

20.2.2024

A9-0038/ 001-001

AMENDMENTS 001-001

by the Committee on Industry, Research and Energy

Report

Romana Jerković

European Digital Identity Framework

A9-0038/2023

Proposal for a regulation (COM(2021)0281 – C9-0200/2021 – 2021/0136(COD))

Amendment 1

AMENDMENTS BY THE EUROPEAN PARLIAMENT*

to the Commission proposal

2021/0136 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

**amending Regulation (EU) No 910/2014 as regards establishing a framework for a
European Digital Identity**

* Amendments: new or amended text is highlighted in bold italics; deletions are indicated by the symbol **■**.

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 Committee¹,

Acting in accordance with the ordinary legislative procedure,

Whereas:

- (1) The Commission Communication of 19 February 2020, entitled “Shaping Europe’s Digital Future”² announces a revision of Regulation (EU) No 910/2014 of the European Parliament and of the Council with the aim of improving 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 2020³, 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.
- (2a) ***The Digital Decade Policy Programme 2030 sets the objective and digital target of a Union framework which, by 2030, leads to wide deployment of a trusted, voluntary, user-controlled digital identity, that will be recognised throughout the Union and allow each user to control their data and presence in online interactions.***
- (3a) ***The Commission Declaration of 26 January 2022 entitled "European Declaration on Digital Rights and Principles for the Digital Decade" underlines every citizen’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***

¹ OJ C , , p. .

² COM/2020/67 final

³ <https://www.consilium.europa.eu/en/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/>

Union are offered an accessible, secure and trusted digital identity that enables access to a broad range of online and offline services, protected against all cyberthreats, including identity theft or manipulation. The Commission Declaration also states that everyone has the right to the protection of their personal data online. That right encompasses the control on how the data is used and with whom it is shared.

- (3b) *Union citizens should have the right to a digital identity that is under their sole control and that enables them to exercise their rights as citizens in the digital environment and to participate in the digital economy. A European digital identity should be legally recognised throughout the Union.*
- (4) A more harmonised approach to digital 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 solutions*, and will strengthen the Single Market by allowing citizens, other residents as defined by national law and *legal entities* to identify *and authenticate* online *and offline in a safe, trustworthy, user friendly*, convenient, *accessible and harmonised way*, across the Union. Everyone should be able to securely access public and private services relying on an improved ecosystem for trust services and on verified proofs of identity and *electronic* attestations of attributes, such as *academic qualifications*, university *degrees or other educational or professional attainments* legally recognised and accepted everywhere in the Union, *or a license or a mandate to represent a company, while creating a uniform set of rules for providers of electronic attestations that ensures a level playing field*. The framework for a European Digital Identity aims 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 and public administrations should be able to rely on electronic documents *that are highly secured and accepted across the Union*. *With regard to electronic identification for public services with very high security identification requirements, it should be possible for Member States to enable notaries and other professionals entrusted with special powers in the public interest to rely on additional remote identity controls, set out in accordance with the principle of proportionality through national legislation.*

- (5) To support the competitiveness of European businesses, 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 they have been issued, thus benefiting from a harmonised European approach to trust, security and interoperability. Users and service providers alike should be able to benefit from the same legal value provided to electronic attestations of attributes across the Union.
- Harmonised digital identity framework has the potential to create economic value by providing easier access to goods and services, by significantly reducing operational costs linked to identification and authentication procedures, for example during the on-boarding of new customers, by reducing damages related to cybercrimes, such as identity theft, data theft and online fraud, and by promoting digital transformation of the Union's micro, small and medium-sized enterprises (SMEs).***
- (5a) ***A fully harmonised digital identity framework would contribute to the creation of a more digitally integrated Union, taking down the digital barriers between Member States and empower the Union citizens and Union residents to enjoy the benefits of digitalisation while increasing transparency and the protection of their rights.***
- (5b) ***In order to encourage the digitalisation of the Member States' public sector services and to ensure wide up-take of the European digital identity framework and the European Digital Identity Wallet (EDIW), this Regulation should support the use of the 'once only' principle in order to reduce administrative burden, to support cross-border mobility of citizens and businesses, and to foster development of interoperable e-government services across the Union. The cross-border application of the 'once only' principle should result in citizens and businesses not having to supply the same data to public authorities more than once, and that it should also be possible to use those data only at the request of the user for the purposes of completing cross-border online procedures. The implementation of this Regulation and of the 'once-only' principle should comply with all applicable data protection rules, including the principle of data minimisation, accuracy, storage limitation, integrity and confidentiality, necessity, proportionality and purpose limitation. The 'once-only' principle should be applied with the explicit consent of the user.***

- (6) *Natural and legal persons who own person identification data should be considered to be Digital Identity subjects. Regulations (EU) 2016/679¹ and (EU) 2018/1725² and Directive 2002/58/EC³ or the European Parliament and of the Council 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 from other services with the personal data relating to the services falling within the scope of this Regulation. **This Regulation further specifies the application of principles of purpose limitation, data minimisation, and data protection by design and by default to specific-use cases, without prejudice to Regulation (EU) 2016/679.***
- (6a) *EDIWs should have the function of a privacy management dashboard embedded into the design, in order to ensure a higher degree of transparency and control of the users over their data. This function should provide an easy, user-friendly interface with an overview of all relying parties with whom the user has shared data, including attributes, and the type of data shared with each relying party. It should allow the user to track all transactions executed through EDIWs, with at least the following data: the time and date of the transaction, the counterpart identification, the 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 to easily request to a relying party the immediate deletion of personal data pursuant Article 17 of Regulation (EU) 2016/679 and to easily report to the competent national authority where a relying party is established if an unlawful or inappropriate request of data is received without leaving the EDIW.*

¹ 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

² *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).*

³ *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 (OJ L 201, 31.7.2002, p. 37)*

- (6b) *Zero knowledge proof allows verification of a claim without revealing the data that proves it, based on cryptographic algorithms. The EDIW should allow for verification of claims inferred from personal data identification or attestation of attributes without having to provide the source data, to preserve the privacy of the user of the EDIW.*
- (7) It is necessary to set out the harmonised conditions for the establishment of a framework for *EDIWs* to be issued *directly by a Member State, under a mandate from a Member State or recognised by a Member State*, which should empower all Union citizens and *Union* residents as defined by national law to *securely request, receive, store, combine and selectively share* data related to their identity *and request deletion of their personal data in a user-friendly way and* under the sole control of the user. *All data should be stored by default on the user's device unless the user explicitly chooses otherwise. This Regulation should reflect shared values and uphold fundamental rights, strong ethical aspects, legal safeguards and liability, thus protecting democratic societies and citizens.* Technologies used to achieve those objectives should be developed aiming towards the highest level of *privacy and security, user convenience, accessibility, and wide usability and seamless interoperability*. Member States should ensure equal access to *and voluntary use of* digital identification to all their nationals and residents. *Member States should not, directly or indirectly, limit access to public services or public-funded services to natural or legal persons who decide not to use a EDIW and should develop and ensure free availability of alternative solutions for such individuals. Private relying parties using EDIWs to provide services should not deny those services or create disadvantageous conditions to consumers not using EDIWs to access their services.*
- (7a) *Where an EDIW is issued directly by a Member State, the competent authority concerned is directly responsible for the issuance and management of the EDIW, using its own resources. Where an EDIW is issued under a mandate from a Member State, the competent authority concerned has authorised a specific organisation to issue and manage the EDIW on its behalf on the basis of a public procurement procedure based on transparent, open and fair competition process in which all interested parties have the opportunity to participate and the best candidate is selected based on specific objective criteria and evaluation process. Where an EDIW is issued and managed independently but recognised by a Member State, the*

competent authority concerned has selected a specific organisation that has already developed an EDIW that complies with this Regulation. It is not necessary for the issuer and the manager of an EDIW to be the same entity.

- (8) In order to ensure compliance within Union law or national law compliant with Union law, *relying parties* should *register* their intent to rely on *EDIWs in the Member State where they are established*. That will allow Member States to protect users from fraud and prevent the unlawful use of identity data and electronic attestations of attributes as well as to ensure that the processing of sensitive data, like health data, can be verified by relying parties in accordance with Union **■** or national law. *The registration and approval processes should be cost-effective and proportional to the risk. The registration should include the data that the relying party intend to request, the intended use of and the reasons for the need of such data, per each different category of services provided by the relying party. Relying parties should provide reasons for their request complies with data minimisation principles.*
- (9) All *EDIWs* should *enable* users to electronically identify and authenticate online and offline across borders for accessing a wide range of public and private services. Without prejudice to Member States' prerogatives as regards the identification of their nationals and residents, *EDIWs* can also serve the institutional needs of public administrations, international organisations and the Union's institutions, bodies, offices and agencies. Offline use 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 level of assurance "high" *for identity proofing*, *EDIWs* should benefit from the potential offered by tamper-proof solutions such as secure elements, to comply with the security requirements under this Regulation. *When on-boarding into EDIWs, users should obtain the qualified electronic signature, free of charge and by default, without having to go through any additional administrative or technical procedures.* **■** To achieve simplification and cost reduction benefits to persons and businesses across the *Union*, including by enabling powers of representation and e-mandates, Member States should issue *EDIWs* relying on common standards *and technical specifications* to ensure seamless interoperability and *to adequately increase the IT security, strengthen robustness against cyber-attacks and thus significantly reduce the potential risks of ongoing digitalisation for*

citizens and businesses. Only Member States' competent authorities can provide a high degree 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 issuing of EDIWs* to rely on the legal identity of citizens, other residents or legal entities. *Reliance on the legal identity should not hinder the possibility of EIDW users to access services through the use of pseudonyms, where there is no legal requirement for legal identity for authentication* Trust in the *EDIWs* would be enhanced by the fact that 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 line with Regulation (EU) 2016/679.

- (9a) EDIWs should include a functionality to generate freely chosen and user managed pseudonyms, as a form of authentication to access online services provided, including services provided by very large online platforms as defined in Regulation (EU) 2022/2065 of the European Parliament and of the Council¹.*
- (9b) Member States should develop harmonised approaches to enable the technical possibility for persons with limited legal capacity, such as minors and for persons with no legal capacity, to use EDIWs, trust services and end-user products.*
- (9c) Natural and legal persons should be able to authorise EDIWs of third-parties to perform certain actions on their behalf, such as by means of powers of attorney or delegations of authority for specific transactions to specific employees or subcontractors in the case of a company or to parents acting on behalf of minor children.*
- (10) In order to achieve a high level of security and trustworthiness, this Regulation establishes the requirements for *EDIWs*. The conformity of *EDIWs* with those requirements should be certified by accredited public or private sector bodies designated by Member States. Relying on a certification scheme based on the availability of commonly agreed standards with Member States should ensure a high level of trust and interoperability. Certification should in particular rely on the relevant

¹ *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).*

European cybersecurity certifications schemes established pursuant to Regulation (EU) 2019/881⁶. Such certification should be without prejudice to certification as regards personal data processing pursuant to Regulation (EC) 2016/679

- (10a) *The transparency of EDIWs and the accountability of their issuers are key elements by which to create social trust in the framework. All issuers of EDIWs should make the source codes available to the public for its scrutiny, in particular for privacy and security. Issuers and managers of EDIWs should be subject to controls and liabilities similar to those of qualified trust services providers.***
- (11) *EDIWs should ensure the highest level of security for the personal data used for identification and authentication irrespective of whether such data is stored locally, in decentralised ledgers or on cloud-based solutions, and taking into account the different levels of risk. Using biometrics to identify and authenticate should not be a precondition for using EDIWs, notwithstanding the requirement for strong user authentication. Biometric data used for the purpose to authenticate a natural person in the context of this Regulation should not be stored in the cloud without the explicit consent of the user. Using biometrics is one of the identifications methods providing a high level of confidence, when used in combination with ‘what you know’ factor. Since biometrics represents a unique characteristic of a person, the use of biometrics should not be obligatory. Furthermore the use of biometric data should be limited to specific scenarios pursuant to Article 9 of Regulation (EU) 2016/679, and requires organisational and security measures, commensurate to the risk that such processing may entail to the rights and freedoms of natural persons and in accordance with Regulation 2016/679. Storing information from EDIWs in the cloud should be an optional feature only active after the user has given explicit consent. Where EDIWs are issued on a personal electronic device of the user, their cryptographic material should be, when technologically possible, stored in the secure elements of EDIWs.***
- (11a) *EDIWs should be secure-by-design. They should implement advanced security features to protect against identity theft, data theft, denial of service and any other***

⁶ 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

cyber threat. This should include state-of-the-art encryption and storage methods that are only accessible to and decryptable by the user, and establishing end-to-end encrypted communication with other EDIWs and relying parties. Additionally, EDIWs should require secure explicit, and active use confirmation for operations.

- (11b) *The use of EDIWs as well as the discontinuation of their use are rights and the choice of users. Member States should develop a simple, user-friendly, speedy and secure procedure for the users to request immediate revocation of validity of EDIWs. For the situations when users are in possession of the device, this functionality should be designed as an integrated feature of EDIWs. A user-friendly and speedy remote mechanism should be established for cases where users do not hold the device in their possession, such as in the case of theft or loss. 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 termination of EDIWs.*
- (11c) *In order to promote uptake of EDIWs and the wider use of digital identities, Member States should not only show the benefits of the relevant services, but 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, older persons and persons lacking digital skills.*
- (12) To ensure that the European digital identity framework is open to innovation, technological development and future-proof, Member States should be encouraged to **jointly** set-up ■ sandboxes to test innovative solutions in a controlled, **time limited** 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. This environment should foster the inclusion of European Small and Medium Enterprises, start-ups and individual innovators and researchers *as well as relevant industry stakeholders, while improving compliance and preventing the placing on the market of solutions which infringe Union law on data protection and IT security.*

- (13) Regulation (EU) 2019/1157 *of the European Parliament and of the Council*⁷ 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.
- (14) The process of notification of electronic identification schemes should be *improved* and accelerated to promote the 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 identity card schemes under Regulation (EU) No 910/2014.
- (15) 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 should foster Member States' cooperation on the security and interoperability of their notified electronic identification schemes.
- (16) Member States should benefit from new, flexible tools to ensure compliance with the requirements of this Regulation and of the relevant implementing acts. This Regulation should allow Member States to use reports and assessments performed by accredited conformity assessment bodies or voluntary ICT security certification schemes, such as 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 the requirements of the Regulation on the interoperability and the security of the notified electronic identification schemes.
- (17) Service providers use the identity data provided by the set of person identification data available from electronic identification schemes pursuant to Regulation (EU) No 910/2014 in order to match users from another Member State with the legal identity of that user. However, despite the use of the eIDAS data set, in many cases ensuring an accurate match requires additional information about the user and specific unique

⁷ 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).

identification procedures at national level. ***In order to ensure a high-level of trust and security of personal data of natural persons, different technical solutions should be considered, including the use or combination of various cryptographic techniques, such as cryptographically verifiable identifiers.*** To further support the usability of electronic identification means ***and implementation of ‘once-only’ principle,*** this Regulation should require Member States to take specific measures to ensure a correct identity match in the process of electronic identification ***exclusively for the cross-border access of public services that requires the identification of the user by law.*** ***In particular, this requirement should not be read as a call for a centralised identity register in the Union for natural persons and reliance would be placed on decentralised national registers.*** The use of ***person identification data or a combination of person identification data, including the use of*** unique and persistent identifiers issued by Member States or generated by EDIWs is important for ensuring that the identity of the user can be verified. National law should be able to require the use of unique and persistent identifiers that are specific to particular sectors or relying parties. EDIWs should be capable of storing those identifiers and disclosing them where requested by the user. For the same purpose, this Regulation should extend the mandatory minimum data set and require the use of a unique and persistent ***electronic identifier for legal persons in accordance with Union law.***

(17a) ***When accessing public and private services across borders, the authentication and identification of EDIW users should be possible. The receiving Member States should be able to unequivocally identify users, upon their request, in those cases where their identification is required by law and to proceed to identity matching. In order to ensure a high level of trust and security of personal data, different technical solutions should be considered, including the use or combination of various state-of-the-art cryptographic techniques and technologies, such as cryptographically verifiable identifiers, unique user-generated digital pseudonyms, self-sovereign identities, and domain-specific identifiers.***

(18) In accordance with Directive (EU) 2019/882 ***of the European Parliament and of the Council***⁸, persons with disabilities should be able to use ***EDIWs***, trust services and

⁸ 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).

end-user products used in the provision of those services on an equal basis with other users.

- (19) 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.
- (20) The provision and use of trust services are becoming increasingly important for international trade and cooperation. International partners of the EU are establishing trust frameworks inspired by Regulation (EU) No 910/2014. Therefore, in order to facilitate the recognition of such services and their providers, implementing legislation may set the conditions under which trust frameworks of third countries could be considered equivalent to the trust framework for qualified trust services and providers in this Regulation, as a complement to the possibility of the mutual recognition of trust services and providers established in the Union and in third countries in accordance with Article 218 of the Treaty.
- (21) *Issuers of EDIWs may need access to specific hardware and software features of smartphones, such as parts of the operating system, secure hardware (secure element, SIM etc.), NFC, Bluetooth, Wi-Fi Aware and biometric sensors. Such features are under the control of operating system and equipment manufacturers. Therefore this Regulation should build on Union acts ensuring contestable and fair markets in the digital sector. In particular, it builds on Article 6(7) of the Regulation (EU) 2022/1925 of the European Parliament and of the Council¹, which requires the providers of core platform services designated as gatekeepers to allow business users and alternative providers of services provided together with, or in support of, core platform services, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware or software features, regardless of whether those features are part of the operating system or are available to or used by that gatekeeper when providing such services.*

¹ *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).*

- (21a) *This Regulation aims to facilitate the creation of, the choice between and the possibility of switching between EDIWs. In order to avoid lock-in effects, the issuers of EDIWs should, at the request of EDIW users, ensure the effective portability of data, including continuous and real-time access to services, and should not be allowed to use contractual, economic or technical barriers to prevent or to discourage effective switching between different EDIWs.***
- (22) In order to streamline the cybersecurity obligations imposed on trust service providers, as well as to enable these providers and their respective competent authorities to benefit from the legal framework established by Directive XXXX/XXXX (NIS2 Directive), trust services are required to take appropriate technical and organisational measures pursuant to Directive XXXX/XXXX (NIS2 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 Directive XXXX/XXXX (NIS2 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 damages or incidents occurred in the context of identification of persons. The cybersecurity risk management requirements and reporting obligations under Directive XXXXXX [NIS2] should be considered 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 XXXX/XXXX (NIS2 Directive). Any requirements pursuant to this Regulation do not affect the obligation to notify personal data breaches under Regulation (EU) 2016/679.
- (23) Due consideration should be given to ensure effective cooperation between the NIS and eIDAS authorities. In cases where the supervisory body under this Regulation is different from the competent authorities designated under Directive XXXX/XXXX [NIS2], those authorities 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 this Regulation and Directive XXXX/XXXX [NIS2]. In particular, the supervisory bodies under this Regulation should be entitled to request the competent authority under Directive XXXXX/XXXX [NIS2] to provide the 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 NIS 2 or require them to remedy non-compliance.

- (24) 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 pan-European electronic registered delivery services and ensure that the identification of the recipients is ensured with a higher level of confidence than the identification of the sender.



- (26) It should be possible to issue and handle trustworthy digital attributes and contribute to reducing administrative burden, empowering citizens and other residents to use them in their private and public transactions. Citizens and other residents should be able, for instance, to demonstrate ownership of a valid driving license 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.
- (27) Any entity that collects, creates and issues attested attributes such as diplomas, licences, certificates of birth should be able to become a provider of electronic attestation of attributes ***and should be responsible for revoking the attestation in the event of falsification, identity theft, or any issuance based on an abusive request.*** Relying parties should use the electronic attestations of attributes as equivalent to attestations in paper format. ***Nevertheless, lawfully issued attestations of attributes in paper form should continue to be accepted by relying parties as an alternative to electronic attestations of attributes.*** An electronic attestation of attributes should not be denied legal effect ***solely*** 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. To that effect, 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. ***The Commission and the Member States should involve professional organisations in laying down the attributes that concern them.***

- (28) ***The wide availability and usability of EDIWs require their acceptance and trust by both private individuals and private service providers. Private relying parties providing services such as 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 EDIWs for the provision of services where strong user authentication for online identification is required by Union or national law. Information requested from the user via the EDIW should be necessary and proportionate for the intended use case of the relying party and should be in line with the principle of data minimisation, ensuring transparency over which data is shared and for what purposes.*** Where very large online platforms as defined in Article 25.1. of Regulation (EU) 2022/2065 require users to authenticate to access online services, those platforms should be mandated to accept the use of EDIWs upon *the* voluntary request of the user. Users should be under no obligation to use EDIWs to access private services ***and should not be restricted or hindered on the grounds that they do not use an EDIW***, but if users wish to do so, *very* large online platforms should accept EDIWs for this 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 this is necessary to increase the protection of users from fraud and secure a high level of data protection. Self-regulatory codes of conduct at Union level ('codes of conduct') should be developed in order to contribute to wide availability and usability of electronic identification means including EDIWs within the scope of this Regulation. The codes of conduct should facilitate wide acceptance of electronic identification means including EDIWs by those service providers which do not qualify as very large platforms and which rely on third party electronic identification services for user authentication. They should be developed within 12 months of the adoption of this Regulation. ■

- (29) ***EDIWs*** should technically enable the selective disclosure of attributes to relying parties ***in a secure and user-friendly manner as one of its key features and advantages. They should also ensure that no attributes are disclosed to parties that are not registered to receive such attributes.*** This feature should become a basic design feature thereby reinforcing convenience and personal data protection including minimisation of processing of personal data ***in particular privacy by design and by default. Mechanisms for the validation of EDIWs, the selective disclosure and authentication of users to access online services should be privacy-preserving thereby preventing the tracking of the user and respecting the principle of purpose limitation, which implies a right to pseudonymity to ensure the user cannot be linked across several relying parties. The technical architecture and implementation of EDIWs should be in full compliance with Regulation (EU) 2016/679. In addition, the decentralised nature of EDIWs should enable self-signing and revocability of attributes and identifiers.***
- (29a) ***Unless specific rules of Union or national law require users to identify themselves, the use of services under a pseudonym should be allowed and should not be restricted by Member States, for example by imposing a general obligation on service providers to limit the pseudonymous use of their services.***
- (30) Attributes provided by the qualified trust service providers as part of the qualified attestation of attributes should be verified against the authentic sources either directly by the qualified trust service provider or via 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.
- (31) Secure electronic identification and the provision of attestation of attributes should offer additional flexibility and solutions for the financial services sector to allow identification of customers and the exchange of specific attributes necessary to comply with, for example, customer due diligence requirements under the Anti Money Laundering Regulation, [reference to be added after the adoption of the proposal], with suitability requirements stemming from investor protection legislation, or to support the fulfilment of strong customer authentication requirements for account login and ***for*** initiation of transactions in the field of payment services.

- (31a) *This Regulation should establish the principle that the legal effect of an electronic signature cannot 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 define 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 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 judicial value of a document to be signed and 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. The use of qualified electronic signatures should be mandated only when the highest level of security and confidence is required.*
- (32) Website authentication services provide users with *a high level of assurance of the identity of the* entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated. The use of website authentication services by websites is voluntary. However, in order for website authentication to become a means to increasing trust, providing a better experience for the user and furthering growth in the internal market, this Regulation lays down minimal security and liability obligations for the providers of website authentication services and their services. To that end, web-browsers should ensure support and interoperability with *qualified* certificates for website authentication pursuant to Regulation (EU) No 910/2014. They should recognise and display *qualified* certificates for website authentication to provide a high level of assurance, allowing website owners to assert their identity as owners of a website and users to identify the website owners with a high degree of certainty. To further promote their usage, public authorities in Member States should consider incorporating *qualified* certificates for website authentication in their websites. *In the case of a security breach, web browsers should be able to take measures that are proportional to their risk. Web browsers should notify the*

Commission immediately of any security breach as well as the measures taken to remedy such breaches with regard to a single certificate or to a set of certificates.

- (33) Many Member States have introduced national requirements for services providing secure and trustworthy digital archiving in order to allow for the long term preservation of electronic documents and associated trust services. To ensure legal certainty and trust, it is essential to provide a legal framework to facilitate the cross border recognition of qualified electronic archiving services. That framework could also open new market opportunities for Union trust service providers.

■

- (36) In order to avoid fragmentation and barriers, due to diverging standards and technical restrictions, and to ensure a coordinated process to avoid endangering the implementation of the future European digital identity framework, a process for close and structured cooperation between the Commission, Member States, *civil society, academics* and the private sector is needed. To achieve this objective, Member States should cooperate. *The 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 aspects of the functionalities and interoperability of the *EDIWs* including eSignatures and of the qualified trust service *providers* for attestation of attributes as laid out in this regulation. In this context, Member States should also reach agreement on common elements of a business model and fee structure of *EDIWs*, to facilitate take up, in particular by *SMEs* in a cross-border context. ■

- (36a) *In order to ensure wide usability and availability, additional financial support measures should be envisaged to support Member States in issuing and managing EDIWs. To that end, the Commission should assess the availability of additional Union funds to be made available for the Member States that would request support in the development, deployment and management of EDIWs.*

- (36b) *In order to ensure a wider use and applicability of EDIWs across the Union, the Commission should build on and leverage the framework of this Regulation when developing sectoral Union instruments, such as the European Social Security Pass and the common European data spaces. The coordination with the European Social*

Security Pass should enable the digital portability of citizens' social security rights across borders and the verification of their entitlements and validity of documents. For the common European data space, EDIWs should enable a higher degree of transparency and control of the users over their data.

(37) The European Data Protection Supervisor has been consulted pursuant to Article 42(1) of Regulation (EU) 2018/1525 of the European Parliament and of the Council¹².

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

HAVE ADOPTED THIS REGULATION:

Article 1

Regulation (EU) 910/2014 is amended as follows:

(1) Article 1 is replaced by the following:

‘This **Regulation** aims **to contribute towards** ensuring the proper functioning of the internal market ■ providing an adequate level of security of electronic identification means and trust services **used across the Union**. For these purposes, this Regulation:

- (a) lays down the conditions under which Member States shall provide and recognise electronic identification means of natural and legal persons, falling under a notified electronic identification scheme of another Member State;
- (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, **non-qualified electronic delivery services, qualified** electronic registered delivery services, certificate services for website authentication, ■ electronic attestation of attributes **and** the management of remote electronic signature and seal creation devices ■ ;

¹² 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).

(d) lays down the conditions for the issuing, *managing and recognition of* European Digital Identity Wallets by Member States *and for ensuring their interoperability and their cross-border use in the Union;*

(da) enables the exercise of the right to safely participate in the digital society and facilitates unrestricted access to online public services throughout the Union for any natural or legal person.’;

(2) Article 2 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. This Regulation applies to electronic identification schemes that have been notified by a Member State, European Digital Identity Wallets issued *and managed* by Member States and to trust service providers that are established in the Union.’;

(b) paragraph 3 is replaced by the following:

‘3. This Regulation does not affect *Union or* national **■** law related to **■** :

(a) the conclusion and validity of contracts, or other legal or procedural obligations relating to form; or

(b) sector-specific requirements for qualified electronic attestation of attributes as regards form with underlying legal effects, in particular in the context of the cross-border recognition of qualified electronic attestation of attributes.’;

(3) Article 3 is amended as follows:

(a) *points (2) to (6) are* replaced by the following:

‘(2) ‘electronic identification means’ means a material and/or immaterial unit, including European Digital Identity Wallets or ID cards following Regulation 2019/1157, containing person identification data and which is used for authentication for an online or offline service;

(3) ‘person identification data’ means a set of data, *issued in accordance with national law*, enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;

- (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 legal *or natural* persons;
- (4a) ‘user’ means a natural or legal person, or a natural person representing a legal person using trust services, notified electronic identification means or European Digital Identity Wallets;*
- (5) ‘authentication’ means an electronic process that enables the *verification* of the origin and integrity of data in electronic form ■ ;
- (5a) ‘identification’ means an electronic process that establish an unequivocal relationship between a set of data and a natural or legal person;**(5b) ‘validation’ means the process of verifying that an electronic signature, an electronic seal, a European Digital Identity Wallet, an electronic identification mean, a relying party authorisation, person identification data, an electronic attestation of attributes or any electronic certificates for trust services is valid and has not been revoked;*
- (5c) ‘zero knowledge proof’ means cryptographic methods by which a relying party can validate that a given statement based on the electronic attestation of attributes held in a user’s European Digital Identity Wallet is true, without conveying any data related to those electronic attestation of attributes to the relying party;*
- (6) ‘relying party’ means a natural or legal person that relies upon an electronic identification *means, including European Digital Identity Wallets*, or a trust service, *directly or through an intermediary, in order to provide services;*”;
- (c) point (14) is replaced by the following:
- ‘(14) ‘certificate for electronic signature’ means an electronic attestation ■ which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;’;
- (d) point (16) is replaced by the following:

‘(16) ‘trust service’ means an electronic service normally provided against payment which consists of:

- (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services, electronic attestation of attributes and certificates related to those services;
- (b) the creation, verification and validation of certificates for website authentication;
- (c) the preservation of electronic signatures, seals or certificates related to those services;
- (d) the electronic archiving of electronic documents;
- (e) the management of remote electronic signature and seal creation devices;

■’;

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

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

(f) the following points ■ are inserted:

‘(23a) ‘remote qualified signature creation device’ means a qualified electronic signature creation device where a qualified trust service provider generates, manages or duplicates the electronic signature creation data on behalf of a signatory;

(23b) ‘remote qualified seal creation device’ means a qualified electronic seal creation device where a qualified trust service provider generates, manages or duplicates the electronic signature creation data on behalf of a seal creator;’;

(g) point (29) is replaced by the following:

‘(29) ‘certificate for electronic seal’ means an electronic attestation or set of attestations that links electronic seal validation data to a legal person and confirms the name of that person;’;

(ga) points (38) and (39) are 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;

(39) ‘qualified certificate for website authentication’ means a certificate for website authentication **that links the website to the natural or legal person to whom the certificate is issued with a high level of assurance**, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;”

■ ’

(i) the following points ■ are added:

‘(42) ‘European Digital Identity Wallet’ **means an electronic identification means which securely stores, manages and validates** identity data **and electronic attestations of attributes**, to provide them to relying parties **and other users of European Digital Identity Wallets on request, and which enables the creation of** qualified electronic signatures and seals;

(43) ‘attribute’ is a feature, characteristic or quality of a natural or legal person or of an entity ■ ;

(44) ‘electronic attestation of attributes’ means an attestation in electronic form that allows the **presentation and** authentication of attributes;

(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) ‘authentic source’ is a repository or system, held under the responsibility of a public sector body or private entity, that contains attributes about a natural or legal person and is considered to be the primary source of that information or recognised as authentic in **Union or** national law;

- (47) ‘electronic archiving’ means a service ensuring *preservation* of electronic data or documents in order to guarantee their integrity, the accuracy of their origin and legal features throughout the conservation period;
- (48) ‘qualified electronic archiving service’ means a service that meets the requirements laid down in Article 45g;
- (49) ‘EU Digital Identity Wallet Trust Mark’ means an indication in a simple, recognisable and clear manner that a Digital Identity Wallet has been issued in accordance with this Regulation;
- (50) ‘strong user authentication’ means an authentication based on the use of *at least two authentication factors* categorised as user knowledge , possession and inherence that are independent, in such a way that the breach of one does not compromise the reliability of the others, and is designed in such a way to protect the confidentiality of the authentication data;
- (51) ‘user account’ means a mechanism that allows a user to access public or private services on the terms and conditions established by the service provider;



- (54) ‘personal data’ means any information as defined in point 1 of Article 4 of Regulation (EU) 2016/679;
- (55) ‘*identity matching*’ means a process where person identification data or person identification means are matched with or linked to an existing account belonging to the same person;
- (55a) ‘offline service’ means the capability of a user to electronically identify and authenticate with a third party with close proximity technologies irrespective of whether the device is connected to the internet or not in order to access a wide range of public and private services.”;*

- (4) Article 5 is replaced by the following:

‘Article 5

Protection of personal data, and use of pseudonyms in electronic transaction

1. *The processing of personal data shall be carried out in accordance with Regulations (EU) 2016/679 and (EU) 2018/1725 and, where relevant, Directive 2002/58/EC, by implementing the principles of data minimisation, purpose limitation, and data protection by design and by default, in particular with respect to the technical measures for the implementation of this Regulation and the interoperability framework in accordance with Article 12 thereof.*
2. Without prejudice to the legal effect given to pseudonyms under national law *and unless specific rules of the Union or national law require users to identify themselves for legal purposes*, the use of pseudonyms in electronic transactions, *freely chosen by the user*, shall *always be allowed and shall not be prohibited or restricted by means of a contract or the terms and conditions applicable to the use of the service.*
3. *Unless specific rules of the Union or national law require users to identify themselves for legal purposes, relying parties shall make reasonable efforts to enable the use of their services without electronic identification or authentication.*’;

(5) in Chapter II the heading is replaced by the following:

‘SECTION I

ELECTRONIC IDENTIFICATION;’

(6) Article 6 is deleted;

(7) the following Articles ■ are inserted:

‘Article 6a

European Digital Identity Wallets

1. For the purpose of ensuring that all natural and legal persons in the Union have secure, *reliable*, trusted and seamless access to cross-border public and private services, *while having full control over their data*, each Member State shall issue *at least one* European Digital Identity Wallet *by ... [18 months after the date of entry into force of this amending Regulation]*.

2. European Digital Identity Wallets shall be issued *and managed in any of the following ways*:
 - (a) *directly* by a Member State;
 - (b) under a mandate from a Member State;
 - (c) independently *from a Member State* but recognised by *that* Member State.
- 2a. *The source code used for providing European Digital Identity Wallets shall be open source and shall be published for auditing and review.*
3. European Digital Identity Wallets shall, *in a user-friendly manner*, enable the user to:
 - (a) securely request and obtain, store, select, combine and share, in a manner that is transparent to, traceable by *and under the sole control of* the user, the necessary █ identification data *to identify and authenticate the user* online and offline in order to use online public and private services;
 - (aa) *securely store, select, combine and share electronic attestation of attributes*;
 - (ab) *securely issue and revoke electronic attestation of attributes issued directly by the user*;
 - (ac) *generate pseudonyms and store them encrypted and locally within it*;
 - (ad) *securely authenticate a third person's European Digital Identity Wallets or a connecting relying party, and receive and authenticate in a transparent and traceable manner the third party identity data and electronic attestation of attributes online and offline*;
 - (ae) *access a data base 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 whom the user has established a connection and where applicable all data shared*;
 - (ii) *easily request to a relying party the deletion of personal data pursuant to Article 17 of the Regulation (EU) 2016/679*;

- (iii) *easily report to the competent national authority where a relying party is established if an unlawful or inappropriate request of data is received without leaving the European Digital Identity Wallet;*
 - (iv) *revoke any electronic attestation of attribute issued by the user;*
 - (b) sign by means of qualified electronic signatures;
 - (ba) *download all users' data, electronic attestation of attributes and configurations;*
 - (bb) *exercise users' rights of data portability by switching to another European Digital Identity Wallet belonging to the same user.*
- 4. **European Digital Identity Wallets** shall, in particular:
 - (a) provide **■** *common protocols and interfaces:*
 - (i) *to securely interact with the electronic identification means associated pursuant to Article 7(2), for the purpose of identifying and authenticating the user;*
 - (ii) *for issuers of electronic attestation of attributes to issue electronic attestation of attributes into the user's European Digital Identity Wallet;*
 - (iii) *to establish unique, private and secure peer-to-peer connections between two European Digital Identity Wallets or between an European Digital Identity Wallet and a relying party;*
 - (iv) *for users of European Digital Identity Wallets and relying parties to request, receive, select, send, authenticate and validate electronic attestations of attributes, person identification data, the identification of relying parties, electronic signatures and electronic seals;*
 - (v) *for users of European Digital Identity Wallets and relying parties to authenticate and validate the European Digital Identity Wallet and approved relying parties;*

- (vi) for users of European Digital Identity Wallets or relying parties, when available, to perform a zero knowledge proof inferred from person identification data or electronic attestation of attributes;*
- (vii) for users of European Digital Identity Wallets to transfer and request reissuance of their own electronic attestation of attributes and configurations to another European Digital Identity Wallet belonging to the same user or a device controlled by the same user;*
- (b) ensure that **■** providers of qualified *and non-qualified electronic* attestations of attributes *are technologically prevented from receiving* any information about the use of these attributes;
- (c) meet the requirements set out in Article 8 with regards to assurance level “high”, in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication;
- (ca) in the case of electronic attestation of attributes with embedded disclosure policies, provide a mechanism to ensure that only the relying party or the user of European Digital Identity Wallets having the necessary electronic attestation of attribute has permission to access it;*
- (cb) provide a mechanism to record digital requests received and digital transactions in a cryptographic manner that ensures that it is not possible to repudiate their authenticity;*
- (cc) provide a mechanism to inform users, without delay, of any security breach that may have entirely or partially compromised their European Digital Identity Wallet or its content and in particular if their European Digital Identity Wallet has been suspended or revoked pursuant to Article 10a.*
-
- (e) ensure that the person identification data referred to in *Article 12(4)*, point (d), *representing* the natural or legal person is associated with it.

- (ea) provide a mechanism allowing the user of the European Digital Identity Wallet to act on behalf of another natural or legal person;*
 - (eb) display an "EU Digital Identity Wallet Trust Mark" for the recognition of qualified electronic attestation of attributes;*
 - (ec) offer qualified electronic signatures to all users by default and free of charge.;*
5. Member States shall provide *free of charge validation mechanisms to:*
- (a) ensure that the authenticity and validity of European Digital Identity Wallets can be verified;*
 - (b) allow relying parties and users of European Digital Identity Wallets to verify that the electronic attestations of attributes are authentic and valid;*
 - (c) allow relying parties, users of European Digital Identity Wallets and qualified trust service providers to verify the authenticity and validity of attributed person identification data;*
- (ca) allow European Digital Identity Wallet users to verify the authenticity and validity of the identity of relying parties approved in accordance with Article 6b(1).*
- 5a. *Member States shall provide means to revoke the validity of the European Digital Identity Wallet:*
- (a) upon the explicit request of the user;*
 - (b) when its security has been compromised;*
 - (c) upon the death of the user or cease of activity of the legal person.*
- 5b. *Member States shall raise awareness about the benefits and risks of the European Digital Identity Wallet by means of communication campaigns. They shall ensure that their citizens are well-trained in its use.*
- 5c. *Issuers 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 provision of services of the European Digital Identity Wallet.*

6. **█** European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance ‘high’. **█**
- 6a. *European Digital Identity Wallets shall ensure security-by-design. European Digital Identity Wallets shall provide the necessary state-of-the-art security functionalities, such as mechanisms to encrypt and store data in a way that is only accessible to and decryptable by the user and establish end-to-end encrypted exchanges with relying parties and other European Digital Identity Wallets. They shall offer resistance to skilled attackers, ensure the confidentiality, integrity and availability of their content, including person identification data and electronic attestation of attributes and request the secure, explicit and active user’s confirmation of its operation.*
- 6b. *The issuance and use of the European Digital Identity Wallets shall be free of charge to all natural and legal persons.*
7. *The technical framework for the European Digital Identity Wallet shall be subject to the following principles:*
- (a) *the user shall be in full control of the European Digital Identity Wallet and the user’s data, including self-certification;*
 - (b) *the European Digital Identity Wallet shall use decentralised elements for the identity architecture;*
 - (c) *the set of electronic identification means, attributes and certificates contained in a European Digital Identity Wallet shall be stored securely and exclusively on devices controlled by the user, unless the user freely consents to storage on third-party devices or to a cloud based option;*
 - (e) *the European Digital Identity Wallet shall allow secure connections between the user and the relying parties;*
 - (f) *the technical architecture of the European Digital Identity Wallet shall prevent the issuer of **█** European Digital Identity Wallets, Member State or any other parties from collecting or obtaining electronic identification means, attributes, electronic documents contained in a European Digital Identity Wallet and information about the use of the European Digital Identity Wallet by the user, except where requested by*

the user using devices in the user's control and the exchange of information via the European Digital Identity Wallet shall not allow providers of electronic attestations of attributes to track, link, correlate or otherwise obtain knowledge of transactions or user behaviour;

- (g) unique and persistent identifiers shall not be accessible to relying parties in cases other than when identification of the user is required by Union or national law;*
- (h) Member States shall ensure that relevant information on the European Digital Identity Wallet is publicly available;*
- (i) personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held;*
- (j) if the European Digital Identity Wallet is provided by private parties in accordance to paragraph 1 (b) and (c), the provisions of **Article 45f(4)** shall apply mutatis mutandis;*
- (k) where attestation of attributes does not require the identification of the user, zero knowledge proof shall be performed;*
- (l) the issuer of the European Digital Identity Wallet shall be the controller for the purposes of Regulation (EU) 2016/679 regarding the processing of personal data in the European Digital Identity Wallet;*
- (m) the European Digital Identity Wallet shall provide a complaint mechanism to enable users to inform the supervisory body under this Regulation and the supervisory authorities established under Regulation (EU) 2016/679 directly where a relying party requests a disproportionate amount of data which is not in line with the registered intended use of that data.*

7a. The use of the European Digital Identity Wallet shall be voluntary. Access to public and private services, access to labour market and freedom to conduct business shall not in any way be restricted or made disadvantageous for natural or legal persons not using European Digital Identity Wallets. It shall

remain possible to access public and private services by other existing identification and authentication means.

9. Article 24(2), points (b), *(d), (e), (f), (fa), (fb)*, (g), and (h) shall apply mutatis mutandis to Member States *directly* issuing *and managing* the European Digital Identity Wallets.
10. The European Digital Identity Wallet shall be made accessible for persons with disabilities in accordance with the accessibility requirements of Annex I to Directive *(EU) 2019/882 and the United Nations Convention on the Rights of Persons with Disabilities¹*, as well as to persons with special needs, including older people and persons with limited access to digital technologies or with insufficient digital literacy.
11. *By ... [6 months after the date of entry into force of this amending Regulation]*, the Commission shall reference standards for the requirements referred to in *this Article* by means of an implementing act on the implementation of the European Digital Identity Wallet. *That* implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).
- 11a. By ... [6 months after the date of entry into force of this amending Regulation], the Commission shall adopt a delegated act in accordance with Article 47 supplementing this Regulation by establishing technical and operational specifications for the requirements referred to in this Article.*
- Article 6b
- European Digital Identity Wallets Relying Parties
1. Where *a* relying party *intends* to rely upon European Digital Identity Wallets *for the provision of public or private services* it shall *register in* to the Member State where the relying party is established. *The relying party's registration shall include information about the data that it intends to request*

¹ *Approved by Council Decision 2010/48/EC of 26 November 2009 concerning the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities (OJ L 23, 27.1.2010, p. 35).*

with regard to each different service provided, the intended use of the data requested and the reasons for the request. The relying party shall notify the Member State about any change to the information notified with undue delay.

- 1a. Relying parties that intend to process special categories of personal data, such as health or biometric data as referred to in Article 9 of the Regulation (EU) 2016/679 shall require prior approval from the competent authorities in the Member State in which they intend to provide their services. Relying parties that are granted the approval shall ensure that processing of personal information is carried out in accordance with Article 6(1) of the Regulation (EU) 2016/679.*
- 1b. Paragraphs 1 and 1a shall be without prejudice to ex-ante approval requirements set out in Union law or national law for the provision of specific services.*
- 1c. Member States shall make the information referred to in paragraph 1 publicly available online, together with the identity of each relying party and their contact details.*
- 1d. Member States shall establish ex-post controls to verify that data requests are proportionate and commensurate with the declared intent and that the principle of data minimisation is respected.*
- 1e. The European Digital Identity Framework Board established pursuant to Article 46c or any Member State shall revoke the authorisation of relying parties in the case of illegal or fraudulent use of the European Digital Identity Wallet, or suspend such authorisation until identified irregularities have been remedied.*
- 2. Member States shall implement a common mechanism for the **identification and authentication** of relying parties **and the verification of the notified data sets referred in Article 6a(4), points (ca) and (cb).***
 - 2a. Where relying parties intend to rely upon European Digital Identity Wallets issued in accordance with this Regulation, they shall authenticate and identify themselves to the user of the European Digital Identity Wallet, before any other form of transaction can take place.*

3. Relying parties shall be responsible for carrying out the procedure for authenticating **and validating** person identification data and electronic attestation of attributes originating from European Digital Identity Wallets.
Relying parties shall accept the use of pseudonyms, unless the identification of the user is required by Union or national law.
- 3a. ***Intermediaries acting on behalf of relying parties are to be considered relying parties and shall not obtain data about the content of the transaction.***
4. ***By ...[6 months after the date of entry into force of this amending Regulation], the Commission shall adopt delegated acts in accordance with Article 47, supplementing this Regulation by establishing technical and operational specifications for the requirements referred to in this Article, in accordance with Article 6a(11a).***

Article 6c

Certification of the European Digital Identity Wallets

1. European Digital Identity Wallets that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and the references of which have been published in the Official Journal of the European Union shall be presumed to be compliant with the cybersecurity relevant requirements set out in Article 6a ***of this Regulation*** in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements. ***When relevant European cybersecurity certification schemes are available, the European Digital Identity Wallet, or parts thereof, shall be certified in accordance with such schemes.***
2. Compliance with the requirements set out in **■ Article 6a(3), (4) and (5)** related to the personal data processing operations carried out by the issuer of the European Digital Identity Wallets shall be certified pursuant to Regulation (EU) 2016/679.
 - 2a. ***Where relevant European functionality and interoperability certification schemes are available, the European Digital Identity Wallet, or parts thereof, shall be certified in accordance with such schemes. Those certification schemes shall provide a presumption of conformity to the functionality and***

interoperability requirements set out in Article 6a. In the absence of certification schemes for functionality and interoperability, the standards referred to in Article 6a(11) shall apply.

3. The conformity of European Digital Identity Wallets with the requirements laid down in Article 6a *of this Regulation* shall be certified by *conformity assessment bodies in accordance with Article 60 of Regulation (EU) 2019/881 for cybersecurity requirements and by certification bodies in accordance with Article 43 of Regulation (EU) 2016/679 for personal data processing operations.*
- 3a. *For the purposes of this Article, European Digital Identity Wallets shall not be subject to the requirements referred to in Articles 7 and 9.*
4. *By ... [6 months after the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of standards, technical specifications, procedures and available Union and national cybersecurity certification schemes pursuant to Regulation (EU) 2019/881 necessary for the certification of the European Digital Identity Wallets referred to in paragraphs 2a and 3 of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2) of this Regulation.*
5. Member States shall communicate to the Commission the names and addresses of the *conformity assessment bodies and certification* bodies referred to in paragraph 3. The Commission shall make that information available to *all* Member States.
6. The Commission shall be empowered to adopt delegated acts in accordance with Article 47, *supplementing this Regulation by establishing the* specific criteria ■ referred to in paragraph 3 *of this Article.*

Article 6d

Publication of a list of certified European Digital Identity Wallets

1. Member States shall inform the Commission without undue delay of the European Digital Identity Wallets that have been issued pursuant to Article 6a and certified by the bodies referred to in Article 6c(3). They shall also inform

the Commission, without undue delay, ***in the event that*** certification is cancelled ***and the reasons for such cancellation***.

2. On the basis of the information received, the Commission shall establish, publish and maintain ***an up-to-date, machine readable*** list of certified European Digital Identity Wallets.
3. ***By ... [6 months after the date of entry into force of this amending Regulation]***, the Commission shall define formats and procedures applicable for the purposes of paragraph 1 ***of this Article*** by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(11). ***That implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).***’;

(8) the following heading is inserted before Article 7:

‘SECTION II

ELECTRONIC IDENTIFICATION SCHEMES;’;

(9) the introductory sentence of Article 7 is replaced by the following:

‘Pursuant to Article 9(1) Member States shall notify, ***by ... [12 months after the entry into force of this Regulation]*** at least one electronic identification scheme including at least one ***electronic*** identification means ***with assurance level 'high' meeting all the following conditions:***’;

(10) 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 of this Article and the basic information thereon.
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 from the date of receipt of that notification.’;

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

"Security breach of electronic identification schemes for cross-border authentication";

(11) the following Article ■ is inserted:

‘Article 10a

Security breach of the European Digital Identity Wallets

1. Where European Digital **Identity** Wallets issued pursuant to Article 6a and the validation mechanisms referred to in Article 6a(5) points (a), (b) and (c) are breached or partly compromised in a manner that affects their reliability or the **confidentiality, integrity or availability of user data, or the** reliability of the other European Digital Identity Wallets, the issuing Member State shall, without delay, suspend the issuance and revoke the validity of the European Digital Identity Wallet and inform **the affected users, the single point of contact designated pursuant to Article 46a, the relying parties**, the other Member States and the Commission accordingly.
 - 1a. **After notification of the security breach of the European Digital Identity Wallet, the single point of contact designated pursuant to Article 46a shall liaise with the relevant national competent authorities and, where necessary, with the European Digital Identity Framework Board established pursuant to Article 46c, the European Data Protection Board, the Commission and ENISA.**
2. Where the breach or compromise referred to in paragraph 1 is remedied, the issuing Member State shall re-establish the issuance and the use of the European Digital Identity Wallet and inform **the national competent authorities of the** other Member States, **the affected users and relying parties, the single point of contact designated pursuant to Article 46a** and the Commission without undue delay.
3. If **no attempt or insufficient progress is made to remedy** the breach or compromise referred to in paragraph 1 ■ within three months of the suspension or revocation, the Member State concerned shall withdraw the European Digital **Identity** Wallet concerned and inform **the affected users, the single point of contact designated pursuant to Article 46a, the relying parties** the other Member States and the Commission on the withdrawal accordingly. Where it is justified by the severity of the breach, the European Digital Identity

Wallet concerned shall be withdrawn without delay *and the relevant decision should be reasoned and communicated to the Commission.*

4. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 6d without undue delay.
5. *By ... [6 months after the date of entry into force of this amending Regulation], the Commission shall adopt a delegated act in accordance with Article 47, supplementing this Regulation by further specifying the measures referred to in paragraphs 1 and 3 of this Article.* ’;

(12) the following Article ■ is inserted:

‘Article 11a

Cross-border user identification

1. When *accessing cross-border public services that requires identification of the user by Union or national law, Member States shall ensure unequivocal identity matching for natural persons using notified electronic identification means or European Digital Identity Wallets. Member States shall provide for technical and organisational measures to ensure the protection of personal data and prevent profiling of users.*
2. *In order to identify natural persons upon their request for accessing services as described in paragraph 1, Member States shall provide a minimum set of person identification data referred to in Article 12.4.(d). Member States that have at least one unique identifier shall, at the request of the user, issue unique and persistent identifiers for cross-border use. Those identifiers may be specific to particular sectors or relying parties, provided that they uniquely identify the user across the Union.*
 - 2a. *Member States shall provide a single unique and persistent identifier for legal persons using electronic identification means or European Digital Identity Wallets.*
3. *By ... [6 months after the date of entry into force of this amending Regulation], the Commission shall adopt an implementing act on the implementation of the European Digital Identity Wallets as referred to in*

Article 6a(11), *laying down further technical specifications that are privacy enhancing and that will ensure trustworthy, secure and interoperable cross-border authentication and identification of users. That implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;*

(13) Article 12 is amended as follows:

(-a) the title is replaced by the following:

‘**■** Interoperability’;

(a) in paragraph 3, points (c) and (d) are *replaced by the following:*

‘(c) it facilitates the implementation of data protection and security by design;

(d) it ensures that personal data is processed in accordance with Regulation (EU) 2016/679.’;

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

‘(d) a reference to a minimum set of person identification data necessary to unequivocally represent a natural or legal person available from electronic identification schemes. In general, insofar as personal data are concerned, the risks to the rights of individuals shall be assessed based on Article 25(1) of Regulation (EU) 2016/679.’;

(ba) paragraph 5 is deleted;

(c) paragraph 6 is deleted;

(ca) paragraph 7 is deleted;

(cb) paragraph 9 is replaced by the following:

‘9. The implementing acts referred to paragraph 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(14) the following Article **■** is inserted:

‘Article 12a

Certification of electronic identification schemes

1. Conformity of notified electronic identification schemes with the requirements laid down in **Articles 8 and 10** may be certified by **conformity** bodies designated by Member States.
2. The peer-review of electronic identification schemes referred to in **Article 46b(5)**, point (c) **of this Regulation** shall not apply to electronic identification schemes or part of such schemes certified in accordance with paragraph 1. Member States may use a certificate or a Union statement of conformity issued in accordance with a relevant European cybersecurity certification scheme established pursuant to Regulation (EU) 2019/881 to demonstrate **full or partial** compliance of such schemes **or parts of such schemes** with the requirements set out in **Article 8(2) of this Regulation** regarding the assurance levels of electronic identification schemes.
 - 2a. **The certification scheme used to demonstrate conformity pursuant to paragraph 1 shall include a two-year vulnerability assessment of the certified product and a continuous threat monitoring, unless such a certification scheme has been established pursuant to Regulation (EU) 2019/881.**
3. Member States shall notify to the Commission with 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.’;

(15) the following heading is inserted after Article 12a:

‘SECTION III

CROSS-BORDER RELIANCE ON ELECTRONIC IDENTIFICATION MEANS’;

(16) the following Articles **12b** are inserted:

‘Article 12b

Cross-border reliance on European Digital Identity Wallets

1. Where Member States require an electronic identification using an electronic identification means and authentication under national law or by administrative practice to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets issued in **accordance** with this Regulation **for the purpose of electronic identification and authentication**

and shall clearly communicate such acceptance to potential users of the service.

2. Where private relying parties providing services are required, by **Union or national** law, to use strong user authentication for online identification, including in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, **telecommunications or education in particular with regard to the recognition of educational and professional qualifications**, private relying parties shall also **offer and** accept the use of European Digital Identity Wallets **and notified electronic identification means with assurance level ‘high’** issued in accordance **with this Regulation for identification and authentication**.
3. Where very large online platforms as defined in **Article 25(1) Regulation (EU) 2022/2065** require users to authenticate to access online services, they shall also accept, **though not exclusively, and facilitate** the use of European Digital Identity Wallets issued in accordance with Article 6a strictly upon voluntary request of the user and in respect of the **right to pseudonyms provided for in this Regulation. In this case, user generated pseudonyms shall be used in connection to a European Digital Identity Wallet. Very large online platforms shall clearly indicate this possibility to users of the service. The combination of person identification data and any other personal data and identifiers linked to the European Digital Identity Wallets with personal or non-personal data from any other services which are not necessary for the provision of the authentication or use of core services, is prohibited unless expressly requested by the user.**
4. The Commission shall, **in cooperation with the Member States, industry and the relevant stakeholders, including civil society**, encourage and facilitate the development of self-regulatory codes of conduct at Union level (‘codes of conduct’), in order to contribute to wide availability and usability of European Digital Identity Wallets within the scope of this Regulation. These codes of conduct shall ensure acceptance of electronic identification means including European Digital Identity Wallets within the scope of this Regulation in particular by service providers relying on third party electronic identification services for user authentication. The Commission will facilitate the

development of such codes of conduct in close cooperation with all relevant stakeholders and encourage service providers to complete the development of codes of conduct within 12 months of the adoption of this Regulation and effectively implement them within 18 months of the adoption of the Regulation.



Article 12c

Mutual recognition of other electronic identification means

1. Where electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access an online service provided by a public sector body in a Member State, the electronic identification means, issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that online service, *and ensuring mutual recognition* provided that the following conditions are met:
 - (a) the electronic identification means is issued under an electronic identification scheme that is included in the list referred to in Article 9;
 - (b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that online service in the Member State concerned, and in any case not lower than an assurance level ‘substantial’;
 - (c) the relevant public sector body in the Member State concerned uses the assurance level ‘substantial’ or ‘high’ in relation to accessing that online service.

Such recognition shall take place no later than 6 months after the Commission publishes the list referred to in point (a) of the first subparagraph.

2. An electronic identification means which is issued within the scope of an electronic identification scheme included in the list referred to in Article 9 and which corresponds to the assurance level ‘low’ may be recognised by public

sector bodies for the purposes of cross-border authentication for the online service provided by those bodies.’;

(17) In Article 13, paragraph 1 is replaced by the following:

1. Notwithstanding paragraph 2 of this Article, 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 and with the cybersecurity risk management obligations under Article 18 of the Directive XXXX/XXXX [NIS2].’;

(18) Article 14 is replaced by the following:

‘Article 14

International aspects

1. The Commission may adopt *delegated* acts, in accordance with Article 47, **supplementing this Regulation by** setting out the conditions under which the requirements of a third country applicable to the trust service providers established in its territory and to the trust services they provide can be considered equivalent to the requirements applicable to qualified trust service providers established in the Union and to the qualified trust services they provide.
2. Where the Commission has adopted *a delegated* act pursuant to paragraph 1 or concluded an international agreement on the mutual recognition of trust services in accordance with Article 218 of the Treaty, trust services provided by providers established in the third country concerned shall be considered equivalent to qualified trust services provided by qualified trust service providers established in the Union.’;

(19) Article 15 is replaced by the following:

‘Article 15

Accessibility *to* persons with disabilities **and special needs**

The provision of trust services and end-user products used in the provision of those services shall be made **available in plain and intelligible language and** accessible for persons with disabilities **or to persons who experience**

functional limitations, such as older people, and persons with limited access to digital technologies, in accordance with the accessibility requirements of Annex I of Directive (EU) 2019/882 on the accessibility requirements for products and services *and the United Nations Convention on the Rights of Persons with Disabilities*¹;

(19a) *Article 16 is replaced by the following:*

"Article 16

Penalties

1. *Without prejudice to Article 31 of the Directive (EU) XXXX/XXXX [NIS2], Member States shall lay down the rules on penalties applicable to infringements of this Regulation. The penalties provided for shall be effective, proportionate and dissuasive, in particular where the infringing party is an SME.*
2. *Member States shall ensure that infringements by qualified trust service providers of the obligations laid down in this Regulation be subject to administrative fines of a maximum of at least EUR 10 000 000 or 2 % of the total worldwide annual turnover of the undertaking to which the qualified trust service provider belonged in the preceding financial year, whichever is higher.*
3. *Member States shall ensure that infringement by non-qualified trust service providers of the obligations laid down in this Regulation be subject to administrative fines of a maximum of at least EUR 7 000 000 or 1,4 % of the total worldwide annual turnover of the undertaking to which the non-qualified trust service provider belongs in the preceding financial year, whichever is higher."*

(20) *Articles 17, 18 and 19 are deleted.*

■

(22) Article 20 is amended as follows:

¹ *Approved by Council Decision 2010/48/EC of 26 November 2009 concerning the conclusion, by the European Community, of the United Nations Convention on the Rights of Persons with Disabilities (OJ L 23, 27.1.2010, p. 35).*

(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 18 of Directive (EU) XXXX/XXXX [NIS2]. ***Where components of trust services have been separately certified in accordance with this regulation, the conformity assessment body responsible for certifying the trust service shall not conduct additional audits of these components. Instead, conformity assessment bodies shall ensure that the interactions between the various components do not impede the trust service's compliance with the requirements laid down in this paragraph.*** Qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within three working days of receipt.’;

(b) in paragraph 2, the last sentence is replaced by the following

‘Without prejudice to any further obligations on data controllers or processors arising from Regulation (EU) 2016/679, where there is any reason to believe that data protection rules could have been breached, the supervisory body shall inform the supervisory authorities under Regulation (EU) 2016/679, the issuer and the controller of the European Digital Identity Wallet without undue delay and shall provide the results of its audits as soon as they are available.’;

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

‘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, taking into account in particular, the extent, duration and consequences of that failure, ***shall*** withdraw the qualified status of that provider or of the service concerned which it provides and, request it, where applicable

within a set time limit, to comply with the requirements of Directive XXXX/XXXX[NIS2]. The supervisory body shall inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1).

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.

4. **By ... [12 months *after the date of entry* into force of this *amending Regulation*]**, the Commission shall, by means of implementing acts, establish reference number for the following standards:
 - (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 of the qualified trust service providers as referred to in paragraph 1, carried out by the conformity assessment bodies;
 - (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 conformity assessment report referred to in paragraph 1.

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

(23) Article 21 is amended as follows:

- (a) paragraph 2 is replaced by the following:
 - ‘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 18 of Dir XXXX [NIS2], the supervisory body shall request the competent authorities referred to in

Dir XXXX [NIS2] to carry out supervisory actions in that regard and to provide information about the outcome within three days from their completion.

Where the supervisory body concludes that the trust service provider and the trust services provided by it comply with the requirements referred to in the first subparagraph, 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 after the date of entry into force of this amending Regulation]*, the Commission shall, by means of implementing acts, define 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).’;

(23a) Article 22 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. Each Member State shall establish, maintain, *regularly update* and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.’;

(b) the following paragraph is inserted:

‘3a. The Commission in coordination with Member States and where relevant ENISA shall develop a harmonised reporting mechanism for qualified trust service providers as well as other interested third parties to appeal in a

transparent and duly reasoned manner the decision of a Member State in respect to inclusion and removal of a qualified trust service provider from the trust list.’;

(c) the following paragraph is added:

‘5a. By ... [6 months after the date of entry into force of this amending Regulation] the Commission shall, by means of implemented acts lay down further details on the process referred to in paragraph 3a of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(24) in Article 23 the following paragraph 2a is added:


‘2a. Paragraph 1 and 2 shall also apply to trust service providers established in third countries and to the services they provide, provided that they have been recognised in the Union in accordance with Article 14.’;

(25) 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 for a trust service, 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 attribute is issued.

The information referred to in the first subparagraph shall be verified by the qualified trust service provider, either directly or by relying on a third party, in any of the following ways:

- (a) by means of a notified electronic identification means which meets the requirements set out in Article 8 with regard to the assurance *level* ‘high’;
- (b) by means of  a certificate of a qualified electronic signature or of a qualified electronic seal issued in *accordance* with point (a), (c) or (d);

- (c) by using other identification methods which ensure the identification of the natural 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 appropriate procedures and in accordance with national laws if other means are not available.’;
- (b) the following paragraph ■ is inserted:
- ‘1a. **By ...** [12 months after the **date of** entry into force of this Regulation], the Commission shall **adopt delegated acts in accordance with Article 47, supplementing this Regulation by setting** out minimum technical specifications, standards and procedures with respect to the verification of identity and attributes in accordance with paragraph 1, point c **of this Article.**’;
- (c) paragraph 2 is amended as follows:
- (1) point (d) is 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.’;
 - (2) the new points (fa) and (fb) are inserted:
 - ‘(fa) 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. Notwithstanding the provisions of Article 18 of Directive EU XXXX/XXX [NIS2], those measures shall include at least the following:
 - (i) measures related to registration and on-boarding procedures to a service;
 - (ii) measures related to procedural or administrative checks;

- (iii) measures related to the management and implementation of services.
- (fb) notify the supervisory body and, where applicable, other relevant bodies of any linked breaches or disruptions in the implementation of the measures referred to in paragraph (fa), points (i), (ii) and, (iii) that has a significant impact on the trust service provided or on the personal data maintained therein.’;
- (3) point (g) and (h) 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.’;
- (4) point (j) is deleted;
- (d) the following paragraph 4a is inserted:
 - ‘4a. Paragraph 3 and 4 shall apply accordingly to the revocation of electronic attestations of attributes.’;
- (e) paragraph 5 is replaced by the following:
 - ‘5. **By ... [12 months after the date of entry into force of this amending Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for the requirements referred to in paragraph 2 of this Article. compliance with the requirements laid down in this Article shall be presumed, where trustworthy systems and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;**

(f) the following paragraph 6 is inserted:

‘6. The Commission shall be empowered to adopt delegated acts *in accordance with Article 47, supplementing this Regulation with regard to* the additional measures referred to in paragraph 2(fa) *of this Article.*’;

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

‘6. Within 12 months after the entry into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards 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 meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(27) In Article 29, the following new paragraph 1a is added:

‘1a. Generating, managing and duplicating *qualified* electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider providing a qualified trust service for the management of a remote electronic qualified signature creation device.’;

(28) the following Article ■ is inserted:

‘Article 29a

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

1. The management of remote qualified electronic signature creation devices as a qualified service may only be carried out 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 only for back-up purposes provided 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 shall 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 signature creation device issued pursuant to Article 30.
2. **By ... [12 months after the entry into force of this *amending* Regulation]**, the Commission shall, by means of implementing acts, establish technical specifications and reference numbers of standards for the purposes of paragraph 1.’;
- (29) In Article 30, the following paragraph 3a is inserted:
- ‘3a. The certification referred to in paragraph 1 shall be valid for 5 years, conditional upon a regular 2 year vulnerabilities assessment. Where vulnerabilities are identified and not remedied, the certification shall be withdrawn.’;
- (30) In Article 31, paragraph 3 is replaced by the following:
- ‘3. **By ... [12 months after the date of entry into force of this *amending* Regulation]**, the Commission shall, by means of implementing acts, define formats and procedures applicable for the purpose of paragraph 1. 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 sub-paragraph is added:

‘Compliance with the requirements laid down in the first sub-paragraph shall be presumed where the validation of qualified electronic signatures meet the standards referred to in paragraph 3.’;
 - (b) paragraph 3 is replaced by the following:

‘3. **By [12 months after the date of entry into force of this *amending* Regulation]**, the Commission shall, by means of implementing acts,

establish reference numbers of standards 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) Article 34 is replaced by the following:

‘Article 34

Qualified preservation service for qualified electronic signatures

1. A qualified preservation service for qualified electronic signatures may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the qualified electronic signature beyond the technological validity period.
2. Compliance with the requirements laid down in the paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures meet the standards referred to in paragraph 3.
3. ***By [12 months after the date of entry into force of this amending Regulation],*** the Commission shall, by means of implementing acts, establish reference numbers of standards 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).’;

(33) Article 37 is amended as follows:

(a) the following paragraph 2a is inserted:

‘2a. Compliance with the requirements for advanced electronic seals referred to in Article 36 and in paragraph 5 of this Article shall be presumed where an advanced electronic seal meets the standards referred to in paragraph 4.’;

(b) paragraph 4 is replaced by the following:

‘4. ***By ... [12 months after the date of entry into force of this amending Regulation],*** the Commission shall, by means of implementing acts, establish reference numbers of standards for advanced electronic seals. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(34) Article 38 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III. Compliance with the requirements laid down in Annex III shall be presumed where a qualified certificate for electronic seal meets the standards referred to in paragraph 6.’;

(b) paragraph 6 is replaced by the following:

‘6. **By ... [12 months after the date of entry into force of this amending Regulation]**, the Commission shall, by means of implementing acts, establish reference numbers of standards for qualified certificates for electronic seals. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(35) the following Article ■ is inserted:

‘Article 39a

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

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

(36) Article 42 is amended as follows:

(a) the following new paragraph 1a 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 accurate time source meet the standards referred to in paragraph 2.’;

(b) paragraph 2 is replaced by the following

‘2. **By ... [12 months after the date of entry into force of this amending Regulation]**, the Commission shall, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for accurate time sources. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(37) Article 44 is amended as follows:

(a) the following paragraph 1a is inserted:

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

(b) paragraph 2 is replaced by the following:

‘2. **By ... [12 months after the date of entry into force of this amending Regulation]**, the Commission shall, by means of implementing acts, establish reference numbers of standards 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).’;

(38) Article 45 is replaced by the following:

‘Article 45

Requirements for qualified certificates for website authentication

1. Qualified certificates for website authentication shall ***allow the authentication and identification of the natural or legal person to whom the certificate was issued with a high level of assurance. Qualified certificates for website authentication shall also*** meet the requirements laid down in Annex IV. Qualified certificates for website authentication shall be deemed compliant with ***this paragraph and*** the requirements laid down in Annex IV where they meet the standards referred to in paragraph 3.
2. Qualified certificates for website authentication referred to in paragraph 1 shall be recognised by web-browsers. ***Web browsers shall not be prevented from taking measures that are both necessary and proportionate to address substantiated risks of breaches of security, user’s privacy and loss of integrity of certificates provided such measures are duly reasoned. In such a case, the web browser shall notify the Commission, ENISA and the qualified trust service provider that issued that certificate or set of certificates without delay of any measure taken. Such recognition means that*** web-browsers shall ensure that the ***relevant*** identity data ***and electronic attestation of attributes provided*** is displayed in a user friendly manner, ***where possible, consistent***

manner, that reflects the state-of-the-art regarding accessibility, user awareness and cybersecurity according to best industry standards. Web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1, with the exception of enterprises, considered to be microenterprises and small enterprises in accordance with Commission Recommendation 2003/361/EC in the first 5 years of operating as providers of web-browsing services.

3. *By ... [12 months after the date of entry into force of this amending Regulation]*, the Commission shall, by means of implementing acts, provide the specifications and reference numbers of standards for qualified certificates for website authentication referred to in paragraph 1 *and 2*. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(39) the following sections 9, 10 and 11 are inserted after Article 45:

‘SECTION 9

ELECTRONIC ATTESTATION OF ATTRIBUTES

Article 45a

Legal effects of electronic attestation of attributes

1. An electronic attestation of attributes shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form *or that it does not meet the requirements for qualified electronic attestations of attributes, or that it has been issued by a trust service provider established in a different Member State.*
2. A qualified electronic attestation of attributes shall have the same legal effect as *a* lawfully issued *attestation* in paper form. *Relying parties shall continue to accept such attestations in paper form as an alternative to electronic attestation of attributes.*
3. A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified electronic attestation of attributes in any other Member State.

Article 45b

Electronic attestation of attributes in public services

When 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 or the public sector body. In such a case, qualified electronic attestation of attributes from other Member States shall also be accepted.

Article 45c

Requirements for qualified attestation of attributes

1. Qualified electronic attestation of attributes shall meet the requirements laid down in Annex V. A qualified electronic attestation of attributes shall be deemed to be compliant with the requirements laid down in Annex V, where it meets the standards referred to in paragraph 4.
2. ***Without prejudice to its content***, qualified electronic attestations of attributes shall not be subject to any mandatory ***technical*** requirement in addition to the requirements laid down in Annex V.
3. 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. ***Only relying parties the user has shared this attribute with shall be able to link the revocation to those attributes.***
4. ***By ... [6 months after the entry*** into force of this ***amending*** Regulation, the Commission shall establish reference numbers of standards for qualified electronic attestations of attributes by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(11).

Article 45d

Verification of attributes against authentic sources

1. Member States shall ensure that, at least for the attributes listed in Annex VI, wherever these attributes rely on authentic sources within the public sector, measures are taken to allow qualified providers of electronic attestations of attributes to verify *free of charge* by electronic means at the request of the user, the authenticity of the attribute directly against the relevant authentic source at national level or via designated intermediaries recognised at national level in accordance with *Union or* national law.
 - 1a. *Authentic sources may issue non-qualified electronic attestation of attributes at the request of the user.*
2. *By ... [6 months after the date of entry into force of this amending Regulation],* taking into account relevant international standards, the Commission shall, *by means of implementing acts*, set out the minimum technical specifications, standards and procedures with reference to the catalogue of attributes and schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(11). *Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).*

Article 45e

Issuing of electronic attestation of attributes to the European Digital Identity Wallets

1. Providers of qualified electronic attestations of attributes shall provide an interface with the European Digital Identity Wallets issued in accordance in Article 6a.
 - 1a. *Public registers shall provide qualified electronic attestation of attributes to the user of a European Digital Identity Wallet at the request of the user.*
 - 1b. *Non-qualified attestation of attributes can be issued by any trust service provider, an authentic source or directly through a European Digital Identity Wallet.*

- 1c. Providers of electronic attestations of attributes established in a Member State other than the Member State that issued user's European Digital Identity Wallet, shall provide that user with the possibility to request, obtain, store and manage the electronic attestation of attributes in an easy manner, with no additional technical, administrative or procedural requirements for the European Digital Identity Wallet issued and managed by the Member State of origin.***

Article 45f

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.
2. Personal data relating to the provision of electronic attestation of attributes services shall be kept logically separate from other data held.
3. Personal data relating to the provision of qualified electronic attestation of attributes services shall be kept physically and logically separate from any other data held.
4. Providers of qualified electronic attestation of attributes' services shall provide such services under a separate legal entity.

SECTION 10

QUALIFIED ELECTRONIC ARCHIVING SERVICES

Article 45fa

Legal effects of an electronic archiving service

1. ***The legal effect and the admissibility of data and documents archived using an electronic archiving service as legal evidence shall not be refused on the sole grounds that this service is in an electronic form or does not fulfil the requirements of a qualified electronic archiving service.***
2. ***The data and documents archived using a qualified electronic archiving service shall benefit from a presumption regarding the integrity of the***

archived data and documents, their availability, their traceability, their accuracy and their origin as well as the identification of users.

Article 45g

Qualified electronic archiving services

A qualified electronic archiving service for electronic documents may only be provided by a qualified trust service provider ***which implements*** procedures and ***uses*** technologies ***that ensure that all the requirements for a qualified electronic archiving service are met.***

Within **24** months after the entry into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for electronic archiving services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 45ga

Requirements for qualified electronic archiving services

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

- (a) they are created or maintained by a qualified trust service provider;***
- (b) they ensure the integrity and the accuracy of their origin and legal features throughout the conservation period;***
- (c) they ensure the accuracy of the date and time of the archiving process;***

2. Compliance with the requirements laid down in paragraph 1 shall be presumed where an electronic archiving service meets the standards referred to in paragraph 3.

3. The Commission may, by means of implementing acts, establish reference numbers of standards for the processes of reception, storing, deletion and transmission of electronic data or documents. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

(39a) the following Articles are inserted:

"Article 46a

National competent authorities and single point of contact

- 1. Each Member State shall establish one or more new national competent authorities to carry out the tasks assigned to them under Article 46b or designate an existing body for that purpose.***
- 2. Each Member State shall designate one national single point of contact on the European digital identity framework (single point of contact). Where a Member State designates only one competent authority, that competent authority shall also be the single point of contact for that Member State.***
- 3. Each single point of contact shall exercise a liaison function to ensure cross-border cooperation of its Member State's competent authorities with the relevant authorities in other Member States, and, where appropriate, the Commission and ENISA, as well as to ensure cross-sectorial cooperation with other national competent authorities within its Member State.***
- 4. Member States shall ensure that the competent authorities established or designated pursuant to paragraph 1 of this Article have the necessary powers and adequate resources to carry out, in an effective and efficient manner, the tasks assigned to them and thereby to fulfil the objectives of this Regulation. Member States shall ensure effective, efficient and secure cooperation of the designated representatives in the European Digital Identity Framework Board established pursuant to Article 46c.***
- 5. Each Member State shall, without undue delay, notify the Commission of the establishment or designation of the competent authority pursuant to paragraph 1. They shall also make public and notify the Commission of the identity and tasks of single point of contact designated pursuant to paragraph 2 and any subsequent changes thereto. The Commission shall publish a list of those single points of contacts.***

Article 46b

Tasks of the national competent authorities

1. *The national competent authorities shall carry the following tasks:*
 - (a) *to monitor and enforce the application of this Regulation;*
 - (b) *to supervise issuers of European Digital Identity Wallets established in its territory through ex ante and ex post supervisory activities, ensuring they meet the requirements laid down in this Regulation and to take corrective actions when they fail to do so;*
 - (c) *to supervise allegedly unlawful or inappropriate behaviours of relying parties established in its territory, in particular when such behaviours have been reported through European Digital Identity Wallets and apply corrective actions if necessary;*
 - (d) *to supervise qualified trust service providers established in the territory of the designating Member State through 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;*
 - (e) *to take action if necessary, in relation to non-qualified trust service providers established in the territory of the designating Member State, through 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;*
 - (f) *to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1);*
 - (g) *to inform the relevant national competent authorities of the Member States concerned, designated pursuant to Directive (EU) XXXX/XXXX [NIS2], of any significant breaches of security or loss of integrity they become aware of in the performance of their tasks and, in the case of a significant breach of security or loss of integrity which concerns other Member States, to inform the single point of contact of the Member State concerned designated pursuant to Directive (EU) XXXX/XXXX (NIS2);*

- (h) to report to the Commission about their main activities in accordance with paragraph 2;*
 - (i) 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);*
 - (j) to cooperate with supervisory authorities established under Regulation (EU) 2016/679, in particular, by informing them without undue delay, about the results of audits of qualified trust service providers, where there is evidence that personal data protection rules have been breached and about security breaches which are likely to constitute personal data breaches, or about suspicions of such breaches that it has become aware of in the performance of its tasks, without prejudice to Regulation (EU) 2016/679;*
 - (k) to grant qualified status to trust service providers and to the services they provide and to withdraw this status in accordance with Articles 20 and 21;*
 - (l) to inform the body responsible for the national trusted list referred to in Article 22(3) about its decisions to grant or to withdraw qualified status, unless that body is also the national competent authority;*
 - (m) to verify the existence and correct application of provisions on termination plans in cases where the qualified trust service provider ceases its activities, including how information is kept accessible in accordance with Article 24(2), point (h);*
 - (n) to require that trust service providers and issuers of European Digital Identity Wallet's remedy any failure to fulfil the requirements laid down in this Regulation;*
 - (o) to cooperate with other national competent authorities and provide them with assistance in accordance with Article 46c.*
- 2. By 31 March each year, each national competent authority shall submit to the Commission a report on its main activities during the previous calendar year.**

3. *The Commission shall make the annual reports referred to in paragraph 2 available to the European Parliament and the Council and make them public.*
4. *By ... [12 months after the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, define the formats and procedures for the report referred to in paragraph 1, point (h) of this Article. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).*
5. *By ... [12 months after the date of entry into force of this amending Regulation], the Commission shall adopt a delegated act in accordance with Article 47, supplementing this Regulation by further specifying the tasks of the national competent authorities referred to in paragraph 1.*

Article 46c

The European Digital Identity Framework Board

1. *The European Digital Identity Framework Board (the 'EDIFB') shall be established.*
2. *The EDIFB shall be composed of representatives of national competent authorities and the Commission.*
3. *Stakeholders and all relevant third parties may be invited to attend meetings of the EDIFB and to participate in its work.*
4. *ENISA shall be invited when issues regarding cyber threats, notification of breaches, cybersecurity certificates or standards or other issues pertaining to the security are discussed.*
5. *The EDIFB shall have the following tasks:*
 - (a) *assist the Commission in the preparation of legislative proposals and policy initiatives in the field of digital wallets, electronic identification means and trust services;*
 - (b) *assist and cooperate with the Commission on the preparation of implementing and delegated acts pursuant to this Regulation;*

- (c) *support the consistent application of this Regulation, among other for the purpose of:*
- (i) *exchanging good practices and information regarding the application of the provisions of this Regulation;*
 - (ii) *examining the relevant developments in the European Digital Identity Wallet, electronic identification and trust services sectors;*
 - (iii) *organising regular joint meetings with relevant interested parties from across the Union to discuss activities carried out by the EDIFB and gather input on emerging policy challenges;*
 - (iv) *issuing common guidelines on the implementation of the Regulation;*
 - (v) *with the support of ENISA, exchanging information, experience and good practice as regards to all cybersecurity aspects of the European Digital Identity Wallet, the electronic identification schemes and trust services;*
 - (vi) *national competent authorities under this Regulation and national competent authorities under Directive (EU) XXXX/XXXX of the European Parliament and of the Council [NIS2] shall cooperate to ensure the continuation of current practices and to build on the knowledge and experience gained in the application of the eIDAS Regulation. In addition, they shall collaborate as to ensure a coherent implementation of the Directive (EU) XXXX/XXXX of the European Parliament and of the Council [NIS2];*
 - (vii) *providing guidance in relation to the development and implementation of policies on notification of breaches, coordinated vulnerability disclosure and common measures as referred to in Articles 10 and 10a;*
 - (viii) *exchanging best practices and information in relation to the cybersecurity measures of this Regulation and on Directive (EU)*

XXXX/XXXX of the European Parliament and of the Council [NIS2] as regards to trust services, in relation to 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;

(ix) carrying out coordinated security risk assessments in cooperation with ENISA;

(x) peer review of notified electronic identification schemes falling under this Regulation.

6. In the framework of the EDIFB, Member States may seek mutual assistance:

(a) upon receipt of a reasoned request from a national competent authority, EDIFB shall provide that national competent authority with assistance so that it can be carried out in a consistent manner, which may cover, in particular, information requests and supervisory measures, such as 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;

(b) where appropriate, Member States may authorise their respective national competent authorities to carry out joint investigations in which staff from other Member States' competent national authority is involved. The arrangements and procedures for such joint actions shall be agreed upon and established by the Member States concerned in accordance with their national law.

7. By ... [6 months after the date of entry into force of this amending Regulation] and every two years thereafter, the EDIFB shall establish a work programme in respect of actions to be undertaken to implement its objectives and tasks.

8. The Commission may adopt implementing acts laying down procedural arrangements necessary for the functioning of the EDIFB. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(39b) *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 6a(11a), Article 6c(6), Article 24(1a) and 24(6), Article 30(4) and Article 46b(5)* 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 6a(11a), Article 6c(6), Article 24(1a) and (6), Article 30(4) and Article 46b(5)* 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 6a(11a), Article 6c(6), Article 24(1a) or (6), Article 30(4) or Article 46b(5)* 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.’;

(40) The following Article **■** is inserted:

‘Article 48a

Reporting requirements

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

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 **and the number of and reasons for the rejection of application of service providers aiming to become a relying party**;
 - (ba) the number of user complaints and consumer protection or data protection incidents relating to relying parties and qualified trust services**;
 - (c) **the type and number of** incidents and down time of the infrastructure at national level preventing the use of *European* Digital Identity *Wallets* **█** ;
 - (ca) the type and number of security incidents, suspected data breaches and affected users of European Digital Identity Wallets or qualified trust service**;
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 March each year, Member States shall submit to the Commission a report on the statistics collected in accordance with paragraph 2.’;

(41) Article 49 is replaced by the following:

‘Article 49

Review

1. The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council **by ... [24 months after the date of entry into force of this amending Regulation]**. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions 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 for amendment of this Regulation.

2. The evaluation report shall include an assessment of the availability, *security* and usability of the identification means including European Digital Identity Wallets in scope of this Regulation and assess whether all online private service providers relying on third party electronic identification services for users authentication, shall be mandated to accept the use of notified electronic identification means and European *Digital Identity Wallet*.
3. In addition, the Commission shall submit a report to the European Parliament and the Council every four years after the report referred to in the first paragraph on the progress towards achieving the objectives of this Regulation.’;

(42) 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 as qualified electronic signature creation devices under this Regulation until [date – OJ please insert period of four years following the entry into force of this 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 [date – PO please insert a period of four years following the entry into force of this Regulation].’;

(43) Annex I is amended in accordance with Annex I to this Regulation;

(44) Annex II is replaced by the text set out in Annex II to this Regulation;

(45) Annex III is amended in accordance with Annex III to this Regulation;

(46) Annex IV is amended in accordance with Annex IV to this Regulation;

(47) a new Annex V is added as set out in Annex V to this Regulation;

(48) a new Annex VI is added to this Regulation.

Article 2

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

The President

For the Council

The President

Annex I

In Annex I, 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;
- (ia) an indication, in a machine-readable format, showing which identity verification method listed in Article 24(1) was used during issuance of the certificate;’.***

Annex II

REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

1. Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:

Qualified electronic signature creation devices shall ensure, by appropriate technical and procedural means, that at least:

- (a) the confidentiality of the electronic signature creation data used for electronic signature creation is reasonably assured;
- (b) the electronic signature creation data used for electronic signature creation can practically occur only once;
- (c) the electronic signature creation data used for electronic signature creation cannot, with reasonable assurance, be derived and the electronic signature is reliably protected against forgery using currently available technology;
- (d) the electronic signature creation data used for electronic signature creation can be reliably protected by the legitimate signatory against use by others.

2. Qualified electronic signature creation devices shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.

Annex III

In Annex III, 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;

(ia) an indication, in machine readable format, showing which identity verification method listed in paragraph 1 of Article 24 was used during issuance of the seal;’

Annex IV

Annex IV 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 ***with a high level of assurance***, or a pseudonym. If a pseudonym is used, it shall be clearly indicated; █

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

(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

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:
 - for a legal person: the name and, where applicable, registration number as stated in the official records,
 - for a natural person: the person's name;
- (c) a set of data unambiguously representing the entity to which the attested attributes is referring to; 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 advanced electronic signature or advanced electronic seal referred to in point (f) 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

MINIMUM LIST OF ATTRIBUTES

Further to Article 45d, Member States shall 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, 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 in cases where these attributes rely on authentic sources within the public sector:

1. Address;
2. *Date of birth*;
3. Gender;
4. Civil status;
5. Family composition;
6. Nationality *or nationalities*
- 6a. *Citizenship or citizenships*;
7. Educational qualifications, titles and licenses;
8. Professional qualifications, titles and licenses;
- 8a. *Documents proving the activation of a protection regime and name of the authorised party designated to act on behalf of the natural person*;
9. Public permits and licenses;
10. *Company* data.