcement of this Regulation, a minimum for the maximum of administrative fines for both qualified and non-qualified trust service providers should be established. Member States should provide for effective, proportionate and dissuasive penalties. When determining the penalties, the size of the affected entities, their business models and the severity of the infringements should be duly taken into consideration.

(45) Member States should lay down rules on penalties for infringements such as direct or indirect practices leading to confusion between non-qualified and qualified trust services or to the abusive use of the EU trust mark by non-qualified trust service providers. The EU trust mark should not be used under conditions which, directly or indirectly, lead to the perception that any non-qualified trust services offered by those providers are qualified.

(46) This Regulation should not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form laid down by Union or national law. In addition, it should not affect national form requirements pertaining to public registers, in particular commercial and land registers.

---

[12] Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

(47) The provision and use of trust services and the benefits brought in terms of convenience and legal certainty in the context of cross-border transactions, in particular when qualified trust services are used, are becoming increasingly important for international trade and cooperation. International partners of the Union are establishing trust frameworks inspired by Regulation (EU) No 910/2014. In order to facilitate the recognition of qualified trust services and of their providers, the Commission may adopt implementing acts to set the conditions under which trust frameworks of third countries could be considered equivalent to the trust framework for qualified trust services and providers thereof in this Regulation. Such an approach should complement the possibility for the mutual recognition of trust services and providers thereof established in the Union and in third countries in accordance with Article 218 of the Treaty on the Functioning of the European Union (TFEU). When setting out the conditions under which the trust frameworks of third countries could be considered to be equivalent to the trust framework for qualified trust services and providers thereof under Regulation (EU) No 910/2014, compliance with the relevant provisions in the Directive (EU) 2022/2555 of the European Parliament and of the Council[13] and Regulation (EU) 2016/679 should be ensured, as well as the use of trusted lists as essential elements to build trust.

[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 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

(48) This Regulation should foster choice and the possibility of switching between European Digital Identity Wallets where a Member State has endorsed more than one European Digital Identity Wallet solution on its territory. In order to avoid lock-in effects in such situations, where technically feasible, the providers of European Digital Identity Wallets should ensure the effective portability of data at the request of European Digital Identity Wallet users, and should not be allowed to use contractual, economic or technical barriers to prevent or to discourage effective switching between different European Digital Identity Wallets.

(49) To ensure the proper functioning of European Digital Identity Wallets, European Digital Identity Wallet providers need effective interoperability and fair, reasonable and non-discriminatory conditions for the European Digital Identity Wallets to access specific hardware and software features of mobile devices. Those components could include, in particular, near field communication antennas and secure elements, including universal integrated circuit cards, embedded secure elements, microSD cards and Bluetooth Low Energy. Access to those components could be under the control of mobile network operators and equipment manufacturers. Therefore, where needed to provide the services of European Digital Identity Wallets, original equipment manufacturers of mobile devices or providers of electronic communication services should not refuse access to such components. In addition, the undertakings that are designated as gatekeepers for core platform services as listed by the Commission pursuant to Regulation (EU) 2022/1925 of the European Parliament and of the Council[14] should remain subject to the specific provisions of that Regulation, building on Article 6(7) thereof.

---

[14] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1).

(50) In order to streamline the cybersecurity obligations imposed on trust service providers, as well as to enable those providers and their respective competent authorities to benefit from the legal framework established by Directive (EU) 2022/2555, trust services are required to take appropriate technical and organisational measures pursuant to that Directive, such as measures addressing system failures, human error, malicious actions or natural phenomena in order to manage the risks posed to the security of network and information systems which those providers use in the provision of their services as well as to notify significant incidents and cyber threats in accordance with that Directive. With regard to the reporting of incidents, trust service providers should notify any incidents having a significant impact on the provision of their services, including such caused by theft or loss of devices, network cable damage or incidents that occur in the context of the identification of persons. The cybersecurity risk management requirements and reporting obligations under Directive (EU) 2022/2555 should be considered to be complementary to the requirements imposed on trust service providers under this Regulation. Where appropriate, established national practices or guidance in relation to the implementation of security and reporting requirements and supervision of compliance with such requirements under Regulation (EU) No 910/2014 should continue to be applied by the competent authorities designated under Directive (EU) 2022/2555. This Regulation does not affect the obligation to notify personal data breaches pursuant to Regulation (EU) 2016/679.

(51) Due consideration should be given to ensure effective cooperation between the supervisory bodies designated pursuant to 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. Where such a supervisory body is different from such a competent authority, they should cooperate closely, in a timely manner by exchanging the relevant information in order to ensure effective supervision and compliance of trust service providers with the requirements set out in Regulation (EU) No 910/2014 and in Directive (EU) 2022/2555. In particular, supervisory bodies designated pursuant to Regulation (EU) No 910/2014 should be entitled to request competent authorities designated or established pursuant Directive (EU) 2022/2555 to provide relevant information needed to grant the qualified status and to carry out supervisory actions to verify compliance of the trust service providers with the relevant requirements under Directive (EU) 2022/2555 or to require them to remedy non-compliance.

(52) It is essential to provide for a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services. That framework could also open new market opportunities for Union trust service providers to offer new Union-wide electronic registered delivery services. In order to ensure that data using a qualified electronic registered delivery service is delivered to the correct addressee, qualified electronic registered delivery services should ensure complete certainty the identification of the addressee while a high level of confidence would suffice as regards the identification of the sender. Providers of qualified electronic registered delivery services should be encouraged by Member States to make their services interoperable with qualified electronic registered delivery services provided by other qualified trust service providers in order to easily transfer electronic registered data between two or more qualified trust service providers and to promote fair practices in the internal market.

(53) In most cases, Union citizens and residents in the Union are unable to exchange digital information relating to their identity, such as their address, age, professional qualifications, driving licence and other permits and payment data, across borders, securely and with a high level of data protection.

(54) It should be possible to issue and handle trustworthy electronic attributes and contribute to reducing administrative burden, empowering Union citizens and residents in the Union to use them in their private and public transactions. Union citizens and residents in the Union should be able, for instance, to demonstrate ownership of a valid driving licence issued by an authority in one Member State, which can be verified and relied upon by the relevant authorities in other Member States, to rely on their social security credentials or on future digital travel documents in a cross border context.

(55) Any service provider that issues attested attributes in electronic form such as diplomas, licences, birth certificates or powers and mandates to represent or act on behalf of natural or legal persons should be considered to be a trust service provider of electronic attestation of attributes. An electronic attestation of attributes should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic attestation of attributes. General requirements should be laid down to ensure that a qualified electronic attestation of attributes has the equivalent legal effect of lawfully issued attestations in paper form. However, those requirements should apply without prejudice to Union or national law defining additional sector-specific requirements as regards form with underlying legal effects and, in particular, the cross-border recognition of qualified electronic attestation of attributes, where appropriate.

(56) The wide availability and usability of European Digital Identity Wallets should enhance their acceptance and trust in them both by private individuals and by private service providers. Therefore, private relying parties providing services, for example in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, telecommunications or education, should accept the use of European Digital Identity Wallets for the provision of services where strong user authentication for online identification is required by Union or national law or by contractual obligation. Any request by the relying party for information from the user of a European Digital Identity Wallet should be necessary for, and proportionate to, the intended use in a given case, should be in line with the principle of data minimisation and should ensure transparency as regards which data is shared and for what purposes. To facilitate the use and acceptance of European Digital Identity Wallets, widely accepted industry standards and specifications should be taken into account in their deployment.

(57) Where very large online platforms within the meaning of Article 33(1) of Regulation (EU) 2022/2065 of the European Parliament and of the Council[15] require users to be authenticated in order to access online services, those platforms should be required to accept the use of European Digital Identity Wallets upon the voluntary request of the user. Users should be under no obligation to use a European Digital Identity Wallet to access private services and should not be restricted or hindered in their access to services on the grounds that they do not use a European Digital Identity Wallet. However, if users wish to do so, very large online platforms should accept them for that purpose, while respecting the principle of data minimisation and the right of the users to use freely chosen pseudonyms. Given the importance of very large online platforms, due to their reach, in particular as expressed in number of recipients of the service and economic transactions, the obligation to accept European Digital Identity Wallets is necessary to increase the protection of users from fraud and to secure a high level of data protection.

(58) Codes of conduct at Union level should be developed in order to contribute to the widespread availability and usability of electronic identification means, including European Digital Identity Wallets within the scope of this Regulation. The codes of conduct should facilitate broad acceptance of electronic identification means including European Digital Identity Wallets by those service providers which do not qualify as very large platforms and which rely on third party electronic identification services for user authentication.

---

[15] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).

(59) Selective disclosure is a concept empowering the owner of data to disclose only certain parts of a larger data set, in order for the receiving entity to obtain only such information as is necessary for the provision of a service requested by a user. The European Digital Identity Wallet should technically enable the selective disclosure of attributes to relying parties. It should be technically possible for the user to selectively disclose attributes, including from multiple, distinct electronic attestations, and to combine and present them seamlessly to relying parties. This feature should become a basic design feature of European Digital Identity Wallets, thereby reinforcing convenience and the protection of personal data, including data minimisation.

(60) Unless specific rules of Union or national law require users to identify themselves, accessing services by using a pseudonym should not be prohibited.

(61) Attributes provided by the qualified trust service providers as part of the qualified attestation of attributes should be verified against authentic sources either directly by the qualified trust service provider or by means of designated intermediaries recognised at national level in accordance with Union or national law for the purpose of secure exchange of attested attributes between identity or attestation of attributes' service providers and relying parties. Member States should establish appropriate mechanisms at national level to ensure that qualified trust service providers issuing qualified electronic attestation of attributes are able, on the basis of the consent of the person to whom the attestation is issued, to verify the authenticity of the attributes relying on authentic sources. It should be possible for appropriate mechanisms to include the use of specific intermediaries or technical solutions in accordance with national law allowing access to authentic sources. Ensuring the availability of a mechanism that allows the verification of attributes against authentic sources is intended to facilitate the compliance of the qualified trust service providers of qualified electronic attestation of attributes with their obligations under Regulation (EU) No 910/2014. A new annex to that Regulation should contain a list of categories of attributes with regard to which Member States are to ensure that measures are taken to allow qualified providers of electronic attestations of attributes to verify by electronic means, at the request of the user, their authenticity against the relevant authentic source.

(62) Secure electronic identification and the provision of attestation of attributes should offer additional flexibility and solutions for the financial services sector to allow the identification of customers and the exchange of specific attributes necessary to comply with, for example, customer due diligence requirements under a future Regulation establishing the Anti Money Laundering Authority, with suitability requirements stemming from investor protection law, or to support the fulfilment of strong customer authentication requirements for online identification for the purposes of account login and of initiation of transactions in the field of payment services.

(63) The legal effect of an electronic signature is not to be challenged on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature. However, it is for national law to establish the legal effect of electronic signatures, except for the requirements provided for in this Regulation according to which the legal effect of a qualified electronic signature is to be considered to be equivalent to that of a handwritten signature. In determining the legal effects of electronic signatures, Member States should take into account the principle of proportionality between the legal value of a document to be signed and the level of security and cost that an electronic signature requires. To increase the accessibility and use of electronic signatures, Member States are encouraged to consider the use of advanced electronic signatures in the day-to-day transactions for which they provide a sufficient level of security and confidence.

(64) In order to ensure the consistency of certification practices across the Union, the Commission should issue guidelines on the certification and recertification of qualified electronic signature creation devices and of qualified electronic seal creation devices, including their validity and limitations in time. This Regulation does not prevent the public or private bodies that have certified qualified electronic signature creation devices from temporarily re-certifying such devices for a short certification period on the basis of the results of the previous certification process, where such re-certification cannot be performed within the legally set time frame for a reason other than a breach or security incident, without prejudice to the obligation to conduct a vulnerability assessment and without prejudice to the applicable certification practice.

(65) The issuance of certificates for website authentication is intended to provide users with assurance with a high level of confidence in the identity of the entity standing behind the website, irrespective of the platform used to display that identity. Those certificates should contribute to the building of trust in conducting business online, as users would have confidence in a website that has been authenticated. The use of such certificates by websites should be voluntary. In order for website authentication to become a means by which to increase trust, to provide a better experience for the user and to foster growth in the internal market, this Regulation lays down a trust framework including minimal security and liability obligations for the providers of qualified certificates for website authentication and requirements for the issuance of those certificates. National trusted lists should confirm the qualified status of website authentication services and of their trust service providers, including their full compliance with the requirements of this Regulation with regard to the issuance of qualified certificates for website authentication. The recognition of qualified certificates for website authentication means that the providers of web-browsers should not deny the authenticity of qualified certificates for website authentication for the sole purpose of attesting the link between the website domain name and the natural or legal person to whom the certificate is issued or confirming the identity of that person. Providers of web-browsers should display the certified identity data and the other attested attributes to the end-user in a user-friendly manner in the browser environment, by technical means of their choice. To that end, providers of web-browsers should ensure support and interoperability with qualified certificates for website authentication issued in full compliance with this Regulation.

The obligation of recognition and interoperability of and support for qualified certificates for website authentication does not affect the freedom of providers of web-browsers to ensure web security, domain authentication and the encryption of web traffic in a manner and by means of technology that they consider to be the most appropriate. In order to contribute to the online security of end-users, providers of web-browsers should, in exceptional circumstances, be able to take precautionary measures that are both necessary and proportionate in reaction to substantiated concerns regarding security breaches or the loss of integrity of an identified certificate or set of certificates. Where they take such precautionary measures, providers of web-browsers should notify, without undue delay, the Commission, the national supervisory body, the entity to which the certificate was issued and the qualified trust service provider that issued that certificate or set of certificates, of any concern with regard to such a security breach or loss of integrity as well as the measures taken relating to the single certificate or set of certificates. Those measures should be without prejudice to the obligation of the providers of web-browsers to recognise qualified website authentication certificates in accordance with the national trusted lists. To further protect Union citizens and residents in the Union and promote the use of qualified certificates for website authentication, public authorities in Member States should consider incorporating qualified certificates for website authentication in their websites. The measures provided for by this Regulation that aim to bring increased coherence between Member States' divergent approaches and practices relating to supervisory procedures are intended to contribute to improved trust and confidence in the security, quality and availability of qualified certificates for website authentication.

(66) Many Member States have introduced national requirements for services providing secure and trustworthy electronic archiving in order to allow for the long-term preservation of electronic data and electronic documents, and associated trust services. To ensure legal certainty, trust and harmonisation across Member States, a legal framework for qualified electronic archiving services should be established, inspired by the framework of the other trust services set out in this Regulation. The legal framework for qualified electronic archiving services should offer trust service providers and users an efficient toolbox that includes functional requirements for the electronic archiving service, as well as clear legal effects when a qualified electronic archiving service is used. Those provisions should apply to electronic data and electronic documents created in electronic form as well as paper documents that have been scanned and digitised. When required, those provisions should permit the preserved electronic data and electronic documents to be ported on different media or formats for the purpose of extending their durability and legibility beyond the technological validity period, while preventing loss and alteration to the extent possible. When electronic data and electronic documents submitted to the electronic archiving service contain one or more qualified electronic signatures or qualified electronic seals, the service should use procedures and technologies capable of extending their trustworthiness for the preservation period of such data, possibly relying on the use of other qualified trust services established by this Regulation. In order to create preservation evidence where electronic signatures, electronic seals or electronic timestamps are used, qualified trust services should be used. To the extent that electronic archiving services are not harmonised by this Regulation, it should be possible for Member States to maintain or introduce national provisions, in accordance with Union law, relating to those services, such as specific provisions for services integrated in an organisation and only used for the internal archives of that organisation. This Regulation should not distinguish between electronic data and electronic documents created in electronic form and physical documents that have been digitised.

(67) The activities of national archives and memory institutions, in their capacity as organisations dedicated to preserving the documentary heritage in the public interest, are usually regulated in national law and they do not necessarily provide trust services within the meaning of this Regulation. In so far such institutions do not provide such trust services, this Regulation is without prejudice to their operation.

(68) Electronic ledgers are a sequence of electronic data records which should ensure their integrity and the accuracy of their chronological ordering. Electronic ledgers should establish a chronological sequence of data records. In conjunction with other technologies, they should contribute to solutions for more efficient and transformative public services such as e-voting, cross-border cooperation of customs authorities, cross-border cooperation of academic institutions and the recording of ownership for real estate in decentralised land registries. Qualified electronic ledgers should establish a legal presumption for the unique and accurate sequential chronological ordering and integrity of the data records in the ledger. Due to their specificities, such as the sequential chronological ordering of data records, electronic ledgers should be distinguished from other trust services such as electronic time stamps and electronic registered delivery services. To ensure legal certainty and promote innovation, a Union-wide legal framework that provides for the cross-border recognition of trust services for the recording of data in electronic ledgers should be established. This should sufficiently prevent the same digital asset from being copied and sold more than once to different parties. The process of creating and updating an electronic ledger depends on the type of ledger used, namely whether it is centralised or distributed. This Regulation should ensure technological neutrality, namely neither favouring, nor discriminating against, any technology used to implement the new trust service for electronic ledgers. In addition, sustainability indicators with regard to any adverse impacts on the climate or other environment- related adverse impacts should be taken into account by the Commission, using adequate methodologies, when preparing the implementing acts specifying the requirements for qualified electronic ledgers.

(69) The role of trust service providers for electronic ledgers should be to ascertain the sequential recording of data into the ledger. This Regulation is without prejudice to any legal obligations of users of electronic ledgers under Union or national law. For instance, use cases that involve the processing of personal data should comply with Regulation (EU) 2016/679 and use cases that relate to financial services should comply with the relevant Union financial services law.

(70) In order to avoid the fragmentation of and barriers in the internal market, due to diverging standards and technical restrictions, and to ensure a coordinated process to avoid affecting the implementation of the European Digital Identity Framework, a process for close and structured cooperation between the Commission, Member States, civil society, academia and the private sector is needed. To achieve that objective, Member States and the Commission should cooperate within the framework set out in the Commission Recommendation (EU) 2021/946[16] to identify a common Union toolbox for the European Digital Identity Framework. In that context, Member States should agree on a comprehensive technical architecture and reference framework, a set of common standards and technical references including recognised existing standards and a set of guidelines and descriptions of best practices covering at least all functionalities and interoperability of European Digital Identity Wallets, including eSignatures and of the qualified trust service providers for electronic attestation of attributes as laid out in this Regulation. In that context, Member States should also agree on common elements with regard to a business model and fee structure for European Digital Identity Wallets, in order to facilitate take up, in particular by SMEs, in a cross-border context. The content of the toolbox should evolve in parallel with and reflect the outcome of the discussion and the process of adoption of the European Digital Identity Framework.

---

16 Commission Recommendation (EU) 2021/946 of 3 June 2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework (OJ L 210, 14.6.2021, p. 51).

(71) This Regulation provides for a harmonised level of quality, trustworthiness and security of qualified trust services, regardless of where the operations are conducted. Thus, a qualified trust service provider should be allowed to outsource its operations related to the provision of a qualified trust service in a third country, where that third country provides adequate guarantees, ensuring that supervisory activities and audits can be enforced as if they were carried out in the Union. When the compliance with this Regulation cannot be fully assured, the supervisory bodies should be able to adopt proportionate and justified measures including the withdrawal of the qualified status of the trust service provided.

(72) To ensure legal certainty as regards the validity of advanced electronic signatures based on qualified certificates, it is essential that the assessment by the relying party carrying out the validation of that advanced electronic signature based on qualified certificates be specified.

(73) Trust service providers should use cryptographic methods reflecting current best practices and trustworthy implementations of those algorithms in order to ensure security and reliability of their trust services.

(74) This Regulation lays down an obligation for qualified trust service providers to verify the identity of a natural or legal person to whom the qualified certificate or the qualified electronic attestation of attribute is issued based on various harmonised methods across the Union. To ensure that qualified certificates and qualified electronic attestations of attributes are issued to the person to whom they belong and that they attest the correct and unique set of data representing the identity of that person, qualified trust service providers issuing qualified certificates or issuing qualified electronic attestations of attributes should, at the moment of the issuance of those certificates and attestations, ensure with complete certainty the identification of that person. Moreover, in addition to the mandatory verification of the identity of the person, if applicable for the issuance of qualified certificates and when issuing a qualified electronic attestation of attributes, qualified trust service providers should ensure with complete certainty the correctness and accuracy of the attested attributes of the person to whom the qualified certificate or the qualified electronic attestation of attributes is issued. Those obligations of result and complete certainty in verifying the attested data should be supported by appropriate means, including by using one or, where required, a combination of specific methods provided for in this Regulation. It should be possible to combine those methods to provide an appropriate basis for the verification of the identity of the person to whom the qualified certificate or a qualified electronic attestation of attributes is issued. It should be possible for such a combination to include reliance on electronic identification means which meet the requirements of assurance level substantial in combination with other means of identity verification. Such electronic identification would allow the fulfilment of the harmonised requirements set out in this Regulation as regards assurance level high as part of additional harmonised remote procedures, ensuring identification with a high level of confidence. Those methods should include the possibility for the qualified trust service provider issuing a qualified electronic attestation of attributes to verify the attributes to be attested by electronic means at the request of the user, in accordance with Union or national law, including against authentic sources.

(75) To keep this Regulation in line with global developments and to follow the best practices on the internal market, the delegated and implementing acts adopted by the Commission should be reviewed and if necessary updated on a regular basis. The assessment of the necessity of those updates should take into account new technologies, practices, standards or technical specifications.

(76) Since the objectives of this Regulation, namely the development of the Union-wide European Digital Identity Framework and of a trust service framework, cannot be sufficiently achieved by the Member States but can rather, by reason of their scale and effects, 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.

(77) The European Data Protection Supervisor has been consulted pursuant to Article 42 (1) of Regulation (EU) 2018/1725.

(78) Regulation (EU) No 910/2014 should therefore be amended accordingly,

HAVE ADOPTED THIS REGULATION:

Article 1

Amendments to Regulation (EU) No 910/2014

Regulation (EU) No 910/2014 is amended as follows:

(1) Article 1 is replaced by the following:

‘*Article 1*

Subject matter

This Regulation aims to ensure the proper functioning of the internal market and the provision of an adequate level of security of electronic identification means and trust services used across the Union, in order to enable and facilitate the exercise by natural and legal persons of the right to participate in digital society safely and to access online public and private services throughout the Union. For those purposes, this Regulation:

(a) lays down the conditions under which Member States are to recognise natural and legal persons’ electronic identification means falling under a notified electronic identification scheme of another Member State and provide and recognise European Digital Identity Wallets;

(b) lays down rules for trust services, in particular for electronic transactions;

(c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, certificate services for website authentication, electronic archiving, electronic attestation of attributes, electronic signature creation devices, electronic seal creation devices, and electronic ledgers.’;

(2) Article 2 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. This Regulation applies to electronic identification schemes notified by a Member State, to European Digital Identity Wallets provided by a Member State and to trust service providers established in the Union.’;

(b) paragraph 3 is replaced by the following:

‘3. This Regulation does not affect Union or national law related to the conclusion and validity of contracts, other legal or procedural obligations relating to form, or sector-specific requirements relating to form.

4. This Regulation is without prejudice to Regulation (EU) 2016/679 of the European Parliament and of the Council*.

---

* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 4.5.2016, p. 1).’;

(3) Article 3 is amended as follows:

(a) points (1) to (5) are replaced by the following:

‘(1) “electronic identification” means the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing another natural person or a legal person;

(2) “electronic identification” means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service or, where appropriate, for an offline service;

(3) “person identification data” means a set of data that is issued in accordance with Union or national law and that enables the establishment of the identity of a natural or legal person, or of a natural person representing another natural person or a legal person.

(4) “electronic identification scheme” means a system for electronic identification under which electronic identification means are issued to natural or legal persons or natural persons representing other natural persons or legal persons;

(5) “authentication” means an electronic process that enables the confirmation of the electronic identification of a natural or legal person or the confirmation of the origin and integrity of data in electronic form;’;

(b) the following point is inserted:

‘(5a) “user” means a natural or legal person, or a natural person representing another natural person or a legal person, that uses trust services or electronic identification means provided in accordance with this Regulation;’;

(c) point (6) is replaced by the following:

‘(6) “relying party” means a natural or legal person that relies upon electronic identification, European Digital Identity Wallets or other electronic identification means, or upon a trust service;’;

(d) point (16) is replaced by the following:

‘(16) “trust service” means an electronic service normally provided for remuneration which consists of any of the following:

(a) the issuance of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services;

(b) the validation of certificates for electronic signatures, certificates for electronic seals, certificates for website authentication or certificates for the provision of other trust services;

(c) the creation of electronic signatures or electronic seals;

(d) the validation of electronic signatures or electronic seals;

(e) the preservation of electronic signatures, electronic seals, certificates for electronic signatures or certificates for electronic seals;

(f) the management of remote electronic signature creation devices or remote electronic seal creation devices;

(g) the issuance of electronic attestations of attributes;

(h) the validation of electronic attestation of attributes;

(i) the creation of electronic timestamps;

(j) the validation of electronic timestamps;

(k) the provision of electronic registered delivery services;

(l) the validation of data transmitted through electronic registered delivery services and related evidence;

(m) the electronic archiving of electronic data and electronic documents;

(n) the recording of electronic data in an electronic ledger;’;

(e) point (18) is replaced by the following:

‘(18) “conformity assessment body” means a conformity assessment body as defined in Article 2, point 13, of Regulation (EC) No 765/2008, which is accredited in accordance with that Regulation as competent to carry out conformity assessment of a qualified trust service provider and the qualified trust services it provides, or as competent to carry out certification of European Digital Identity Wallets or electronic identification means;’;

(f) point (21) is replaced by the following:

‘(21) “product” means hardware or software, or relevant components of hardware or software, which are intended to be used for the provision of electronic identification and trust services;’;

(g) the following points are inserted:

‘(23a) “remote qualified electronic signature creation device” means a qualified electronic signature creation device that is managed by a qualified trust service provider in accordance with Article 29a on behalf of a signatory;

(23b) “remote qualified electronic seal creation device” means a qualified electronic seal creation device that is managed by a qualified trust service provider in accordance with Article 39a on behalf of a seal creator;’;

(h) point (38) is replaced by the following:

‘(38) “certificate for website authentication” means an electronic attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued;’;

(i) point (41) is replaced by the following:

‘(41) “validation” means the process of verifying and confirming that data in electronic form are valid in accordance with this Regulation;’;

(j) the following points are added:

‘(42) “European Digital Identity Wallet” means an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals;

(43) “attribute” means a characteristic, quality, right or permission of a natural or legal person or of an object;

(44) “electronic attestation of attributes” means an attestation in electronic form that allows attributes to be authenticated;

(45) “qualified electronic attestation of attributes” means an electronic attestation of attributes which is issued by a qualified trust service provider and meets the requirements laid down in Annex V;

(46) “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 a public sector body that is responsible for an authentic source or by a public sector body that is designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45f and with Annex VII;

(47) “authentic source” means a repository or system, held under the responsibility of a public sector body or private entity, that contains and provides attributes about a natural or legal person or object and that is considered to be a primary source of that information or recognised as authentic in accordance with Union or national law, including administrative practice;

(48) “electronic archiving” means a service ensuring the receipt, storage, retrieval and deletion of electronic data and electronic documents in order to ensure their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period;

(49) “qualified electronic archiving service” means an electronic archiving service which is provided by a qualified trust service provider and which meets the requirements laid down in Article 45j;

(50) “EU Digital Identity Wallet Trust Mark” means a verifiable, simple and recognisable indication which is communicated in a clear manner that a European Digital Identity Wallet has been provided in accordance with this Regulation;

(51) “strong user authentication” means an authentication based on the use of at least two authentication factors from different categories of either knowledge, something only the user knows, possession, something only the user possesses or inherence, something the user is, that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data;

(52) “electronic ledger” means a sequence of electronic data records, ensuring the integrity of those records and the accuracy of the chronological ordering of those records;

(53) “qualified electronic ledger” means an electronic ledger which is provided by a qualified trust service provider and which meets the requirements laid down in Article 45l;

(54) “personal data” means any information as defined in Article 4, point (1), of Regulation (EU) 2016/679;

(55) “identity matching” means a process where person identification data, or electronic identification means are matched with or linked to an existing account belonging to the same person;

(56) “data record” means electronic data recorded with related meta-data supporting the processing of the data;

(57) “offline mode” means, as regards the use of European Digital Identity Wallets, an interaction between a user and a third party at a physical location using close proximity technologies, whereby the European Digital Identity Wallet is not required to access remote systems via electronic communication networks for the purpose of the interaction.’;

(4) Article 5 is replaced by the following:

‘*Article 5*
Pseudonyms in electronic transaction

Without prejudice to specific rules of Union or national law requiring users to identify themselves or to the legal effect given to pseudonyms under national law, the use of pseudonyms that are chosen by the user shall not be prohibited.’;

(5) in Chapter II, the following section is inserted:

‘SECTION 1
EUROPEAN DIGITAL IDENTITY WALLET

Article 5a
European Digital Identity Wallets

1. For the purpose of ensuring that all natural and legal 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. European Digital Identity Wallets shall be provided in one or more of the following ways:

   (a) directly by a Member State;

   (b) under a mandate from a Member State;

   (c) independently of a Member State but recognised by that Member State.

3. The source code of the application software components of European Digital Identity Wallets shall be open-source licensed. Member States may provide that, for duly justified reasons, the source code of specific components other than those installed on user devices shall not be disclosed.

4. European Digital Identity Wallets shall enable the user, in a manner that is user-friendly, transparent, and traceable by the user, to:

(a) securely request, obtain, select, combine, store, delete, share and present, under the sole control of the user, person identification data and, where applicable, in combination with electronic attestations of attributes, to authenticate to relying parties online and, where appropriate, in offline mode, in order to access public and private services, while ensuring that selective disclosure of data is possible;

(b) generate pseudonyms and store them encrypted and locally within the European Digital Identity Wallet;

(c) securely authenticate another person's European Digital Identity Wallet, and receive and share person identification data and electronic attestations of attributes in a secured way between the two European Digital Identity Wallets;

(d) access a log of all transactions carried out through the European Digital Identity Wallet via a common dashboard enabling the user to:

(i) view an up-to-date list of relying parties with which the user has established a connection and, where applicable, all data exchanged;

(ii) easily request the erasure by a relying party of personal data pursuant to Article 17 of the Regulation (EU) 2016/679;

(iii) easily report a relying party to the competent national data protection authority, where an allegedly unlawful or suspicious request for data is received;

(e) sign by means of qualified electronic signatures or seal by means of qualified electronic seals;

(f) download, to the extent technically feasible, the user's data, electronic attestation of attributes and configurations;

(g) exercise the user's rights to data portability.

5. European Digital Identity Wallets shall, in particular:

(a) support common protocols and interfaces:

(i) for issuance of person identification data, qualified and non-qualified electronic attestations of attributes or qualified and non-qualified certificates to the European Digital Identity Wallet;

(ii) for relying parties to request and validate person identification data and electronic attestations of attributes;

(iii) for the sharing and presentation to relying parties of person identification data, electronic attestation of attributes or of selectively disclosed related data online and, where appropriate, in offline mode;

(iv) for the user to allow interaction with the European Digital Identity Wallet and display an EU Digital Identity Wallet Trust Mark;

(v) to securely onboard the user by using an electronic identification means in accordance with Article 5a(24);

(vi) for interaction between two persons' European Digital Identity Wallets for the purpose of receiving, validating and sharing person identification data and electronic attestations of attributes in a secure manner;

(vii) for authenticating and identifying relying parties by implementing authentication mechanisms in accordance with Article 5b;

(viii) for relying parties to verify the authenticity and validity of European Digital Identity Wallets;

(ix) for requesting a relying party the erasure of personal data pursuant to Article 17 of Regulation (EU) 2016/679;

(x) for reporting a relying party to the competent national data protection authority where an allegedly unlawful or suspicious request for data is received;

(xi) for the creation of qualified electronic signatures or electronic seals by means of qualified electronic signature or electronic seal creation devices;

(b) not provide any information to trust service providers of electronic attestations of attributes about the use of those electronic attestations;

(c) ensure that the relying parties can be authenticated and identified by implementing authentication mechanisms in accordance with Article 5b;

(d) meet the requirements set out in Article 8 with regard to assurance level high, in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication;

(e) in the case of the electronic attestation of attributes with embedded disclosure policies, implement the appropriate mechanism to inform the user that the relying party or the user of the European Digital Identity Wallet requesting that electronic attestation of attributes has the permission to access such attestation;

(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, legal person or the natural person representing the natural or legal person, and is associated with that European Digital Identity Wallet;

(g) offer all natural persons the ability to sign by means of qualified electronic signatures by default and free of charge.

Notwithstanding point (g) of the first subparagraph, Member States may provide for proportionate measures to ensure that the use of qualified electronic signatures free-of-charge by natural persons is limited to non-professional purposes.

6. Member State shall inform users, without delay, of any security breach that could have entirely or partially compromised their European Digital Identity Wallet or its contents, in particular if their European Digital Identity Wallet has been suspended or revoked pursuant to Article 5e.

7. Without prejudice to Article 5f, Member States may provide, in accordance with national law, for additional functionalities of European Digital Identity Wallets, including interoperability with existing national electronic identification means. Those additional functionalities shall comply with this Article.

8. Member States shall provide validation mechanisms free-of-charge, in order to:

   (a) ensure that the authenticity and validity of European Digital Identity Wallets can be verified;

   (b) allow users to verify the authenticity and validity of the identity of relying parties registered in accordance with Article 5b.

9. Member States shall ensure that the validity of the European Digital Identity Wallet can be revoked in the following circumstances:

   (a) upon the explicit request of the user;

   (b) where the security of the European Digital Identity Wallet has been compromised;

   (c) upon the death of the user or cease of activity of the legal person.

10. Providers of European Digital Identity Wallets shall ensure that users can easily request technical support and report technical problems or any other incidents having a negative impact on the use of European Digital Identity Wallets.

11. European Digital Identity Wallets shall be provided under an electronic identification scheme with assurance level high.

12. European Digital Identity Wallets shall ensure security-by-design.

13. The issuance, use and revocation of the European Digital Identity Wallets shall be free of charge to all natural persons.

14. Users shall have full control of the use of and of the data in their European Digital Identity Wallet. The provider of the European Digital Identity Wallet shall neither collect information about the use of the European Digital Identity Wallet which is not necessary for the provision of European Digital Identity Wallet services, nor combine person identification data or any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by that provider or from third-party services which are not necessary for the provision of European Digital Identity Wallet services, unless the user has expressly requested otherwise. Personal data relating to the provision of the European Digital Identity Wallet shall be kept logically separate from any other data held by the provider of the European Digital Identity Wallet. If the European Digital Identity Wallet is provided by private parties in accordance with paragraph 2, points (b) and (c), of this Article, the provisions of Article 45h(3) shall apply *mutatis mutandis.*

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 or legal 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.

16. The technical framework of the European Digital Identity Wallet shall:

    (a) not allow providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to obtain data that allows transactions or user behaviour to be tracked, linked or correlated, or knowledge of transactions or user behaviour to be otherwise obtained, unless explicitly authorised by the user;

    (b) enable privacy preserving techniques which ensure unlikability, where the attestation of attributes does not require the identification of the user.

17. Any processing of personal data carried out by the Member States or on their behalf by bodies or parties responsible for the provision of European Digital Identity Wallets as electronic identification means shall be carried out in accordance with appropriate and effective data protection measures. Compliance of such processing with Regulation (EU) 2016/679 shall be demonstrated. Member States may introduce national provisions to further specify the application of such measures.

18. Member States shall, without undue delay, notify the Commission of information about:

(a) the body responsible for establishing and maintaining the list of registered relying parties that rely on European Digital Identity Wallets in accordance with Article 5b(5) and the location of that list;

(b) the bodies responsible for the provision of European Digital Identity Wallets in accordance with Article 5a(1);

(c) the bodies responsible for ensuring that the person identification data is associated with the European Digital Identity Wallet in accordance with Article 5a(5), point (f);

(d) the mechanism allowing for the validation of the person identification data referred to in Article 5a(5), point (f), and of the identity of the relying parties;

(e) the mechanism by which to validate the authenticity and validity of European Digital Identity Wallets.

The Commission shall make available the information notified pursuant to the first subparagraph to the public through a secure channel, in electronically signed or sealed form suitable for automated processing.

19. Without prejudice to paragraph 22 of this Article, Article 11 shall apply *mutatis mutandis* to the European Digital Identity Wallet.

20. Article 24(2), points (b), and (d) to (h), shall apply *mutatis mutandis* to providers of European Digital Identity Wallets.

21. European Digital Identity Wallets shall be made accessible for use, by persons with disabilities, on an equal basis with other users, in accordance with Directive (EU) 2019/882 of the European Parliament and of the Council*.

22. For the purposes of the provision of European Digital Identity Wallets, European Digital Identity Wallets and the electronic identification schemes under which they are provided shall not be subject to the requirements laid down in Articles 7, 9, 10, 12 and 12a.

23. By … [6 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraphs 4, 5, 8 and 18 of this Article on the implementation of the European Digital Identity Wallet. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

24. The Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures in order to facilitate the onboarding of users to the European Digital Identity Wallet either by electronic identification means conforming to assurance level high or by electronic identification means conforming to assurance level substantial in conjunction with additional remote onboarding procedures that together meet the requirements of assurance level high. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 5b

European Digital Identity Wallet-Relying Parties

1. Where a relying party intends to rely upon European Digital Identity Wallets for the provision of public or private services by means of digital interaction, the relying party shall register in the Member State where it is established.

2. The registration process shall be cost-effective and proportionate-to-risk. The relying party shall provide at least:

   (a) the information necessary to authenticate to European Digital Identity Wallets, which as a minimum includes:

      (i) the Member State in which the relying party is established; and

      (ii) the name of the relying party and, where applicable, its registration number as stated in an official record together with identification data of that official record;

(b) the contact details of the relying party;

(c) the intended use of European Digital Identity Wallets, including an indication of the data to be requested by the relying party from users.

3. Relying parties shall not request users to provide any data other than that indicated pursuant to paragraph 2, point (c).

4. Paragraphs 1 and 2 shall be without prejudice to Union or national law that is applicable to the provision of specific services.

5. Member States shall make the information referred to in paragraph 2 publicly available online in electronically signed or sealed form suitable for automated processing.

6. Relying parties registered in accordance with this Article shall inform Member States without delay about any changes to the information provided in the registration pursuant to paragraph 2.

7. Member States shall provide a common mechanism for allowing the identification and authentication of relying parties, as referred to in Article 5a(5), point (c).

8. Where relying parties intend to rely upon European Digital Identity Wallets, they shall identify themselves to the user.

9. Relying parties shall be responsible for carrying out the procedure for authenticating and validating person identification data and electronic attestation of attributes requested from European Digital Identity Wallets. Relying parties shall not refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.

10. Intermediaries acting on behalf of relying parties shall be deemed to be relying parties and shall not store data about the content of the transaction.

11. By ... [6 months from the date of entry into force of this amending Regulation], the Commission shall establish technical specifications and procedures for the requirements referred to in paragraphs 2, 5 and 6 to 9 of this Article by means of implementing acts on the implementation of European Digital Identity Wallets as referred to in Article 5a(23). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 5c

Certification of European Digital Identity Wallets

1. The conformity of European Digital Identity Wallets and the electronic identification scheme under which they are provided with the requirements laid down in Article 5a(4), (5), (8), the requirement for logical separation laid down in Article 5a(14) and, where applicable, with the standards and technical specifications referred to in Article 5a(24), shall be certified by conformity assessment bodies designated by Member States.

2. Certification of the conformity of European Digital Identity Wallets with requirements referred to in paragraph 1 of this Article, or parts thereof, that are relevant for cybersecurity shall be carried out in accordance with European cybersecurity certification schemes adopted pursuant to Regulation (EU) 2019/881 of the European Parliament and of the Council[**] and referred to in the implementing acts referred to in paragraph 6 of this Article.

3. For requirements referred to in paragraph 1 of this Article that are not relevant for cybersecurity, and, for requirements referred to in paragraph 1 of this Article that are relevant for cybersecurity, to the extent that cybersecurity certification schemes as referred to in paragraph 2 of this Article do not, or only partially, cover those cybersecurity requirements, also for those requirements, Member States shall establish national certification schemes following the requirements set out in the implementing acts referred to in paragraph 6 of this Article. Member States shall transmit their draft national certification schemes to the European Digital Identity Cooperation Group established pursuant to Article 46e(1) (the "Cooperation Group"). The Cooperation Group may issue opinions and recommendations.

4. Certification pursuant to paragraph 1 shall be valid for up to five years, provided that a vulnerability assessment is carried out every two years. Where a vulnerability is identified and not remedied in a timely manner, certification shall be cancelled.

5. Compliance with the requirements set out in Article 5a of this Regulation related to the personal data processing operations may be certified pursuant to Regulation(EU) 2016/679.

6. By ... [6 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the certification of European Digital Identity Wallets referred to in paragraph 1, 2 and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

7. Member States shall communicate to the Commission the names and addresses of the conformity assessment bodies referred to in paragraph 1. The Commission shall make that information available to all Member States.

8. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 establishing specific criteria to be met by the designated conformity assessment bodies referred to in paragraph 1 of this Article.

Article 5d

Publication of a list of certified European Digital Identity Wallets

1. Member States shall inform the Commission and the Cooperation Group established pursuant to Article 46e(1) without undue delay of European Digital Identity Wallets that have been provided pursuant to Article 5a and certified by the conformity assessment bodies referred to in Article 5c(1). They shall inform the Commission and the Cooperation Group established pursuant to Article 46e(1), without undue delay if a certification is cancelled and shall state the reasons for the cancellation.

2. Without prejudice to Article 5a(18), the information provided by Member States referred to in paragraph 1 of this Article shall include at least:

(a) the certificate and certification assessment report of the certified European Digital Identity Wallet;

(b) a description of the electronic identification scheme under which the European Digital Identity Wallet is provided;

(c) the applicable supervisory regime and information on the liability regime with respect to the party providing the European Digital Identity Wallet;

(d) the authority or authorities responsible for the electronic identification scheme;

(e) arrangements for suspension or revocation of the electronic identification scheme or authentication or of the compromised parts concerned.

3. On the basis of the information received pursuant to paragraph 1, the Commission shall establish, publish in the *Official Journal of the European Union* and maintain in a machine-readable form a list of certified European Digital Identity Wallets.

4. A Member State may submit a request to the Commission to remove a European Digital Identity Wallet and the electronic identification scheme under which it is provided from the list referred to in paragraph 3.

5. Where there are changes to the information provided pursuant to paragraph 1, the Member State shall provide the Commission with updated information.

6. The Commission shall keep the list referred to in paragraph 3 updated by publishing in the *Official Journal of the European Union* the corresponding amendments to the list within one month of receipt of a request pursuant to paragraph 4 or of updated information pursuant to paragraph 5.

7. By ... [6 months from the date of entry into force of this amending Regulation], the Commission shall establish the formats and procedures applicable for the purposes of paragraphs 1, 4 and 5 of this Article by means of implementing acts on the implementation of European Digital Identity Wallets as referred to in Article 5a(23). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 5e

Security breach of European Digital Identity Wallets

1. Where European Digital Identity Wallets provided pursuant to Article 5a, the validation mechanisms referred to in Article 5a(8) or the electronic identification scheme under which the European Digital Identity Wallets are provided are breached or partly compromised in a manner that affects their reliability or the reliability of other European Digital Identity Wallets, the Member State that provided the European Digital Identity Wallets shall, without undue delay, suspend the provision and the use of European Digital Identity Wallets.

   Where justified by the severity of the security breach or compromise referred to in the first subparagraph, the Member State shall withdraw European Digital Identity Wallets without undue delay.

The Member State shall inform the users affected, the single points of contact designated pursuant to Article 46c(1), the relying parties and the Commission accordingly.

2. If the security breach or compromise referred to in paragraph 1, first subparagraph, of this Article is not remedied within three months of the suspension, the Member State that provided the European Digital Identity Wallets shall withdraw European Digital Identity Wallets and revoke their validity. The Member State shall inform the users affected, the single points of contact designated pursuant to Article 46c(1), the relying parties and the Commission of the withdrawal accordingly.

3. Where the security breach or compromise referred to in paragraph 1, first subparagraph, of this Article is remedied, the providing Member State shall re-establish the provision and the use of European Digital Identity Wallets and inform the affected users and relying parties, the single points of contact designated pursuant to Article 46c(1) and the Commission without undue delay.

4. The Commission shall publish in the *Official Journal of the European Union* the corresponding amendments to the list referred to in Article 5d without undue delay.

5. By … [6 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the measures referred to 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 48(2).

Article 5f

Cross-border reliance on European Digital Identity Wallets

1. Where Member States require electronic identification and authentication to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets that are provided in accordance with this Regulation.

2. Where private relying parties that provide services, with the exception of microenterprises and small enterprises as defined in Article 2 of the Annex to Commission Recommendation 2003/361/EC***, are required by Union or national law to use strong user authentication for online identification or where strong user authentication for online identification is required by contractual obligation, including in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, those private relying parties shall, no later than 36 months from the date of entry into force of the implementing acts referred to in Article 5a(23) and Article 5c(6) and only upon the voluntary request of the user, also accept European Digital Identity Wallets that are provided in accordance with this Regulation.

3. Where providers of very large online platforms as referred to in Article 33 of Regulation (EU) 2022/2065 of the European Parliament and of the Council**** require user authentication for access to online services, they shall also accept and facilitate the use of European Digital Identity Wallets that are provided in accordance with this Regulation for user authentication only upon the voluntary request of the user and in respect of the minimum data necessary for the specific online service for which authentication is requested.

4. In cooperation with Member States, the Commission shall facilitate the development of codes of conduct in close collaboration with all relevant stakeholders, including civil society, in order to contribute to the wide availability and usability of European Digital Identity Wallets within the scope of this Regulation, and to encourage service providers to complete the development of codes of conduct.

5. Within 24 months after deployment of the European Digital Identity Wallets, the Commission shall assess the demand for, and the availability and usability of, European Digital Identity Wallets, taking into account criteria such as user take-up, cross-border presence of service providers, technological developments, evolution in usage patterns and consumer demand.

---

* Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (OJ L 151, 7.6.2019, p. 70).

** Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

*** Commission Recommendation 2003/361/EC of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises (OJ L 124, 20.5.2003, p. 36).

**** Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (OJ L 277, 27.10.2022, p. 1).’;

(6) the following heading is inserted before Article 6:

‘SECTION 2
ELECTRONIC IDENTIFICATION SCHEMES’;

(7) in Article 7, point (g) is replaced by the following:

‘(g) at least six months prior to notification pursuant to Article 9(1), the notifying Member State provides the other Member States, for the purposes of Article 12(5), with a description of that scheme in accordance with the procedural arrangements established by the implementing acts adopted pursuant to Article 12(6);’;

(8) in Article 8(3), the first subparagraph is replaced by the following:

‘3 By 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification means.’;

(9) in Article 9, paragraphs 2 and 3 are replaced by the following:

‘2. The Commission shall, without undue delay, publish in the *Official Journal of the European Union* a list of the electronic identification schemes which were notified pursuant to paragraph 1 together with basic information about those schemes.

3. The Commission shall publish in the *Official Journal of the European Union* the amendments to the list referred to in paragraph 2 within one month of the date of receipt of that notification.';

(10) in Article 10, the title is replaced by the following:

'Security breach of electronic identification schemes';

(11) the following article is inserted:

'*Article 11a*
Cross-border identity matching

1. When acting as relying parties for cross-border services, Member States shall ensure unequivocal identity matching for natural persons using notified electronic identification means or European Digital Identity Wallets.

2. Member States shall provide for technical and organisational measures to ensure a high level of protection of personal data used for identity matching and to prevent the profiling of users.

3. By … [6 months from the date of entry into force of this amending Regulation], the Commission shall establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraph 1 of this Article by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(12) Article 12 is amended as follows:

(a) the title is replaced by the following:

‘Interoperability’;

(b) paragraph 3 is amended as follows:

(i) point (c) is replaced by the following:

‘(c) it facilitates the implementation of privacy and security by design;’;

(ii) point (d) is deleted;

(c) in paragraph 4, point (d) is replaced by the following:

‘(d) a reference to a minimum set of person identification data necessary to uniquely represent a natural or legal person, or a natural person representing another natural person or a legal person, which is available from electronic identification schemes;’;

(d) paragraphs 5 and 6 are replaced by the following:

‘5. Member States shall carry out peer reviews of the electronic identification schemes that fall within the scope of this Regulation and that are to be notified pursuant to Article 9(1), point (a).

6. By 18 March 2025, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements for the peer reviews referred to in paragraph 5 of this Article with a view to fostering a high level of trust and security appropriate to the degree of risk. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(e) paragraph 7 is deleted;

(f) paragraph 8 is replaced by the following:

'8. By 18 September 2025, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1 of this Article, the Commission shall, subject to the criteria set out in paragraph 3 of this Article and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(13) the following articles are inserted in Chapter II:

‘*Article 12a*

Certification of electronic identification schemes

1. The conformity of electronic identification schemes to be notified with the cybersecurity requirements laid down in this Regulation, including conformity with the cybersecurity relevant requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes, shall be certified by conformity assessment bodies designated by Member States.

2. Certification pursuant to paragraph 1 of this Article shall be carried out under a relevant cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 or parts thereof, insofar as the cybersecurity certificate or parts thereof cover those cybersecurity requirements.

3. Certification pursuant to paragraph 1 shall be valid for up to five years, provided that a vulnerability assessment is carried out every two years. Where a vulnerability is identified and not remedied within three months of such identification, certification shall be cancelled.

4. Notwithstanding paragraph 2, Member States may request, in accordance with that paragraph, additional information from a notifying Member State about electronic identification schemes or part thereof certified.

5. The peer review of electronic identification schemes referred to in Article 12(5) shall not apply to electronic identification schemes or parts of such schemes certified in accordance with paragraph 1 of this Article. Member States may use a certificate or a statement of conformity, issued in accordance with a relevant certification scheme or parts of such schemes, with the non-cybersecurity-related requirements set out in Article 8(2) regarding the assurance level of electronic identification schemes.

6. Member States shall communicate to the Commission the names and addresses of the conformity assessment bodies referred to in paragraph 1. The Commission shall make that information available to all Member States.

Article 12b

Access to hardware and software features

Where providers of European Digital Identity Wallets and issuers of notified electronic identification means that act in a commercial or professional capacity and use core platform services as defined in Article 2, point (2), of Regulation (EU) 2022/1925 of the European Parliament and of the Council* for the purpose or in the course of providing European Digital Identity Wallet services and electronic identification means to end-users are business users as defined in Article 2, point (21), of that Regulation, gatekeepers shall in particular allow them effective interoperability with, and, for the purposes of interoperability, access to, the same operating system, hardware or software features. Such effective interoperability and access shall be allowed free of charge and regardless of whether the hardware or software features are part of the operating system, are available to, or are used by, that gatekeeper when providing such services, within the meaning of Article 6(7) of Regulation (EU) 2022/1925. This Article is without prejudice to Article 5a(14) of this Regulation.

_____

* Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) (OJ L 265, 12.10.2022, p. 1).';

(14) in Article 13, paragraph 1 is replaced by the following:

‘1. Notwithstanding paragraph 2 of this Article and without prejudice to Regulation (EU) 2016/679, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation. Any natural or legal person who has suffered material or non-material damage as a result of an infringement of this Regulation by a trust service provider shall have the right to seek compensation in accordance with Union and national law.

The burden of proving the intention or negligence of a non-qualified trust service provider shall lie with the natural or legal person claiming the damage referred to in the first subparagraph.

The intention or negligence of a qualified trust service provider shall be presumed unless that qualified trust service provider proves that the damage referred to in the first subparagraph occurred without the intention or negligence of that qualified trust service provider.’;

(15) Articles 14, 15 and 16 are replaced by the following:

‘*Article 14*

International aspects

1. Trust services provided by trust service providers established in a third country or by an international organisation shall be recognised as legally equivalent to qualified trust services provided by qualified trust service providers established in the Union, where the trust services originating from the third country or from the international organisation are recognised by means of implementing acts or an agreement concluded between the Union and the third country or the international organisation pursuant to Article 218 TFEU.

   The implementing acts referred to in the first subparagraph shall be adopted in accordance with the examination procedure referred to in Article 48(2).

2. The implementing acts and the agreement referred to in paragraph 1 shall ensure that the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are met by the trust service providers in the third country concerned or by the international organisation and by the trust services they provide. Third countries and international organisations shall in particular establish, maintain and publish a trusted list of recognised trust service providers.

3. The agreement referred to in paragraph 1 shall ensure that the qualified trust services provided by qualified trust service providers established in the Union are recognised as legally equivalent to trust services provided by trust service providers in the third country or by the international organisation with which the agreement is concluded.

Article 15

Accessibility for persons with disabilities and special needs

The provision of electronic identification means, trust services and end-user products that are used in the provision of those services shall be made available in plain and intelligible language, in accordance with the United Nations Convention on the Rights of Persons with Disabilities and with the accessibility requirements of Directive (EU) 2019/882, thus also benefiting persons who experience functional limitations, such as elderly people, and persons with limited access to digital technologies.

Article 16

Penalties

1. Without prejudice to Article 31 of Directive (EU) 2022/2555 of the European Parliament and of the Council*, Member States shall lay down the rules on penalties applicable to infringements of this Regulation. Those penalties shall be effective, proportionate and dissuasive.

2. Member States shall ensure that infringements of this Regulation by qualified and non-qualified trust service providers be subject to administrative fines of a maximum of at least:

(a) EUR 5 000 000 where the trust service provider is a natural person; or

(b) where the trust service provider is a legal person, EUR 5 000 000 or 1 % of the total worldwide annual turnover of the undertaking to which the trust service provider belonged in the financial year preceding the year in which the infringement occurred, whichever is higher.

3. Depending on the legal system of the Member States, the rules on administrative fines may be applied in such a manner that the fine is initiated by the competent supervisory body and imposed by competent national courts. The application of such rules in those Member States shall ensure that those legal remedies are effective and have an equivalent effect to administrative fines imposed directly by supervisory authorities.

---

* Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).’;

(16) in Chapter III, Section 2, the title is replaced by the following:

‘Non-qualified trust services’;

(17) Articles 17 and 18 are deleted;

(18) the following article is inserted in Chapter III, Section 2:

‘*Article 19a*
Requirements for non-qualified trust service providers

1. A non-qualified trust service provider providing non-qualified trust services shall:

(a) have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the non-qualified trust service, which shall, notwithstanding Article 21 of Directive (EU) 2022/2555, include at least measures relating to:

(i) registration and onboarding procedures for a trust service;

(ii) procedural or administrative checks needed to provide trust services;

(iii) the management and implementation of trust services;

(b) notifying the supervisory body, the identifiable affected individuals, the public if it is of public interest and, where applicable, other relevant competent authorities, of any security breaches or disruptions in the provision of the service or the implementation of the measures referred to in point (a) (i), (ii) or (iii), that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any case no later than 24 hours of having become aware of any security breaches or disruptions.

2. By … [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for paragraph 1, point (a), of this Article. Compliance with the requirements laid down in this Article shall be presumed where those standards, specifications and procedures are met. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(19) Article 20 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The audit shall confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation and in Article 21 of Directive (EU) 2022/2555. Qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within three working days of receipt.'

(b) the following paragraphs are inserted:

‘1a. Qualified trust service providers shall inform the supervisory body at the latest one month before any planned audits and shall allow the supervisory body to participate as an observer upon request.

1b. Member States shall, without undue delay, notify to the Commission the names, addresses and accreditation details of the conformity assessment bodies referred to in paragraph 1 and any subsequent changes thereto. The Commission shall make that information available to all Member States.’;

(c) paragraphs 2, 3 and 4 are replaced by the following:

‘2. Without prejudice to paragraph 1, the supervisory body may at any time audit or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers, at the expense of those trust service providers, to confirm that they and the qualified trust services provided by them fulfil the requirements laid down in this Regulation. Where personal data protection rules appear to have been breached, the supervisory body shall, without undue delay, inform the competent supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679.

3. Where the qualified trust service provider fails to fulfil any of the requirements set out by this Regulation, the supervisory body shall require it to provide a remedy within a set time limit, if applicable.

Where that provider does not provide a remedy and, where applicable within the time limit set by the supervisory body, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service it provides.

3a. Where the competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 informs the supervisory body that the qualified trust service provider fails to fulfil any of the requirements set out in Article 21 of that Directive, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service that it provides.

3b. Where the supervisory authorities established pursuant to Article 51 of Regulation (EU) 2016/679 informs the supervisory body that the qualified trust service provider fails to fulfil any of the requirements set out in that Regulation, the supervisory body, where justified in particular by the extent, duration and consequences of that failure, shall withdraw the qualified status of that provider or of the affected service it provides.

3c. The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned. The supervisory body shall inform the body notified pursuant to Article 22(3) of this Regulation for the purposes of updating the trusted lists referred to in paragraph 1 of that Article and the competent authority designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555.

4. By ... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the following:

(a) the accreditation of the conformity assessment bodies and for the conformity assessment report referred to in paragraph 1;

(b) the auditing requirements for the conformity assessment bodies to carry out their conformity assessment, including composite assessment, of the qualified trust service providers as referred to in paragraph 1;

(c) the conformity assessment schemes for carrying out the conformity assessment of the qualified trust service providers by the conformity assessment bodies and for the provision of the report referred to in paragraph 1.

Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(20) Article 21 is amended as follows:

(a) paragraphs 1 and 2 are replaced by the following:

‘1. Where trust service providers intend to start providing a qualified trust service, they shall notify the supervisory body of their intention together with a conformity assessment report issued by a conformity assessment body confirming the fulfilment of the requirements laid down in this Regulation and in Article 21 of Directive (EU) 2022/2555.

2. The supervisory body shall verify whether the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation and, in particular, with the requirements for qualified trust service providers and for the qualified trust services they provide.

In order to verify the compliance of the trust service provider with the requirements laid down in Article 21 of Directive (EU) 2022/2555, the supervisory body shall request the competent authorities designated or established pursuant to Article 8(1) of that Directive to carry out supervisory actions in that regard and to provide information about the outcome without undue delay and in any event within two months of receipt of that request. If the verification is not concluded within two months of the notification, those competent authorities shall inform the supervisory body specifying the reasons for the delay and the period within which the verification is to be concluded.

Where the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements laid down in this Regulation, the supervisory body shall grant qualified status to the trust service provider and the trust services it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1), not later than three months after notification in accordance with paragraph 1 of this Article.

Where the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider specifying the reasons for the delay and the period within which the verification is to be concluded.';

(b) paragraph 4 is replaced by the following:

'4. By ... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish the formats and procedures of the notification and verification for the purposes of paragraphs 1 and 2 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(21) Article 24 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. When issuing a qualified certificate or a qualified electronic attestation of attributes, a qualified trust service provider shall verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of attributes is to be issued.

1a. The verification of the identity referred to in paragraph 1 shall be performed, by appropriate means, by the qualified trust service provider, either directly or by means of a third party, on the basis of one of the following methods or, when needed, on a combination thereof in accordance with the implementing acts referred to in paragraph 1c:

(a) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to assurance level high;

(b) by means of a certificate of a qualified electronic signature or of a qualified electronic seal, issued in compliance with point (a), (c) or (d);

(c) by using other identification methods which ensure the identification of the person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;

(d) through the physical presence of the natural person or of an authorised representative of the legal person, by means of appropriate evidence and procedures, in accordance with national law.

1b. The verification of the attributes referred to in paragraph 1 shall be performed, by appropriate means, by the qualified trust service provider, either directly or by means of a third party, on the basis of one of the following methods or, where necessary, on a combination thereof, in accordance with the implementing acts referred to in paragraph 1c:

(a) by means of the European Digital Identity Wallet or a notified electronic identification means which meets the requirements set out in Article 8 with regard to assurance level high;

(b) by means of a certificate of a qualified electronic signature or of a qualified electronic seal, issued in accordance with paragraph 1a, point (a), (c) or (d);

(c) by means of a qualified electronic attestation of attributes;

(d) by using other methods, which ensure the verification of the attributes with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;

(e) by means of the physical presence of the natural person or of an authorised representative of the legal person, by means of appropriate evidence and procedures, in accordance with national law.

1c. By... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the verification of identity and attributes in accordance with paragraphs 1, 1a and 1b of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(b) paragraph 2 is amended as follows:

(i) point (a) is replaced by the following:

'(a) inform the supervisory body at least one month before implementing any change in the provision of its qualified trust services or at least three months in case of an intention to cease those activities;';

(ii) points (d) and (e) are replaced by the following:

'(d) before entering into a contractual relationship, inform, in a clear, comprehensive and easily accessible manner, in a publicly accessible space and individually any person seeking to use a qualified trust service of the precise terms and conditions regarding the use of that service, including any limitations on its use;

(e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them, including using suitable cryptographic techniques;';

(iii) the following points are inserted:

'(fa) notwithstanding Article 21 of Directive (EU) 2022/2555, have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the qualified trust service, including at least measures related to the following:

(i) registration and onboarding procedures for a service;

(ii) procedural or administrative checks;

(iii) the management and implementation of services;

(fb) notify the supervisory body, the identifiable affected individuals, other relevant competent bodies where applicable and, at the request of the supervisory body, the public if it is of public interest, of any security breaches or disruptions in the provision of the service or the implementation of the measures referred to in point (fa)(i), (ii) or (iii) that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any event within 24 hours of the incident;';

(iv) points (g), (h) and (i) are replaced by the following:

‘(g) take appropriate measures against forgery, theft or misappropriation of data or, without right, deleting, altering or rendering data inaccessible;

(h) record and keep accessible for as long as necessary after the activities of the qualified trust service provider have ceased, all relevant information concerning data issued and received by the qualified trust service provider, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;

(i) have an up-to-date termination plan to ensure the continuity of service in accordance with provisions that are verified by the supervisory body pursuant to Article 46b(4), point (i);’;

(v) point (j) is deleted;

(vi) the following subparagraph is added:

‘The supervisory body may request information in addition to the information notified pursuant to point (a) of the first subparagraph or the result of a conformity assessment and may condition the granting of the permission to implement the intended changes to the qualified trust services. If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider, specifying the reasons for the delay and the period within which the verification is to be concluded.’;

(c) paragraph 5 is replaced by the following:

‘4a. Paragraphs 3 and 4 shall apply accordingly to the revocation of qualified electronic attestations of attributes.

4b. The Commission shall be empowered to adopt delegated acts in accordance with Article 47, establishing additional measures referred to in paragraph 2, point (fa), of this Article.

5. By ... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements referred to in paragraph 2 of this Article. Compliance with the requirements laid down in this paragraph shall be presumed where those standards, specifications and procedures are met. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(22) the following article is inserted in Chapter III, Section 3:

‘*Article 24a*

Recognition of qualified trust services

1. Qualified electronic signatures based on a qualified certificate issued in one Member State and qualified electronic seals based on a qualified certificate issued in one Member State shall be recognised, respectively, as qualified electronic signatures and qualified electronic seals in all other Member States.

2. Qualified electronic signature creation devices and qualified electronic seal creation devices certified in one Member State shall be recognised, respectively, as qualified electronic signature creation devices and qualified electronic seal creation devices in all other Member States.

3. A qualified certificate for electronic signatures, a qualified certificate for electronic seals, a qualified trust service for the management of remote qualified electronic signature creation devices and a qualified trust service for the management of remote qualified electronic seal creation devices provided in one Member State shall be recognised, respectively, as a qualified certificate for electronic signatures, a qualified certificate for electronic seals, a qualified trust service for the management of remote qualified electronic signature creation devices and a qualified trust service for the management of remote qualified electronic seal creation devices in all other Member States.

4. A qualified validation service for qualified electronic signatures and a qualified validation service for qualified electronic seals provided in one Member State shall be recognised, respectively, as a qualified validation service for qualified electronic signatures and a qualified validation service for qualified electronic seals in all other Member States.

5. A qualified preservation service for qualified electronic signatures and a qualified preservation service for qualified electronic seals provided in one Member State shall be recognised, respectively, as a qualified preservation service for qualified electronic signatures and a qualified preservation service for qualified electronic seals in all other Member States.

6. A qualified electronic time stamp provided in one Member State shall be recognised as a qualified electronic time stamp in all other Member States.

7. A qualified certificate for website authentication issued in one Member State shall be recognised as a qualified certificate for website authentication in all other Member States.

8. A qualified electronic registered delivery service provided in one Member State shall be recognised as a qualified electronic registered delivery service in all other Member States.

9. A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified electronic attestation of attributes in all other Member States.

10. A qualified electronic archiving service provided in one Member State shall be recognised as a qualified electronic archiving service in all other Member States.

11. A qualified electronic ledger provided in one Member State shall be recognised as a qualified electronic ledger in all other Member States.';

(23) in Article 25, paragraph 3 is deleted;

(24) Article 26 is amended as follows:

(a) the single paragraph becomes paragraph 1;

(b) the following paragraph is added:

'2. By ... [24 months from the date of entry into force of this amended Regulation], the Commission shall assess whether it is necessary to adopt implementing acts to establish a list of reference standards and, where necessary, establish specifications and procedures for advanced electronic signatures. On the basis of that assessment, the Commission may adopt such implementing acts. Compliance with the requirements for advanced electronic signatures shall be presumed where an advanced electronic signature complies with the standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(25) in Article 27, paragraph 4 is deleted;

(26) in Article 28, paragraph 6 is replaced by the following:

‘6. By... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for electronic signature. Compliance with the requirements laid down in Annex I shall be presumed where a qualified certificate for electronic signature complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(27) in Article 29, the following paragraph is inserted:

‘1a. Generating or managing electronic signature creation data or duplicating such signature creation data for back-up purposes shall be carried out only on behalf of the signatory, at the request of the signatory, and by a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic signature creation device.’;

(28) the following article is inserted:

‘*Article 29a*

Requirements for a qualified service for the management of remote qualified electronic signature creation devices

1. The management of remote qualified electronic signature creation devices as a qualified service shall be carried out only by a qualified trust service provider that:

   (a) generates or manages electronic signature creation data on behalf of the signatory;

   (b) notwithstanding point (1)(d) of Annex II, duplicates the electronic signature creation data for back-up purposes only, provided that the following requirements are met:

      (i) the security of the duplicated datasets must be at the same level as for the original datasets;

      (ii) the number of duplicated datasets must not exceed the minimum needed to ensure continuity of the service;

   (c) complies with any requirements identified in the certification report of the specific remote qualified electronic signature creation device issued pursuant to Article 30.

2. By... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, specifications and procedures for the purposes of paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(29) in Article 30, the following paragraph is inserted:

'3a. The validity of a certification referred to in paragraph 1 shall not exceed five years, provided that vulnerabilities assessments are carried out every two years. Where vulnerabilities are identified and not remedied, the certification shall be cancelled.';

(30) in Article 31, paragraph 3 is replaced by the following:

'3. By... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish the formats and procedures applicable for the purpose of paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(31) Article 32 is amended as follows:

(a) in paragraph 1, the following subparagraph is added:

'Compliance with the requirements laid down in the first subparagraph of this paragraph shall be presumed where the validation of qualified electronic signatures complies with the standards, specifications and procedures referred to in paragraph 3.';

(b) paragraph 3 is replaced by the following:

‘3. By.... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the validation of qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(32) the following article is inserted:

‘*Article 32a*
Requirements for the validation of advanced electronic signatures based on qualified certificates

1. The process for the validation of an advanced electronic signature based on a qualified certificate shall confirm the validity of an advanced electronic signature based on a qualified certificate, provided that:

(a) the certificate that supports the signature was, at the time of signing, a qualified certificate for electronic signature complying with Annex I;

(b) the qualified certificate was issued by a qualified trust service provider and was valid at the time of signing;

(c) the signature validation data corresponds to the data provided to the relying party;

(d) the unique set of data representing the signatory in the certificate is correctly provided to the relying party;

(e) the use of any pseudonym is clearly indicated to the relying party if a pseudonym was used at the time of signing;

(f) the integrity of the signed data has not been compromised;

(g) the requirements provided for in Article 26 were met at the time of signing.

2. The system used for validating the advanced electronic signature based on qualified certificate shall provide to the relying party the correct result of the validation process and shall allow the relying party to detect any security relevant issues.

3. By ... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the validation of advanced electronic signatures based on qualified certificates. Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the validation of advanced electronic signature based on qualified certificates complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(33) in Article 33, paragraph 2 is replaced with the following text:'

'2. By.... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified validation service referred to in paragraph 1 of this Article. Compliance with the requirements laid down in paragraph 1 of this Article shall be presumed where the qualified validation service for qualified electronic signatures complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(34) Article 34 is amended as follows:

(a) the following paragraph is inserted:

'1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures complies with the standards, specifications and procedures referred to in paragraph 2.';

(b) paragraph 2 is replaced by the following:

'2. By... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the qualified preservation service for qualified electronic signatures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(35) in Article 35, paragraph 3 is deleted;

(36) Article 36 is amended as follows:

(a) the single paragraph becomes paragraph 1;

(b) the following paragraph is added:

‘2. By... [24 months from the date of entry into force of this amending Regulation], the Commission shall assess whether it is necessary to adopt implementing acts to establish a list of reference standards and, where necessary, establish specifications and procedures for advanced electronic seals. On the basis of that assessment, the Commission may adopt such implementing acts. Compliance with the requirements for advanced electronic seals shall be presumed where an advanced electronic seal complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(37) in Article 37, paragraph 4 is deleted;

(38) in Article 38, paragraph 6 is replaced by the following:

‘6. By... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for electronic seals. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(39) the following article is inserted:

‘*Article 39a*
Requirements for a qualified service for the management of remote qualified electronic seal creation devices

Article 29a shall apply *mutatis mutandis* to a qualified service for the management of remote qualified electronic seal creation devices.’;

(40) the following article is inserted in Chapter III, Section 5:

‘*Article 40a*
Requirements for the validation of advanced electronic seals based on qualified certificates

Article 32a shall apply *mutatis mutandis* to the validation of advanced electronic seals based on qualified certificates.’;

(41) in Article 41, paragraph 3 is deleted;

(42) Article 42 is amended as follows:

(a) the following paragraph is inserted:

‘1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the binding of date and time to data and the accuracy of the time source comply with the standards, specifications and procedures referred to in paragraph 2.’;

(b) paragraph 2 is replaced by the following

‘2. By ... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the binding of date and time to data and for establishing the accuracy of time sources. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(43) Article 44 is amended as follows:

(a) the following paragraph is inserted:

‘1a. Compliance with the requirements laid down in paragraph 1 shall be presumed where the process for sending and receiving data complies with the standards, specifications and procedures referred to in paragraph 2.’;

(b) paragraph 2 is replaced by the following:

‘2. By ... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for processes for sending and receiving data. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(c) the following paragraphs are inserted:

‘2a. Providers of qualified electronic registered delivery services may agree on interoperability between qualified electronic registered delivery services which they provide. Such interoperability framework shall comply with the requirements laid down in paragraph 1 and such compliance shall be confirmed by a conformity assessment body.

2b. The Commission may, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the interoperability framework referred to in paragraph 2a of this Article. The technical specifications and content of standards shall be cost-effective and proportionate. The implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(44) Article 45 is replaced by the following:

‘*Article 45*

Requirements for qualified certificates for website authentication

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV. The evaluation of compliance with those requirements shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 2 of this Article.

1a. Qualified certificates for website authentication issued in accordance with paragraph 1 of this Article shall be recognised by providers of web-browsers. Providers of web-browsers shall ensure that the identity data attested in the certificate and additional attested attributes are displayed in a user-friendly manner. Providers of web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1 of this Article, with the exception of microenterprises or small enterprises as defined in Article 2 of the Annex to Recommendation 2003/361/EC during the first five years of operating as providers of web-browsing services.

1b. Qualified certificates for website authentication shall not be subject to any mandatory requirements other than the requirements laid down in paragraph 1.

2. By ... [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified certificates for website authentication, referred to in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(45) the following article is inserted:

'*Article 45a*
Cybersecurity precautionary measures

1. Providers of web-browsers shall not take any measures contrary to their obligations set out in Article 45, in particular the requirements to recognise qualified certificates for website authentication and to display the identity data provided in a user-friendly manner.

2. By way of derogation from paragraph 1 and only in the event of substantiated concerns related to security breaches or the loss of integrity of an identified certificate or set of certificates, providers of web-browsers may take precautionary measures in relation to that certificate or set of certificates.

3. Where a provider of a web-browser takes precautionary measures pursuant to paragraph 2, the provider of the web-browser shall notify its concerns in writing, without undue delay, together with a description of the measures taken to mitigate those concerns, to the Commission, the competent supervisory body, the entity to whom the certificate was issued and to the qualified trust service provider that issued that certificate or set of certificates. Upon receipt of such a notification, the competent supervisory body shall issue an acknowledgement of receipt to the provider of the web-browser in question.

4. The competent supervisory body shall investigate the issues raised in the notification in accordance with Article 46b(4), point (k). Where the outcome of that investigation does not result in the withdrawal of the qualified status of the certificate, the supervisory body shall inform the provider of the web-browser accordingly and shall request that provider to put an end to the precautionary measures referred to in paragraph 2 of this Article.';

(46) the following sections are added in Chapter III:

‘SECTION 9
ELECTRONIC ATTESTATION OF ATTRIBUTES

Article 45b
Legal effects of electronic attestation of attributes

1. An electronic attestation of attributes shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole ground that it is in electronic form or that it does not meet the requirements for qualified electronic attestations of attributes.

2. A qualified electronic attestation of attributes and attestations of attributes issued by, or on behalf of, a public sector body responsible for an authentic source shall have the same legal effect as lawfully issued attestations in paper form.

3. An attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source in one Member State shall be recognised as an attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source in all Member States.

Article 45c

Electronic attestation of attributes in public services

Where an electronic identification using an electronic identification means and authentication is required under national law to access an online service provided by a public sector body, person identification data in the electronic attestation of attributes shall not substitute electronic identification using an electronic identification means and authentication for electronic identification unless specifically allowed by the Member State. In such a case, qualified electronic attestation of attributes from other Member States shall also be accepted.

Article 45d

Requirements for qualified electronic attestation of attributes

1. Qualified electronic attestation of attributes shall meet the requirements laid down in Annex V.

2. The evaluation of compliance with the requirements laid down in Annex V shall be carried out in accordance with the standards, specifications and procedures referred to in paragraph 5 of this Article.

3. Qualified electronic attestations of attributes shall not be subject to any mandatory requirement in addition to the requirements laid down in Annex V.

4. Where a qualified electronic attestation of attributes has been revoked after initial issuance, it shall lose its validity from the moment of its revocation and its status shall not in any circumstances be reverted.

5. By ... [6 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic attestations of attributes. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 45e

Verification of attributes against authentic sources

1. Member States shall ensure, within 24 months of the date of entry into force of the implementing acts referred to in Articles 5a(23) and 5c(6), that, at least for the attributes listed in Annex VI, wherever those attributes rely on authentic sources within the public sector, measures are taken to allow qualified trust service providers of electronic attestations of attributes to verify those attributes by electronic means at the request of the user, in accordance with Union or national law.

2. By … [6 months from the date of entry into force of this amending Regulation], the Commission shall, taking into account relevant international standards, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the catalogue of attributes, as well as schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes for the purposes of paragraph 1 of this Article. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 45f

Requirements for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source

1. An electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall meet the following requirements:

   (a) those set out in Annex VII;

   (b) the qualified certificate supporting the qualified electronic signature or qualified electronic seal of the public sector body referred to in Article 3, point (46), identified as the issuer referred to in point (b), of Annex VII, containing a specific set of certified attributes in a form suitable for automated processing and:

      (i) indicating that the issuing body is established in accordance with Union or national law as the responsible for the authentic source on the basis of which the electronic attestation of attributes is issued or as the body designated to act on its behalf;

      (ii) providing a set of data unambiguously representing the authentic source referred to in point (i); and

      (iii) identifying the Union or national law referred to in point (i).

2. The Member State where public sector bodies referred to in Article 3, point (46), are established shall ensure that the public sector bodies that issue electronic attestations of attributes meet a level of reliability and trustworthiness equivalent to qualified trust service providers in accordance with Article 24.

3. Member States shall notify public sector bodies referred to in Article 3, point (46), to the Commission. That notification shall include a conformity assessment report issued by a conformity assessment body confirming that the requirements set out in paragraphs 1, 2 and 6 of this Article are met. The Commission shall make available to the public, through a secure channel, the list of public sector bodies referred to in Article 3, point (46), in electronically signed or sealed form suitable for automated processing.

4. Where an electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source has been revoked after initial issuance, it shall lose its validity from the moment of its revocation and its status shall not be reverted.

5. An electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall be deemed to be compliant with the requirements laid down in paragraph 1, where it complies with the standards, specifications and procedures referred to in paragraph 6.

6. By … [6 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).

7. By … [6 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the purposes of paragraph 3 of this Article. Those implementing acts shall be consistent with the implementing acts referred to in Article 5a(23) on the implementation of the European Digital Identity Wallet. They shall be adopted in accordance with the examination procedure referred to in Article 48(2).

8. Public sector bodies referred to in Article 3, point (46), issuing electronic attestation of attributes shall provide an interface with European Digital Identity Wallets that are provided in accordance with Article 5a.

Article 45g

Issuing of electronic attestation of attributes to European Digital Identity Wallets

1. Providers of electronic attestations of attributes shall provide European Digital Identity Wallet users with the possibility to request, obtain, store and manage the electronic attestation of attributes irrespective of the Member State where the European Digital Identity Wallet is provided.

2. Providers of qualified electronic attestations of attributes shall provide an interface with European Digital Identity Wallets that are provided in accordance in Article 5a.

Article 45h

Additional rules for the provision of electronic attestation of attributes services

1. Providers of qualified and non-qualified electronic attestation of attributes services shall not combine personal data relating to the provision of those services with personal data from any other services offered by them or their commercial partners.

2. Personal data relating to the provision of electronic attestation of attributes services shall be kept logically separate from other data held by the provider of electronic attestation of attributes.

3. Providers of qualified electronic attestation of attributes' services shall implement the provision of such qualified trust services in a manner that is functionally separate from other services provided by them.

SECTION 10

ELECTRONIC ARCHIVING SERVICES

Article 45i

Legal effect of electronic archiving services

1. Electronic data and electronic documents preserved using an electronic archiving service shall not be denied legal effect or admissibility as evidence in legal proceedings on the sole ground that they are in electronic form or that they are not preserved using a qualified electronic archiving service.

2. Electronic data and electronic documents preserved using a qualified electronic archiving service shall enjoy the presumption of their integrity and of their origin for the duration of the preservation period by the qualified trust service provider.

Article 45j

Requirements for qualified electronic archiving services

1. Qualified electronic archive services shall meet the following requirements:

   (a) they are provided by qualified trust service providers;

   (b) they use procedures and technologies capable of ensuring the durability and legibility of electronic data and electronic documents beyond the technological validity period and at least throughout the legal or contractual preservation period, while maintaining their integrity and the accuracy of their origin;

(c) they ensure that those electronic data and those electronic documents are preserved in such a way that they are safeguarded against loss and alteration, except for changes concerning their medium or electronic format;

(d) they shall allow authorised relying parties to receive a report in an automated manner that confirms that electronic data and electronic documents retrieved from a qualified electronic archive enjoy the presumption of integrity of the data from the beginning of the preservation period to the moment of retrieval.

The report referred to in point (d) of the first subparagraph shall be provided in a reliable and efficient way and shall bear the qualified electronic signature or qualified electronic seal of the provider of the qualified electronic archiving service.

2. By … [12 months from the date of the entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for qualified electronic archiving services. Compliance with the requirements for qualified electronic archive services shall be presumed where a qualified electronic archive service complies with those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 11

ELECTRONIC LEDGERS

Article 45k

Legal effects of electronic ledgers

1. An electronic ledger shall not be denied legal effect or admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form or that it does not meet the requirements for qualified electronic ledgers.

2. Data records contained in a qualified electronic ledger shall enjoy the presumption of their unique and accurate sequential chronological ordering and of their integrity.

Article 45l

Requirements for qualified electronic ledgers

1. Qualified electronic ledgers shall meet the following requirements:

   (a) they are created and managed by one or more qualified trust service providers;

   (b) they establish the origin of data records in the ledger;

   (c) they ensure the unique sequential chronological ordering of data records in the ledger;

   (d) they record data in such a way that any subsequent change to the data is immediately detectable, ensuring their integrity over time.

2. Compliance with the requirements laid down in paragraph 1 shall be presumed where an electronic ledger complies with the standards, specifications and procedures referred to in paragraph 3.

3. By … [12 months from the date of the entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and, where necessary, establish specifications and procedures for the requirements laid down in paragraph 1 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(47) the following chapter is inserted:

'CHAPTER IVa
GOVERNANCE FRAMEWORK

Article 46a
Supervision of the European Digital Identity Wallet Framework

1. Member States shall designate one or more supervisory bodies established in their territory.

The supervisory bodies designated pursuant to the first subparagraph shall be given the necessary powers and adequate resources for the exercise of their tasks in an effective, efficient and independent manner.

2. Member States shall notify to the Commission the names and the addresses of their supervisory bodies designated pursuant to paragraph 1 and any subsequent changes thereto. The Commission shall publish a list of the notified supervisory bodies.

3. The role of the supervisory bodies designated pursuant to paragraph 1 shall be:

   (a) to supervise providers of European Digital Identity Wallets established in the designating Member State and to ensure, by means of *ex ante* and *ex post* supervisory activities, that those providers and European Digital Identity Wallets they provide meet the requirements laid down in this Regulation;

   (b) to take action, if necessary, in relation to providers of European Digital Identity Wallets established in the territory of the designating Member State, by means of *ex post* supervisory activities, when informed that providers or European Digital Identity Wallets that they provide infringe this Regulation.

4. The tasks of the supervisory bodies designated pursuant to paragraph 1 shall include, in particular, the following:

   (a) to cooperate with other supervisory bodies and to provide them with assistance in accordance with Articles 46c and 46e;

   (b) to request information necessary to monitor compliance with this Regulation;

(c) to inform the relevant competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 of the Member States concerned of any significant security breaches or loss of integrity of which they become aware in the performance of their tasks and, in the case of a significant security breach or loss of integrity which concerns other Member States, to inform the single point of contact designated or established pursuant to Article 8(3) of Directive (EU) 2022/2555 of the Member State concerned and the single points of contact designated pursuant to Article 46c(1) of this Regulation in the other Member States concerned, and to inform the public or require providers of European Digital Identity Wallet to do so where the supervisory body determines that disclosure of the security breach or of the loss of integrity would be in the public interest;

(d) to carry out on-site inspections and off-site supervision;

(e) to require that providers of European Digital Identity Wallets remedy any failure to fulfil the requirements laid down in this Regulation;

(f) to suspend or cancel the registration and inclusion of relying parties in the mechanism referred to in Article 5b(7) in the case of illegal or fraudulent use of the European Digital Identity Wallet;

(g) to cooperate with competent 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 infringed and about security breaches which appear to constitute personal data breaches.

5. Where the supervisory body designated pursuant to paragraph 1 requires the provider of a European Digital Identity Wallet to remedy any failure to fulfil requirements under this Regulation pursuant to paragraph 4, point (e), and that provider does not act accordingly and, if applicable, within a time limit set by that supervisory body, the supervisory body designated pursuant to paragraph 1 may, taking into account, in particular, the extent, duration and consequences of that failure, order the provider to suspend or to cease the provision of the European Digital Identity Wallet. The supervisory body shall inform the supervisory bodies of other Member States, the Commission, relying parties and users of the European Digital Identity Wallet without undue delay of the decision to require the suspension or cessation of the provision of the European Digital Identity Wallet.

6. By 31 March each year, each supervisory body designated pursuant to paragraph 1 shall submit to the Commission a report on its main activities in the previous calendar year. The Commission shall make those annual reports available to the European Parliament and the Council.

7. By … [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish the formats and procedures for the report referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 46b

Supervision of trust services

1. Member States shall designate a supervisory body established in their territory or designate, upon mutual agreement with another Member State, a supervisory body established in that other Member State. That supervisory body shall be responsible for supervisory tasks in the designating Member State as regards trust services.

   The supervisory bodies designated pursuant to the first subparagraph shall be given the necessary powers and adequate resources for the exercise of their tasks.

2. Member States shall notify to the Commission the names and addresses of their supervisory bodies designated pursuant to paragraph 1 and any subsequent changes thereto. The Commission shall publish a list of the notified supervisory bodies.

3. The role of the supervisory bodies designated pursuant to paragraph 1 shall be:

   (a) to supervise qualified trust service providers established in the territory of the designating Member State and to ensure, by means of *ex ante* and *ex post* supervisory activities, that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in this Regulation;

   (b) to take action, if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, by means of *ex post* supervisory activities, when informed that those non-qualified trust service providers or the trust services they provide allegedly do not meet the requirements laid down in this Regulation.

4. The tasks of the supervisory body designated pursuant to paragraph 1 shall include in particular the following:

(a) to inform the relevant competent authorities designated or established pursuant to Article 8(1) of Directive (EU) 2022/2555 of the Member States concerned of any significant security breach or loss of integrity of which it becomes aware in the performance of its tasks and, in the case of a significant security breach or loss of integrity which concerns other Member States, to inform the single point of contact designated or established pursuant to Article 8(3) Directive (EU) 2022/2555 of the Member State concerned and the single points of contact designated pursuant to Article 46c(1) of this Regulation in the other Member States concerned, and to inform the public or require the trust service provider 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;

(b) to cooperate with other supervisory bodies and to provide them with assistance in accordance with Articles 46c and 46e;

(c) to analyse the conformity assessment reports referred to in Article 20(1) and Article 21(1);

(d) to report to the Commission about its main activities in accordance with paragraph 6 of this Article;

(e) to carry out audits or request a conformity assessment body to perform a conformity assessment of the qualified trust service providers in accordance with Article 20(2);

(f) to cooperate with competent 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;

(g) to grant qualified status to trust service providers and to the services they provide, and to withdraw that status in accordance with Articles 20 and 21;

(h) to inform the body responsible for the national trusted list referred to in Article 22(3) of its decisions to grant or withdraw qualified status, unless that body is also the supervisory body designated pursuant to paragraph 1 of this Article;

(i) to verify the existence and correct application of provisions on termination plans where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with Article 24(2), point (h);

(j) to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation;

(k) to investigate claims made by providers of web-browsers pursuant to Article 45a and to take action if necessary.

5. Member States may require the supervisory body designated pursuant to paragraph 1 to establish, maintain and update a trust infrastructure in accordance with national law.

6. By 31 March each year, each supervisory body designated pursuant to paragraph 1 shall submit to the Commission a report on its main activities in the previous calendar year. The Commission shall make those annual reports available to the European Parliament and the Council.

7. By … [12 months from the date of entry into force of this amending Regulation], the Commission shall adopt guidelines on the exercise by the supervisory bodies designated pursuant to paragraph 1 of this Article of the tasks referred to in paragraph 4 of this Article, and, by means of implementing acts, establish the formats and procedures for the report referred to in paragraph 6 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 46c

Single points of contact

1. Each Member State shall designate a single point of contact for trust services, European Digital Identity Wallets and notified electronic identification schemes.

2. Each single point of contact shall exercise a liaison function to facilitate cross-border cooperation between the supervisory bodies for trust service providers and between the supervisory bodies for the providers of European Digital Identity Wallets and, where appropriate, with the Commission and European Union Agency for Cybersecurity (ENISA) and with other competent authorities within its Member State.

3. Each Member State shall make public and, without undue delay, notify to the Commission the names and the addresses of the single point of contact designated pursuant to paragraph 1 and any subsequent change thereto.

4. The Commission shall publish a list of the single points of contact notified pursuant to paragraph 3.

Article 46d

Mutual assistance

1. In order to facilitate the supervision and enforcement of obligations under this Regulation, the supervisory bodies designated pursuant to Article 46a(1) and Article 46b(1) may seek, including through the Cooperation Group established pursuant to Article 46e(1), mutual assistance from the supervisory bodies of another Member State where the provider of the European Digital Identity Wallet or the trust service provider is established, or where its network and information systems are located or its services are provided.

2. The mutual assistance shall at least entail that:

(a) the supervisory body applying supervisory and enforcement measures in one Member State shall inform and consult the supervisory body from the other Member State concerned;

(b) a supervisory body may request the supervisory body of another Member State concerned to take supervisory or enforcement measures, including, for instance, requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21 regarding the provision of trust services;

(c) where appropriate, supervisory bodies may carry out joint investigations with the supervisory bodies of other Member States.

The arrangements and procedures for joint actions under the first subparagraph shall be agreed upon and established by the Member States concerned in accordance with their national law.

3. A supervisory body to which a request for assistance is addressed may refuse that request on any of the following grounds:

(a) the assistance requested is not proportionate to the supervisory activities of the supervisory body carried out in accordance with Articles 46a and 46b;

(b) the supervisory body is not competent to provide the requested assistance;

(c) providing the requested assistance would be incompatible with this Regulation.

4. By … [12 months from the date of entry into force of this amending Regulation] and every two years thereafter, the Cooperation Group established pursuant to Article 46e(1) shall issue guidance on the organisational aspects and procedures for the mutual assistance referred to in paragraphs 1 and 2 of this Article.

Article 46e

The European Digital Identity Cooperation Group

1. In order to support and facilitate Member States' cross-border cooperation and exchange of information on trust services, European Digital Identity Wallets and notified electronic identification schemes, the Commission shall establish a European Digital Identity Cooperation Group (the "Cooperation Group").

2. The Cooperation Group shall be composed of representatives appointed by the Member States and of the Commission. The Cooperation Group shall be chaired by the Commission. The Commission shall provide the Cooperation Group's Secretariat.

3. Representatives of relevant stakeholders may, on an ad hoc basis, be invited to attend meetings of the Cooperation Group and to participate in its work as observers.

4. ENISA shall be invited to participate as observer in the workings of the Cooperation Group when it exchanges views, best practices and information on relevant cybersecurity aspects such as notification of security breaches, and when the use of cybersecurity certificates or standards are addressed.

5. The Cooperation Group shall have the following tasks:

   (a) exchange advice and cooperate with the Commission on emerging policy initiatives in the field of digital identity wallets, electronic identification means and trust services;

   (b) advise the Commission, as appropriate, in the early preparation of draft implementing and delegated acts to be adopted pursuant to this Regulation;

   (c) in order to support the supervisory bodies in the implementation of the provisions of this Regulation:

      (i) exchange best practices and information regarding the implementation of the provisions of this Regulation;

      (ii) assess the relevant developments in the digital identity wallet, electronic identification and trust services sectors;

      (iii) organise joint meetings with relevant interested parties from across the Union to discuss activities carried out by the cooperation group and gather input on emerging policy challenges;

(iv) with the support of ENISA, exchange views, best practices and information on relevant cybersecurity aspects concerning European Digital Identity Wallets, electronic identification schemes and trust services;

(v) exchange best practices in relation to the development and implementation of policies on the notification of security breaches, and common measures as referred to in Articles 5e and 10;

(vi) organise joint meetings with the NIS Cooperation Group established pursuant to Article 14(1) of Directive (EU) 2022/2555 to exchange relevant information in relation to trust services and electronic identification related cyber threats, incidents, vulnerabilities, awareness raising initiatives, trainings, exercises and skills, capacity building, standards and technical specifications capacity as well as standards and technical specifications;

(vii) discuss, upon a request of a supervisory body, specific requests for mutual assistance as referred to in Article 46d;

(viii) facilitate the exchange of information between the supervisory bodies by providing guidance on the organisational aspects and procedures for the mutual assistance referred to in Article 46d;

(d) organise peer reviews of electronic identification schemes to be notified under this Regulation.

6. Member States shall ensure effective and efficient cooperation of their designated representatives in the Cooperation Group.

7. By … [12 months from the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in paragraph 5, point (d), of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(48) Article 47 is amended as follows:

(a) paragraphs 2 and 3 are replaced by the following:

'2. The power to adopt delegated acts referred to in Article 5c(7), Article 24(6) and Article 30(4) shall be conferred on the Commission for an indeterminate period of time from 17 September 2014.

3. The delegation of power referred to in Article 5c(7), Article 24(6) and Article 30(4) may be revoked at any time by the European Parliament or by the Council. A decision to revoke shall put an end to the delegation of the power specified in that decision. It shall take effect the day following the publication of the decision in the *Official Journal of the European Union* or at a later date specified therein. It shall not affect the validity of any delegated acts already in force.';

(b) paragraph 5 is replaced by the following:

‘5. A delegated act adopted pursuant to Article 5c(7), Article 24(6) or Article 30(4) shall enter into force only if no objection has been expressed either by the European Parliament or the Council within a period of two months of notification of that act to the European Parliament and the Council or if, before the expiry of that period, the European Parliament and the Council have both informed the Commission that they will not object. That period shall be extended by two months at the initiative of the European Parliament or of the Council.’;

(49) the following article is inserted in Chapter VI:

‘*Article 48a*

Reporting requirements

1. Member States shall ensure the collection of statistics in relation to the functioning of European Digital Identity Wallets and the qualified trust services provided on their territory.

2. The statistics collected in accordance with paragraph 1 shall include the following:

(a) the number of natural and legal persons having a valid European Digital Identity Wallet;

(b) the type and number of services accepting the use of the European Digital Identity Wallet;

(c) the number of user complaints and consumer protection or data protection incidents relating to relying parties and qualified trust services;

(d) a summary report including data on incidents preventing the use of the European Digital Identity Wallet;

(e) a summary of significant security incidents, data breaches and affected users of European Digital Identity Wallets or of qualified trust services.

3. The statistics referred to in paragraph 2 shall be made available to the public in an open and commonly used, machine-readable format.

4. By 31 March each year, Member States shall submit to the Commission a report on the statistics collected in accordance with paragraph 2.';

(50) Article 49 is replaced by the following:

'*Article 49*
Review

1. The Commission shall review the application of this Regulation and shall, by ... [24 months from the date of entry into force of the amending Regulation], submit a report to the European Parliament and to the Council. In that report, the Commission shall, in particular, evaluate whether it is appropriate to modify the scope of this Regulation or its specific provisions including, in particular, the provisions included in Article 5c(5), taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments. Where necessary, that report shall be accompanied by a proposal to amend this Regulation.

2. The report referred to in paragraph 1 shall include an assessment of the availability, security and usability of the notified electronic identification means and European Digital Identity Wallets that fall within the scope of this Regulation and assess whether all online private service providers relying on third-party electronic identification services for users authentication, shall be required to accept the use of notified electronic identification means and European Digital Identity Wallet.

3. By ... [6 years from the date of entry into force of this amending Regulation] and every four years thereafter, the Commission shall submit a report to the European Parliament and the Council on progress made towards achieving the objectives of this Regulation.';

(51) Article 51 is replaced by the following:

'*Article 51*
Transitional measures

1. Secure signature creation devices of which the conformity has been determined in accordance with Article 3(4) of Directive 1999/93/EC shall continue to be considered to be qualified electronic signature creation devices under this Regulation until … [36 months from the date of entry into force of this amending Regulation].

2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall continue to be considered as qualified certificates for electronic signatures under this Regulation until … [24 months from the date of entry into force of this amending Regulation].

3. The management of remote qualified electronic signature and seal creation devices by qualified trust service providers other than qualified trust service providers providing qualified trust services for the management of remote qualified electronic signature and seal creation devices in accordance with Articles 29a and 39a may be carried out without the need to obtain the qualified status for the provision of these management services until … [24 months from the date of entry into force of this amending Regulation].

4. Qualified trust service providers that have been granted their qualified status under this Regulation before ... [date of entry into force of this amending Regulation] shall submit a conformity assessment report to the supervisory body proving compliance with Article 24(1), (1a) and (1b) as soon as possible and in any event by … [24 months from the date of entry into force of this amending Regulation].'

(52) Annexes I to IV are amended, respectively, in accordance with Annexes I to IV to this Regulation;

(53) new Annexes V, VI and VII are added as set out in Annexes V, VI and VII to this Regulation.

Article 2

Entry into force

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

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

Done at …,

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

ANNEX I

In Annex I to Regulation (EU) No 910/2014, point (i) is replaced by the following:

‘(i) the information or the location of the services that can be used to enquire about the validity status of the qualified certificate;’.

ANNEX II

In Annex II to Regulation (EU) No 910/2014, points 3 and 4 are deleted.

ANNEX III

In Annex III to Regulation (EU) No 910/2014, point (i) is replaced by the following:

‘(i) the information or the location of the services that can be used to enquire about the validity status of the qualified certificate;’

ANNEX IV

Annex IV to Regulation (EU) No 910/2014 is amended as follows:

(1) point (c) is replaced by the following:

‘(c) for natural persons: at least the name of the person to whom the certificate has been issued, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;

(ca) for legal persons: a unique set of data unambiguously representing the legal person to whom the certificate is issued, with at least the name of the legal person to whom the certificate is issued and, where applicable, the registration number as stated in the official records;’;

(2) point (j) is replaced by the following:

‘(j) the information or the location of the certificate validity status services that can be used to enquire about the validity status of the qualified certificate.’.

ANNEX V

‘ANNEX V

REQUIREMENTS FOR QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES

Qualified electronic attestation of attributes shall contain:

(a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as a qualified electronic attestation of attributes;

(b) a set of data unambiguously representing the qualified trust service provider issuing the qualified electronic attestation of attributes including at least, the Member State in which that provider is established and:

(i) for a legal person: the name and, where applicable, registration number as stated in the official records,

(ii) for a natural person: the person’s name;

(c) a set of data unambiguously representing the entity to which the attested attributes refer; if a pseudonym is used, it shall be clearly indicated;

(d) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes;

(e) details of the beginning and end of the attestation's period of validity;

(f) the attestation identity code, which must be unique for the qualified trust service provider and, if applicable, the indication of the scheme of attestations that the attestation of attributes is part of;

(g) the qualified electronic signature or qualified electronic seal of the issuing qualified trust service provider;

(h) the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge;

(i) the information or location of the services that can be used to enquire about the validity status of the qualified attestation.'.

ANNEX VI

‘ANNEX VI

MINIMUM LIST OF ATTRIBUTES

Pursuant to Article 45e, Member States shall ensure that measures are taken to allow qualified trust service providers of electronic attestations of attributes to verify by electronic means at the request of the user, the authenticity of the following attributes against the relevant authentic source at national level or via designated intermediaries recognised at national level, in accordance with Union or national law and where these attributes rely on authentic sources within the public sector:

1. Address;

2. Age;

3. Gender;

4. Civil status;

5. Family composition;

6. Nationality or citizenship;

7. Educational qualifications, titles and licences;

8. Professional qualifications, titles and licences;

9. Powers and mandates to represent natural or legal persons

10. Public permits and licences;

11. For legal persons, financial and company data.’.

ANNEX VII

‘ANNEX VII

REQUIREMENTS FOR ELECTRONIC ATTESTATION OF ATTRIBUTES ISSUED BY OR ON BEHALF OF A PUBLIC BODY RESPONSIBLE FOR AN AUTHENTIC SOURCE

An electronic attestation of attributes issued by or on behalf of a public body responsible for an authentic source shall contain:

(a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as an electronic attestation of attributes issued by or on behalf of a public body responsible for an authentic source;

(b) a set of data unambiguously representing the public body issuing the electronic attestation of attributes, including at least, the Member State in which that public body is established and its name and, where applicable, its registration number as stated in the official records;

(c) a set of data unambiguously representing the entity to which the attested attributes refer; if a pseudonym is used, it shall be clearly indicated;

(d) the attested attribute or attributes, including, where applicable, the information necessary to identify the scope of those attributes;

(e) details of the beginning and end of the attestation's period of validity;

(f) the attestation identity code, which must be unique for the issuing public body and, if applicable, an indication of the scheme of attestations that the attestation of attributes is part of;

(g) the qualified electronic signature or qualified electronic seal of the issuing body;

(h) the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge;

(i) the information or location of the services that can be used to enquire about the validity status of the attestation.'.