Council of the European Union

Brussels, 25 November 2022
(OR. en)

14959/22

Interinstitutional File:
2021/0136(COD)

LIMITE

TELECOM 473
COMPET 919
MI 844
DATAPROTECT 321
JAI 1497
CODEC 1774

NOTE

From:	Permanent Representatives Committee (Part 1)
To:	Council
No. prev. doc.:	14344/22
No. Cion doc.:	9471/21
Subject:	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 - General approach

I. INTRODUCTION

1. The Commission adopted the proposal for a Regulation on a European Digital Identity (**European eID**) on 3 June 2021[1]. The initiative amends the eIDAS Regulation from 2014[2], which had laid the necessary foundations to safely access services and carry out transactions online and across borders in the EU.

[1] doc. 9471/21.
[2] Regulation (EU) No 910/2014.

2. The proposal, based on Article 114 TFEU, requires Member States to issue a European Digital Identity Wallet under a notified eID scheme, built on common technical standards, following compulsory certification. In order to set up the necessary technical architecture, speed up the implementation of the revised Regulation, provide guidelines to Member States and avoid fragmentation, the proposal was accompanied by a Recommendation for the development of a Union Toolbox.

3. The proposed Regulation aims to ensure universal access for people and businesses to secure and trustworthy electronic identification and authentication by means of a personal digital wallet on a mobile phone.

II. WORK IN THE OTHER INSTITUTIONS

1. In the European Parliament, the proposal was referred to the Committee on Industry, Research and Energy (ITRE), with three committees being asked for an opinion, namely the Committee on the Internal Market and Consumer Protection (IMCO), the Committee on Legal Affairs (JURI) and the Committee on Civil Liberties, Justice and Home Affairs (LIBE). The rapporteur for the file is Romana Jerković (S&D, Croatia). The ITRE Committee has not yet adopted its report.

2. On 15 July 2021 the European Economic and Social Committee was invited to give its opinion on the proposal, which was subsequently delivered on 20 October 2021. The European Committee of the Regions spontaneously issued an opinion on the proposal on 12 October 2021.

3. The European Data Protection Supervisor (EDPS) published formal comments on the proposal on 28 July 2021.

III. STATE OF PLAY IN THE COUNCIL

1. In the Council, the proposal has been examined in the Working Party on Telecommunications and Information Society (WP TELECOM), which started discussions under the Portuguese Presidency in June 2021. The analysis of the proposal continued in WP TELECOM under the Slovenian Presidency, and the first reading was successfully concluded on 15 November 2021.

2. The French Presidency presented its **first compromise proposal** on 15 February and 5 April, and the **second one** was discussed on 23 May and 9 June. In connection with a policy debate held at WP TELECOM of 19 July 2022, the Czech Presidency — building on the work of the French Presidency — singled out major outstanding high-level issues and asked delegations to express their preferred options, with a view to redrafting the relevant parts of the second compromise proposal accordingly. The revised version resulted in a **third compromise proposal** that was presented by the Czech Presidency at the WP TELECOM of 5 and 8 September. Additional iterations and related adjustments successfully fostered a deeper level of convergence on most of the outstanding issues.

3. However, the **fourth compromise proposal**, introduced to delegations at the WP TELECOM of 28 September, revealed persisting divergence between Member States around one high-level issue in particular, namely the Level of Assurance ('LoA') chosen for the European Digital Identity Wallet. Some of the Member States that already have a national eID system in place initially adopted, and subsequently invested, in a LoA 'substantial', whereas in the current eID proposal a LoA 'high' is required. Being aware of a high number of electronic identification means of LoA 'substantial' issued in some Member States, the Czech Presidency has further proposed a mechanism to facilitate the on boarding of users, thereby contributing to the uptake of European Digital Identity Wallets. The provision allows users to enrol to the European Digital Identity Wallet by utilizing existing national eID means at LoA 'substantial' in conjunction with additional remote on-boarding procedures that together meet the requirements of LoA 'high'. Technical and operational specifications are subject to implementing legislation and conformity with requirements shall be certified.

4. The **fifth compromise proposal** was discussed during the WP TELECOM meeting of 25 October. During the WP TELECOM meeting on 8 November 2022 the Czech Presidency presented the limited changes made and, further to the additional comments and drafting suggestions received from delegations, prepared the **final version of the compromise text** in view of submitting it to Coreper.

5. On 18 November Coreper examined this compromise proposal and **unanimously agreed to submit it to the TTE (Telecommunications) Council, without any changes, in view of a general approach** at its meeting of 6 December 2022.

IV. MAIN ELEMENTS OF THE COMPROMISE PROPOSAL

1. The European Digital Identity Wallet

One of the main policy objectives of the Commission proposal for a European Digital Identity Wallet ('Wallet') is to provide citizens and other residents, as defined by national law, with a harmonised European Digital Identity means based on the concept of a European Digital Identity Wallet. As an electronic identification means ('eID means') issued under national schemes at assurance level 'high', the Wallet would be an eID means in its own right based on the issuing of person identification data and the Wallet by Member States.

2. Assurance level of the European Digital Identity Wallet

Assurance levels ('LoA') should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned. Based on the broad support recorded in Working Party meetings and in the Coreper debate of 14 October, the Wallet must be issued within an electronic identification system meeting the LoA 'high'. Furthermore, a specific provision on the on-boarding of users has been added to **Article 6a**. This change is meant to address the concerns of Member States where a significant number of national eID means at LoA 'substantial' has already been issued. The provision enables a user to use their national eID means in conjunction with additional remote on-

boarding procedures to make identity proofing at LoA 'high' possible and, ultimately, to obtain a Wallet. Since the draft eID Regulation relies on cybersecurity certifications schemes that should bring a harmonised level of trust in the security of European Digital Identity Wallets, also the secure storage of cryptographic material is expected to become subject to cybersecurity certification. The Presidency has therefore proposed a new **Recital (10b)** addressing these technical preconditions of achieving of LoA 'high' and enabling for a follow-up process within the implementation of European Digital Identity Wallets.

3. Notification of relying parties

3.1 **Article 6b** on notification of relying parties has been rephrased. As a general rule, the notification process by means of which the relying party communicates its intent to rely on the Wallet should be cost-effective, proportionate-to-risk and ensure that the relying party provides at least the information necessary to authenticate to the Wallet. By default, only minimum information is required, and the notification should allow for the use of automated or simple self-reporting procedures.

3.2 A specific regime may however be necessary due to sectoral requirements, such as those applicable to the processing of special categories of personal data. A corresponding provision has therefore been introduced that aims to cover cases where a more stringent registration or authorization procedure is required. Conversely, where Union or national law does not lay down specific requirements in order to access information provided by means of the Wallet, Member States may exempt such relying parties from the obligation to notify their intent to rely on Wallets.

4. Certification

4.1 The Regulation should leverage, rely on and mandate the use of relevant and existing Cybersecurity Act certification schemes, or parts thereof, to certify the compliance of Wallets, or parts thereof, with the applicable cybersecurity requirements. Consequently, the Cybersecurity Act framework applies fully, including the peer review mechanism between national cybersecurity certification authorities provided within the Cybersecurity Act. In order to align as much as possible the eID Regulation and the Cybersecurity Act, Member States will designate public and private bodies accredited to certify the Wallet as provided in the Cybersecurity Act.

4.2 In addition, the Commission is encouraged to mandate ENISA to undertake the development and adoption of a dedicated Cybersecurity Act scheme for the cybersecurity certification of the Wallet. Until such scheme is developed, the EUCC scheme (Common Criteria based European cybersecurity certification scheme) published under the Cybersecurity Act will be used as the baseline methodology for the Wallet certification. For requirements not related to cybersecurity, notably those covering other functional and operational aspects of the Wallet, a list of specifications, procedures and reference standards is to be established. These requirements are subject to certification.

5. Implementing period for the provision of the Wallet

Based on guidance by Member States, it has been proposed that the implementing period of 24 months is counted from the adoption of the implementing acts referred to in **Article 6a(11)** and **Article 6c(4)**.

6. Fees

It has been clarified in **Article 6a(6a)** and corresponding recital that the issuance, use for authentication and revocation of Wallets should be free of charge to natural persons. Except when Wallets are used for authentication, services relying on the use of the Wallet may incur costs, e.g. the issuance of the electronic attestations of attributes to the Wallet.

7. Access to hardware and software features including the Secure Element

The Presidency has suggested to provide for explicit articulation with Regulation (EU) 2022/1925, which ensures access to hardware and software features as part of core platform services provided by gatekeepers. The newly added **Article 12b** clarifies that providers of Wallets and issuers of notified electronic identification means acting in a commercial or professional capacity are business users of gatekeepers within the meaning of the respective definition in the DMA. Recital wording has been added to outline the implication of the interlink with the DMA, namely that gatekeepers should be required to ensure, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware or software features that are available or used in the provision of its own complementary and supporting services.

8. Alternate possibilities to issue electronic attestation of attributes by public bodies

The issuance of qualified electronic attestation of attributes by qualified providers has been retained, including the obligation for Member States, to ensure that attributes can be verified against an authentic source within the public sector. In addition to that, a possibility that electronic attestation of attributes with the same legal effects as qualified electronic attestation of attributes may be issued to the Wallet directly by the public sector body responsible for the authentic source or by designated public sector body on behalf of a public sector body responsible for an authentic source has been introduced, provided that necessary requirements are met. The proposal is reflected in new **Articles 45a**, **45da** and in **Annex VII**.

9. Record Matching

The original **Article 11a** has been renamed to Record Matching as this better reflects the objective of the provision. Based on the discussion, the concept of unique and persistent identifier has been retained for Wallets. The respective definition clarifies that the identifier may consist of a combination of several national and sectoral identifiers as long as it serves its purpose. It is explicitly stated that record matching may be facilitated by qualified electronic attestation of attributes. Further, a safeguarding provision has been incorporated into **Article 11a** according to which Member States shall ensure the protection of personal data and prevent profiling of users. Lastly, Member States in their capacity as relying parties, shall ensure record matching.

VI. CONCLUSION

1. In light of the above, the Council is invited to:

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

   – confirm a general approach on the proposal for Regulation on a European Digital Identity (European eID) at the meeting of the TTE (Telecommunications) Council on 6 December 2022.

ANNEX

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

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

Having regard to the proposal from the European Commission,

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

Having regard to the opinion of the European Economic and Social Committee[3],

Acting in accordance with the ordinary legislative procedure,

Whereas:

(1) The Commission Communication of 19 February 2020, entitled "Shaping Europe's Digital Future"[4] 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.

[3] OJ C , , p. .
[4] COM/2020/67 final

(2) In its conclusions of 1-2 October 2020[5], the European Council called on the Commission to propose the development of a Union-wide framework for secure public electronic identification, including interoperable digital signatures, to provide people with control over their online identity and data as well as to enable access to public, private and cross-border digital services.

(3) The Commission Communication of 9 March 2021 entitled "2030 Digital Compass: the European way for the Digital Decade"[6] sets the objective of a Union framework which, by 2030, leads to wide deployment of a trusted, user-controlled identity, allowing each user to control their own online interactions and presence.

(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 and will strengthen the Single Market by allowing citizens, other residents as defined by national law and businesses to identify online in a convenient and uniform way across the Union. The European Digital Identity Wallet will provide natural and legal persons across the Union with a harmonised electronic identification means that will enable them to authenticate and share data linked to their identity. 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 attestations of attributes, such as a university degree legally recognised and accepted everywhere in the Union. 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 at European level. 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 in a given format.

---

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

6 COM/2021/118 final/2

(4a) Several Member States have implemented and largely use electronic identification means that nowadays are accepted by service providers in the Union. Additionally, investments were made into both national and cross-border solutions based on the current eIDAS Regulation, including the eIDAS nodes interoperability technical infrastructure. In order to guarantee complementarity and a fast adoption of European Digital Identity Wallets by current users of notified electronic identification means and to minimise the impacts on existing service providers, European Digital Identity Wallets are expected to benefit from building on the experience with existing electronic identification means and taking advantage of the deployed eIDAS infrastructure at European and national levels.

(5) To support the competitiveness of European businesses, online 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 provided, 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.

(6) Regulation (EU) No 2016/679[7] applies 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. Personal data relating to the provision of European Digital Identity Wallets should be kept logically separate from any other data held by the issuer. This Regulation does not prevent issuers of European Digital Identity Wallets to apply additional technical measures contributing to protection of personal data, such as physical separation of personal data relating to the provision of Wallets from any other data held by the issuer.

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

(7) It is necessary to set out the harmonised conditions for the establishment of a framework for European Digital Identity Wallets to be provided by Member States, which should empower all Union citizens and other residents as defined by national law to share securely data related to their identity in a user friendly and convenient way under the sole control of the user. Technologies used to achieve those objectives should be developed aiming towards the highest level of security, privacy, user convenience and wide usability. Member States should ensure equal access to digital identification to all their nationals and residents.

(8) To ensure that relying parties can rely on the use of European Digital Identity Wallets and to protect the user against unlawful use of sensitive data, relying parties should be registered as part of a notification process. The notification requirements applicable to relying parties should in most cases be based on the provision of a limited amount of information required for the authentication of the relying party towards the European Digital Identity Wallet. The requirements should also allow for the use of automated or simple self-reporting procedures, including the reliance on and the use of existing registers by Member States. At the same time, for categories of sensitive data, specific regimes may exist at national or Union level, which may impose more stringent registrations and authorisation requirements on relying parties in order to prevent the unlawful use of identity data in such cases. In other use cases, relying parties may be exempted from notifying their intent to rely on the European Digital Wallet, for example, when a right to verify specific attributes does not require or allow for the authentication of the relying party by electronic means. Typically, in these in-person scenarios the user is able to identify the relying party thanks to the context, such as when interacting with a car rental clerk or pharmacist. The notification process is meant to be driven by sectoral Union or national laws as this allows to accommodate various use cases that may differ in terms of registration requirements, of mode of operation (online/offline), or in terms of the requirement to authenticate devices able to interface with the European Digital Identity Wallet. The verification of the use of the European Digital Identity Wallet by relying parties should not be mandated to be enforced at the level of the European Digital Identity Wallet.

(9) All European Digital Identity Wallets should allow 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, Wallets 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", the European Digital Identity Wallets should benefit from the potential offered by tamper-proof solutions such as secure elements, to comply with the security requirements under this Regulation. The European Digital Identity Wallets should also allow users to create and use qualified electronic signatures and seals which are accepted across the EU. To achieve simplification and cost reduction benefits to persons and businesses across the EU, including by enabling powers of representation and e-mandates, Member States should issue European Digital Identity Wallets relying on common standards to ensure seamless interoperability and a high level of security. 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 that the European Digital Identity Wallets rely on the legal identity of citizens, other residents or legal entities. Trust in the European Digital Identity Wallets would be enhanced by the fact that issuing parties are required to implement appropriate technical and organisational measures to ensure a level of security commensurate to the risks raised for the rights and freedoms of the natural persons, in line with Regulation (EU) 2016/679. The issuance, use for authentication and the revocation of European Digital Identity Wallets shall be free of charge to natural persons. Services relying on the use of the Wallet may incur costs related to, for instance, the issuance of the electronic attestations of attributes to the Wallet.

(9a) It is beneficial to facilitate the uptake and use of European Digital Identity Wallets by seamlessly integrating them with the ecosystem of public and private digital services already implemented at national, local or regional level. To achieve this goal, Member States may provide for legal and organizational measures in order to increase flexibility for issuers of European Digital Identity Wallets and to allow for additional functionalities of European Digital Identity Wallets beyond what is set out by this Regulation, including by enhanced interoperability with existing national eID means. This should be by no means to the detriment of providing core functions of the European Digital Identity Wallets as set out in this Regulation nor to promote existing national solutions over European Digital Identity Wallets. Since they go beyond this Regulation, those additional functionalities do not benefit from the provisions on cross-border reliance on European Digital Identity Wallets set out in this Regulation.

(10) To achieve a high level of data protection, security and trustworthiness, this Regulation should establish a harmonized framework detailing the common specifications and requirements applicable to the European Digital Identity Wallets. The conformity of European Digital Identity Wallets with those requirements should be certified by accredited conformity assessment bodies designated by Member States. Certification should rely, in particular, on relevant European cybersecurity certifications schemes, or parts thereof, established pursuant to Regulation (EU) 2019/881[8], as far as they cover the cybersecurity requirements applicable to European Digital Identity Wallets. Relying on European cybersecurity certifications schemes should bring a harmonised level of trust in the security of the European Digital Identity Wallets, irrespective where they are issued across the Union. The cybersecurity certification of the European Digital Identity Wallets should build on the role of the National Cybersecurity Certification Authorities to supervise and monitor the compliance of the certificates issued by the conformity assessment bodies within their jurisdiction with the relevant European cybersecurity schemes. Similarly, certification should leverage, as appropriate, on standards and technical specifications as specified in Regulation (EU) 2019/881. Such specifications may be used as state-of-the-art documents, as specified under relevant cybersecurity certification schemes pursuant to Regulation (EU) 2019/881. When no relevant European cybersecurity certification schemes established pursuant to Regulation (EU) 2019/881 cover the certification of relevant services or processes contributing to the security of the Wallet, appropriate schemes should be created in accordance with Title III of Regulation (EU) 2019/881. A common and harmonized scheme for the certification of European Digital Identity Wallets should be established for the assessment of their compliance with the common specifications and requirements provided in this Regulation, other than those related to cybersecurity and data protection, notably those covering functional and operational aspects. Regarding this certification, in order to ensure a high level of trust and transparency, mechanisms and procedures should be established aiming to foster peer learning and cooperation between Member States on the monitoring and review of the certification bodies and the certificates and certification reports they issue. Such peer learning mechanism should be without prejudice to Regulation (EC) 2016/679 and Regulation (EU) 2019/881. Certification of the Wallet under Regulation (EC) 2016/679 is a voluntary tool among others that can be used to demonstrate compliance with the requirements laid down in Regulation (EC) 2016/679 as they apply to European Digital Identity Wallets and their provision to European citizens.

[8] 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

(10a) The on-boarding of citizens and residents to the European Digital Identity Wallet should be facilitated by relying on electronic identification means issued at level of assurance 'high'. Electronic identification means issued at level of assurance 'substantial' should be relied upon only in cases where harmonised technical and operational specifications using electronic identification means issued at level of assurance 'substantial' in combination with other supplementary means of identity verification will allow the fulfillment of the requirements set out in this Regulation as regards level of assurance 'high'. Such supplementary means or measures should be reliable and easy to utilize by the users and could be built on the possibility to use remote on-boarding procedures, qualified certificates supported by qualified signatures, qualified electronic attestation of attributes or a combination thereof. To ensure sufficient uptake of European Digital Identity Wallets, harmonised technical and operational specifications for on-boarding of users by using electronic identification means, including those issued at level of assurance 'substantial', should be set out in implementing acts.

(10b) The objective of this Regulation is to provide the user with a fully mobile, secure and user-friendly European Digital Identity Wallet. As a transitional measure until the availability of certified tamper-proof solutions, such as secure elements within the users' devices, the European Digital Identity Wallets may rely upon certified external secure elements for the protection of the cryptographic material and other sensitive data or upon notified national solutions at level of assurance 'high' in order to demonstrate compliance with the relevant requirements of the Regulation as regards the level of assurance of the Wallet. The use of the above-mentioned transitional measure should be limited to use cases requiring level of assurance 'high', such as on-boarding of the user to the Wallet and authenticating to services requiring level of assurance 'high'. When authenticating to services requiring level of assurance 'substantial', European Digital Identity Wallets should not require the use of the above-mentioned transitional measure. This Regulation should be without prejudice to national conditions for the issuance and use of certified external secure element in case this transitional measure relies on it.

(11) European Digital Identity Wallets should ensure the highest level of protection and security for the personal data used for authentication irrespective of whether such data is stored locally or on cloud-based solutions, taking into account the different levels of risk. The processing of biometric data as an authentication factor in strong user authentication is one of the identifications methods providing a high level of confidence, in particular when used in combination with other elements of authentication. Since biometric data represents a unique characteristic of a person, the processing of biometric data is only allowed under the exceptions of Article 9(2) of Regulation (EU) 2016/679 and requires appropriate safeguards, commensurate to the risk that such processing may entail to the rights and freedoms of natural persons.

(11a) The functioning of European Digital Identity Wallets should be transparent and allow for verifiable processing of personal data. In order to achieve this, Member States are encouraged to disclose the source code of software components of European Digital Identity Wallets that are related to processing of personal data and data of legal persons. Disclosure of such source code enables society, including users and developers, to understand its operation. This also has the potential of increasing users' trust in the Wallet ecosystem and contributing to the security of Wallets by allowing anyone to report vulnerabilities and errors in the code. This entices suppliers to deliver and maintain a highly secure product. Additionally and where appropriate Member States are also encouraged to make the source code available under an open source license. An open source license enables society, including users and developers, to modify and reuse the source code.

(12) To ensure that the European Digital Identity framework is open to innovation, technological development and future-proof, Member States should be encouraged to set-up jointly sandboxes to test innovative solutions in a controlled and secure environment in particular to improve the functionality, protection of personal data, security and interoperability of the solutions and to inform future updates of technical references and legal requirements. This environment should foster the inclusion of European Small and Medium Enterprises, start-ups and individual innovators and researchers.

(13) Regulation (EU) No 2019/1157[9] 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 simplified 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 identification schemes under Regulation 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, as foreseen in 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.

[9] 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).

(17a) The use of unique and persistent identifiers issued by Member States or generated by the European Digital Identity Wallet, jointly with the use of person identification data, is essential to ensure that the identity of the user, in particular in the public sector and when mandated by national or Union law, can be verified. This Regulation should ensure that the European Digital Identity Wallet can provide a mechanism to enable record matching, including by the use of qualified electronic attestations of attributes, and allow for the inclusion of unique and persistent identifiers in the person identification data set. A unique and persistent identifier may consist of either single or multiple identification data that can be sector-specific as long as it serves to uniquely identify the user across the Union. The European Digital Identity Wallet should also provide a mechanism that allows for the use of relying party specific identifiers in cases when the use of a unique and persistent identifier is required by national or Union law. In all cases, the mechanism provided to facilitate record matching and the use of unique and persistent identifiers should ensure that the user is protected against misuse of personal data according to this Regulation and applicable Union law, in particular Regulation (EU) 2016/679, including against the risk of profiling and tracking related to the use of the European Digital Identity Wallet.

(17aa) It is essential to take into consideration the needs of users, thereby boosting demand for European Digital Identity Wallets. There should be meaningful use cases and online services relying on European Digital Identity Wallets available. For convenience of users and in order to ensure cross-border availability of such services, it is important to undertake actions in order to facilitate a similar approach to design, development and implementation of online services in all Member States. Non-binding guidelines on how to design, develop and implement online services relying on European Digital Identity Wallets have the potential of becoming a useful tool to achieve this goal. These guidelines should be prepared in due account of the interoperability framework of the Union. Member States should have a leading role when it comes to adopting them.

(18) In line with Directive (EU) 2019/882[10], persons with disabilities should be able to use the European digital identity wallets, trust services and 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 national or Union 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. When setting out 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, compliance with the relevant provisions in the Directive XXXX/XXXX, (NIS2 Directive) and Regulation (EU) 2016/679 should also be ensured, as well as the use of trusted lists as essential elements to build trust.

[10] 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).

(21) This Regulation should build on Union acts ensuring contestable and fair markets in the digital sector. In particular, it builds on the Regulation (EU) 2022/1925, which introduces rules for providers of core platform services designated as gatekeepers and, among others, prohibits gatekeepers to require business users to use, offer or interoperate with an identification service of the gatekeeper in the context of services offered by the business users using the core platform services of that gatekeeper. Article 6(7) of the Regulation 2022/1925 requires gatekeepers to allow business users and providers of ancillary services access to and interoperability with the same operating system, hardware or software features that are available or used in the provision by the gatekeeper of any ancillary services. According to Article 2 (15) of the Digital Markets Act identification services constitute a type of ancillary services. Business users and providers of ancillary services should therefore be able to access such hardware or software features, such as secure elements in smartphones, and to interoperate with them through the European Digital Identity Wallets or Member States' notified electronic identification means.

(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. In order to ensure that the data using a qualified electronic registered delivery service is delivered to the correct addressee, qualified electronic registered delivery services should ensure with full certainty the identification of the addressee while a high level of confidence would suffice as regard to the identification of the sender. Providers of qualified electronic registered delivery services should be encouraged by Member States to have their services to be interoperable with qualified electronic registered delivery services provided by other qualified trust service providers in order to easily transfer the electronic registered data between two or more qualified trust service providers and to promote fair practices in the internal market.

(25) In most cases, citizens and other residents cannot digitally exchange, across borders, information related to their identity, such as addresses, age and professional qualifications, driving licenses and other permits and payment data, securely and with a high level of data protection.

(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. Relying parties should use the electronic attestations of attributes as equivalent to attestations in paper format. Therefore, an electronic attestation of attributes should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic attestation of attributes. 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.

(28) Wide availability and usability of the European Digital Identity Wallets require their acceptance by private service providers. Private relying parties providing services in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications should accept the use of European Digital Identity Wallets for the provision of services where strong user authentication is required by national or Union law or by contractual obligation. To facilitate the use and acceptance of the European Digital Identity Wallet, widely accepted industry standards and specifications should be taken into account. Where very large online platforms as defined in Article 25.1. of Regulation [reference DSA Regulation] require users to authenticate to access online services, those platforms should be mandated to accept the use of European Digital Identity Wallets upon voluntary request of the user. Users should be under no obligation to use the wallet to access private services, but if they wish to do so, large online platforms should accept the European Digital Identity Wallet for this purpose while respecting the principle of data minimisation. 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 European Digital Identity Wallets within the scope of this Regulation. The codes of conduct should facilitate wide acceptance of electronic identification means including European Digital Identity Wallets by those service providers which do not qualify as very large platforms and which rely on third party electronic identification services for user authentication. They should be developed within 12 months of the adoption of this Regulation. The Commission should assess the effectiveness of these provisions for the availability and usability for the user of the European Digital Identity Wallets after 24 months of their deployment.

(29) Selective disclosure is a concept empowering the owner of data to disclose only certain parts of a larger data set, in order for the receiving entity to obtain only information that is required, e.g. for a user to disclose only data to a relying party that is necessary for provision of a service requested by a user. The European Digital Identity Wallet should technically enable the selective disclosure of attributes to relying parties. Such selectively disclosed attributes, including when originally parts of multiple distinct electronic attestations, may be subsequently combined and presented to relying parties. This feature should become a basic design feature thereby reinforcing convenience and the protection of personal data including data minimisation.

(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 national or Union law for the purpose of secure exchange of attested attributes between identity or attestation of attributes' service providers and relying parties. Member States should establish appropriate mechanisms at national level to ensure that qualified trust service providers issuing qualified electronic attestation of attributes are able, based on the consent of the person to whom the attestation is issued, to verify the authenticity of the attributes relying on authentic sources. Appropriate mechanisms may include the use of specific intermediaries or technical solutions in compliance with national law allowing access to authentic sources. Ensuring the availability of a mechanism that will allow for the verification of attributes against authentic sources should facilitate the compliance of the qualified trust service providers of qualified electronic attestation of attributes with their obligations set by this Regulation. Annex VI contains a list of categories of attributes for which Member States should ensure that measures are taken to allow qualified providers of electronic attestations of attributes to verify by electronic means, at the request of the user, their authenticity against the relevant authentic source. Specific attributes falling into these categories should be agreed upon Member States.

(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 online identification for the purpose of account login and initiation of transactions in the field of payment services.

(31a) In order to ensure the consistency of certification practices across the EU, the Commission should issue guidelines on the certification and recertification of qualified electronic signature creation devices and of qualified electronic seal creation devices, including their validity and limitations in time. This regulation does not prevent Member States from allowing public or private bodies that have certified qualified electronic signature creation devices to temporarily extend the validity of certification when a recertification of the same device could not be performed within the legally defined timeframe for a reason other than a breach or security incident, and without prejudice to the applicable certification practice.

(32) Website authentication services provide users with a high level of assurance that there is a genuine and legitimate entity standing behind the website, irrespective of the platform used to display it. Those services contribute to the building of trust and confidence in conducting business online and to reducing instances of fraud online. The use of website authentication services by websites should be voluntary. However, in order for website authentication to become a means to increase trust, providing a better experience for the user and furthering growth in the internal market, this Regulation should lay down minimal security and liability obligations for the providers of website authentication services and their services. To that end, providers of web-browsers should ensure support and interoperability with qualified certificates for website authentication pursuant to Regulation (EU) No 910/2014. They should recognise qualified certificates for website authentication and allow for the display of the certified identity data to the end-user in the browser environment based on the specifications set out in accordance with this Regulation. The recognition of a qualified certificate for website authentication as a qualified certificate issued by a qualified trust service provider should ensure that the identity data included in the certificate can be authenticated and verified in accordance with this Regulation. This should not affect the possibility for providers of web-browsers to address major non-conformities related to breach of security and loss of integrity of individual certificates, thus contributing to the online security of end-users. To further protect citizens and promote their usage, public authorities in Member States should consider incorporating qualified certificates for website authentication in their websites.

(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 data and associated trust services. To ensure legal certainty, trust and harmonization across Member states, a legal framework for qualified electronic archiving services should be established, inspired by the framework of the other trust services set out in this Regulation. This framework should offer trust service providers and users an efficient toolbox that includes functional requirements for the electronic archiving service, as well as clear legal effects when a qualified electronic archiving service is used. These provisions should apply to electronically born documents as well as paper documents that have been scanned and digitised. When required, these provisions should allow for the preserved electronic data to be ported on different media or formats for the purpose of extending their durability and legibility beyond the technological validity period, while minimising loss and alteration to the greatest extent possible. When electronic data submitted to the digital archiving service contain one or more qualified electronic signatures or qualified electronic seals, the service should use procedures and technologies capable of extending their trustworthiness for the preservation period of such data, possibly relying on the use of other qualified electronic trust services established by this Regulation. For creating preservation evidence where electronic signatures, electronic seals or electronic timestamps are used, qualified electronic trust services should be used. As far as electronic archiving services are not harmonised by this Regulation, Member States may maintain or introduce national provisions, in conformity with Union law, relating to those services, such as specific provisions allowing some derogations for services integrated in an organisation and strictly used for "internal archives" of this organisation. This Regulation should not distinguish between electronically born documents and physical documents that have been digitised.

(33a) National archives and memory institutions, in their capacity as organizations dedicated to preserving the documentary heritage in public interest, are usually mandated to conduct their activities by national law and do not necessarily provide trust services within the meaning of this Regulation. In so far these institutions do not provide such services, this Regulation is without prejudice to their operation.

(34) Electronic ledgers are a sequence of electronic data records which ensure their integrity and the accuracy of their chronological ordering. The purpose of electronic ledgers is to establish a chronological sequence of data records to prevent that digital assets are copied and sold to several recipients. Electronic ledgers can, for example, be used for digital records of ownership in global trade, supply chain financing, the digitalisation of intellectual property rights or of commodities such as electricity. In conjunction with other technologies, they can contribute to solutions for more efficient and transformative public services such as e-voting, cross border cooperation of customs authorities, cross border cooperation of academic institutions, or the recording of ownership for real estate in decentralised land registries. Qualified electronic ledgers create a legal presumption for the unique and accurate sequential chronological ordering and integrity of the data records in the ledger. The specific attributes of electronic ledgers, that is the sequential chronological ordering of data records, distinguishes electronic ledgers from other trust services such as electronic time stamps and electronic registered delivery services. Namely, neither the time stamping of digital documents, nor their transfer by means of electronic registered delivery services could without further technical or organisational measures sufficiently prevent the same digital asset from being copied and sold more than once to different parties. The process of creating and updating an electronic ledger depends on the type of ledger used (centralised or distributed).

(35) To prevent fragmentation of the internal market a pan-European legal framework should be established allowing for the cross-border recognition of trust services for the recording of data in qualified electronic ledgers. Trust service providers for electronic ledgers should be mandated to ascertain the sequential recording of data into the ledger. This Regulation is notwithstanding any legal obligations that users of electronic ledgers may need to comply with under Union and national law. For instance, use cases that involve the processing of personal data should comply with Regulation (EU) 2016/679. Use cases that involve crypto assets should be compatible with all applicable financial rules including, for example, the Markets in Financial Instruments Directive[11], the Payment Services Directive[12], the E-Money Directive[13], as well as with possible future legislation on Markets in Crypto Assets and with anti-money laundering rules which could be included in the Transfer of Funds Regulation[14], and could require crypto asset service providers to verify the identity of users of electronic ledgers in order to comply with international anti-money laundering standards.

[11] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC, OJ L 173, 12.6.2014, p. 349–496.

[12] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, OJ L 337, 23.12.2015, p. 35–127.

[13] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC, OJ L 267, 10.10.2009, p. 7–17.

[14] See the Commission's proposal of 20.7.2021 to recast Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds, COM/2021/422 final.

(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 and the private sector is needed. To achieve this objective, Member States should cooperate within the framework set out in the Commission Recommendation XXX/XXXX [Toolbox for a coordinated approach towards a European Digital Identity Framework][15] to identify a Toolbox for a European Digital Identity framework. The Toolbox should include a comprehensive technical architecture and reference framework, a set of common standards and technical references and a set of guidelines and descriptions of best practices covering at least all aspects of the functionalities and interoperability of the European Digital Identity Wallets including eSignatures and of the qualified trust service 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 the European Digital Identity Wallets, to facilitate take up, in particular by small and medium sized companies in a cross-border context. The content of the toolbox should evolve in parallel with and reflect the outcome of the discussion and process of adoption of the European Digital Identity Framework.

(36a) Member States should lay down rules on penalties for infringements such as direct or indirect practices leading to confusion between non-qualified and qualified trust services or to the abusive use of the EU trust mark by non-qualified trust service providers. The EU trust mark should not be used under conditions which, directly or indirectly, lead to the belief that any non-qualified trust services offered by this provider are qualified.

[15] [insert reference once adopted]

(36b) This Regulation should ensure a harmonized level of quality, trustworthiness and security of qualified trust services, regardless of the place where the operations are conducted. Thus, a qualified trust service provider should be allowed to outsource its operations related to the provision of a qualified trust service outside of the Union, should it provide the guarantees, ensuring that supervisory activities and audits can be enforced as if these operations were carried out in the Union. When the compliance with the Regulation cannot be fully assured, the supervisory bodies should be able to adopt proportionate and justified measures including withdrawal of the qualified status of the trust service provided.

(36c) To ensure legal certainty as regards the validity of advanced electronic signatures based on qualified certificates, it is essential to specify the components of an advanced electronic signature based on qualified certificates, which should be assessed by the relying party carrying out the validation of that signature.

(36d) Trust service providers should use cryptographic algorithms reflecting current best practices and trustworthy implementations of these algorithms in order to ensure security and reliability of their trust services.

(36e) This Regulation should set out an obligation for qualified trust service providers to verify the identity of a natural or legal person to whom the qualified certificate is issued based on various harmonized methods across the EU. Such a method may include the reliance on electronic identification means which meets the requirements of level of assurance 'substantial' in combination with additional harmonized remote procedures which ensures the identification of the person with a high level of confidence.

(36f) Issuers of European Digital Identity Wallets and issuers of notified electronic identification means acting in a commercial or professional capacity using core platform services offered by gatekeepers for the purpose of or in the course of providing goods and services to end-users should be considered business users in accordance with Art. 2(21) of Regulation (EU) 2022/1925. The gatekeepers should therefore be required to ensure, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same operating system, hardware or software features that are available or used in the provision of its own complementary and supporting services and hardware. This should allow issuers of European Digital Identity Wallets and issuers of notified electronic identification means to interconnect through interfaces or similar solutions to the respective features as effectively as the gatekeeper's own services or hardware.

(36g) To keep this Regulation in line with current developments and to follow the practices on the internal market, the delegated and implementing acts adopted by the Commission should be reviewed and if necessary updated on a regular basis. The assessment of the necessity of these updates should take into account new technologies, practices, standards or technical specifications emerged on the internal market.

(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 Council[16].

(38) Regulation (EU) 910/2014 should therefore be amended accordingly,

[16] 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).

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 at ensuring the proper functioning of the internal market and providing an adequate level of security of electronic identification means and trust services. For these purposes, this Regulation:

(aa) 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;

(ab) lays down the conditions under which Member States shall provide and recognise European Digital Identity Wallets;

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

(c) establishes a legal framework for electronic signatures, electronic seals, electronic time stamps, electronic documents, electronic registered delivery services, certificate services for website authentication, electronic validation of electronic signatures, electronic seals and their certificates, electronic validation of certificates for website authentication, electronic preservation of electronic signatures, electronic seals and their certificates, electronic archiving, electronic attestation of attributes, the management of remote qualified electronic signature and seal creation devices, and electronic ledgers;

(2) Article 2 is amended as follows:

(a) paragraph 1 is replaced by the following:

‘1. This Regulation applies to electronic identification schemes that have been notified by a Member State, European Digital Identity Wallets provided 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 national or Union law related to the conclusion and validity of contracts or other legal or procedural obligations relating to form or sector-specific requirements relating to form.’;

(3) Article 3 is amended as follows:

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

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

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

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

(aa) point (3) is replaced by the following:

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

(b) point (4) is replaced by the following:

‘(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 natural or legal persons;’;

(ba) point (5) is replaced by the following:

(5) ‘authentication’ means an electronic process that enables the electronic identification of a natural or legal person to be confirmed, or the origin and integrity of data in electronic form to be confirmed;

(bb) the following point (5a) is inserted:

(5a) ‘user’ means a natural or legal person, or a natural person representing a natural or legal person, using trust services or electronic identification means, provided according to this Regulation;

(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 for remuneration which consists of:

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

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

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

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

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

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

(f) the issuing of electronic attestations of attributes;

(fa) the validation of electronic attestation of attributes;

(g) the creation of electronic timestamps;

(ga) the validation of electronic timestamps;

(gb) the provision of electronic registered delivery services;

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

(h) the electronic archiving of electronic data; or

(i) the recording of electronic data into an electronic ledger;

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

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

(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 (23a) and (23b) are inserted:

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

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

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

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

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

‘(41) ‘validation’ means the process of verifying and confirming that data in electronic form are valid according to the requirements of this Regulation’;

(i) the following points (42) to (55b) are added:

‘(42) ‘European Digital Identity Wallet’ is an electronic identification means that allows the user to store and retrieve identity data, including person identification data, electronic attestations of attributes linked to their identity, to provide them to relying parties on request and to use them for authentication, online and, where appropriate, offline, for a service in accordance with Article 6a; and enables to sign by means of qualified electronic signatures and seal by means of qualified electronic seals;’;

(43) ‘attribute’ represents the characteristic, quality, right or permission of a natural or legal person or of an object;

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

(45a) ‘electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source’ means an electronic attestations of attributes issued by a public sector body responsible for an authentic source or by a public sector body designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45da and meeting the requirements laid down in Annex VII;

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

(47) ‘electronic archiving’ means a service ensuring the receipt, storage, retrieval and deletion of electronic data in order to guarantee their durability and legibility as well as to preserve their integrity, confidentiality and proof of origin throughout the preservation period;

(48) ‘qualified electronic archiving service’ means an electronic archiving service that meets the requirements laid down in Article 45ga;

(49) ‘EU Digital Identity Wallet Trust Mark’ means a verifiable indication in a simple, recognisable and clear manner that a European Digital Identity Wallet has been provided in accordance with this Regulation;

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

-(53) ‘electronic ledger’ means a sequence of electronic data records, which ensures their integrity and the accuracy of their chronological ordering’;

(53a) ‘qualified electronic ledger’ means an electronic ledger that meets the requirements laid down in Article 45i;

(54) ‘Personal data’ means any information as defined in point 1 of Article 4 of Regulation (EU) 2016/679’;

(55) ‘record matching’ means a process where person identification data, person identification means, qualified electronic attestation of attributes or attestations of attributes issued by or on behalf of a public sector body responsible for an authentic source are matched with or linked to an existing account belonging to the same person’;

(55a) 'unique and persistent identifier' means an identifier which may consist of either single or multiple national or sectoral identification data, is associated with a single user within a given system and persistent in time;

(55b) 'data record' means electronic data recorded with related meta-data (or attributes) supporting the processing of the data.

(55c) 'offline use of European Digital Identity Wallets' means an interaction between a user and a relying party at a physical location, whereby the Wallet is not required to access remote systems via electronic communication networks for the purpose of the interaction.

'*Article 5*

Pseudonyms in electronic transaction

Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.';

(5) in Chapter II the following heading is inserted before Article 6a:

'SECTION I

European Digital Identity Wallet;

(7) the following Articles (6a, 6b, 6c and 6d) 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, trusted and seamless cross-border access to public and private services, each Member State shall ensure that a European Digital Identity Wallet is provided within 24 months after the entry into force of the implementing acts referred to in paragraph 11 and Article 6c(4).

2. European Digital Identity Wallets shall be provided:

   (a) by a Member State;

   (b) under a mandate from a Member State; or

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

3. European Digital Identity Wallets are electronic identification means that shall enable the user in a manner that is transparent and traceable by the user to:

   (a) securely request, select, combine, store, delete and present electronic attestation of attributes and person identification data to relying parties, including to authenticate online and, where appropriate, offline in order to use public and private services, while ensuring that selective disclosure of data is possible;

   (b) sign by means of qualified electronic signatures and seal by means of qualified electronic seals.

4. European Digital Identity Wallets shall, in particular:

(a) provide a common set of interfaces:

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

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

(3) for the presentation to relying parties of person identification data or electronic attestation of attributes online and, where appropriate, also offline;

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

(b) not provide any information to trust service providers of electronic attestations of attributes about the use of these attributes after their issuance;

(ba) Ensure that the identity of relying parties can be validated by implementing authentication mechanisms in accordance with Article 6b;

(c) meet the requirements set out in Article 8 with regards to assurance level 'high'applicable mutatis mutandis to the management and use of person identification data through the Wallet, including electronic identification and authentication;

-(e) ensure that the person identification data referred to in Articles 12(4), point (d) uniquely and persistently represent the natural person, legal person or the natural person representing the natural or legal person, who is associated with the Wallet;

4a Member States shall provide for procedures to enable the user to report possible loss or misuse of their wallet and request its revocation.

5. Member States shall provide validation mechanisms for the European Digital Identity Wallets:

(a) to ensure that its authenticity and validity can be verified;

-(d) to allow the user to authenticate relying parties in accordance with Article 6b;

6. The European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance 'high'.

6a The issuance, use for authentication and the revocation of the European Digital Identity Wallets shall be free of charge to natural persons.

6b Without prejudice to Article 6db, Member States may provide, in accordance with national law, for additional functionalities of the European Digital Identity Wallets, including interoperability with existing national eID means.

7. The users shall be in full control of the use of the European Digital Identity Wallet and of the data in their European Digital Identity Wallet. The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it. Personal data relating to the provision of European Digital Identity Wallets shall be kept logically separate from any other data held by the issuer of European Digital Identity Wallets. If the European Digital Identity Wallet is provided by private parties in accordance to paragraph 2 (b) and (c), the provisions of article 45f paragraph 4 shall apply mutatis mutandis.

7a. Member States shall notify to the Commission, without undue delay information about:

(a) the body responsible for establishing and maintaining the list of notified relying parties that rely on the European Digital Identity Wallets in accordance with Article 6b(2);

(b) the bodies responsible for the provision of the European Digital Identity Wallets in accordance with Article 6a(1);

(c) the bodies responsible for ensuring that the person identification data is associated with the Wallet in accordance with Article 6a(4)(e);

The notification shall also provide information about the mechanism allowing for the validation of the person identification data referred to in Article 12(4) and of the identity of the relying parties.

The Commission shall make available to the public, through a secure channel, the information referred in this paragraph in electronically signed or sealed form suitable for automated processing.

8. Article 11 shall apply mutatis mutandis to the European Digital Identity Wallet.

9. Article 24(2), points (b), (e), (g), and (h) shall apply mutatis mutandis to the issuer of 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 Directive 2019/882.

11. Within 6 months of the entering into force of this Regulation, the Commission shall establish technical and operational specifications and reference standards for the requirements referred to in paragraphs 3, 4, 5 and 7a by means of an implementing act on the implementation of the European Digital Identity Wallet. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).

11a. The Commission shall establish technical and operational specifications as well as reference standards in order to facilitate the on-boarding to the European Digital Identity Wallet of users using either electronic identification means conforming to level 'high' or electronic identification means conforming to level 'substantial' in conjunction with additional remote on-boarding procedures that together meet the requirements of level of assurance 'high'. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 6b

European Digital Identity Wallets Relying Parties

1. Where relying parties that provide private or public services intend to rely upon European Digital Identity Wallets provided in accordance with this Regulation, they shall notify it to the Member State where the relying parties are established.

1a The notification procedure shall be cost-effective and proportionate-to-risk and ensure that relying parties provide at least the information necessary to authenticate to European Digital Identity Wallets. This should as a minimum include the Member State in which they are established and the name of the relying party and, where applicable, its registration number as stated in the official records.

1b The notification requirement shall be without prejudice to other notification and registration requirements in accordance with Union or national law such as those applicable to special categories of personal data, which may require additional authorisation requirements.

1c Member States may exempt relying parties from the notification requirement where Union or national law does not provide for specific notification or registration requirements in order to access information provided by means of the European Digital Identity Wallet. The exempted relying parties may not need to authenticate to the European Digital Identity Wallet.

1d Relying parties notified in accordance with this Article shall inform without delay the Member State about any subsequent change in the information initially provided.

2. Relying parties shall ensure the implementation of authentication mechanisms referred to in Article 6a(4)(ba).

3. Relying parties shall be responsible for carrying out the procedure for authenticating persons and validating electronic attestation of attributes originating from European Digital Identity Wallets obtained through the common interface according to Article 6a (4)(a)(2).

4. Within 6 months of the entering into force of this Regulation, the Commission shall establish technical and operational specifications for the requirements referred to in paragraphs 1, 1a and 1d by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(11). This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 6c

Certification of the European Digital Identity Wallets

1. The conformity of European Digital Identity Wallets with the requirements laid down in article 6a(3), (4), (5), with the requirement for logical separation laid down in paragraph Article 6a(7), and where applicable with the requirements laid down in Article 6a(11a), shall be certified by conformity assessment bodies accredited in accordance with Article 60 of the Cybersecurity Act and with the schemes, specifications, standards and procedures referenced in accordance with paragraph 4 points (a), (aa) and (aaa), and designated by Member States. The certification shall not exceed five years, conditional upon a regular two-year vulnerabilities assessment. Where vulnerabilities are identified and not remedied within three months, the certification shall be cancelled.

2. As regards compliance with the data protection requirements under Article 6a(7), the certification under paragraph 1 may be complemented by a certification pursuant to Article 42 of Regulation (EU) 2016/679.

3. The conformity of the European Digital Identity Wallets, or parts thereof, with the cybersecurity relevant requirements set out in Article 6a(3), (4), (5), (7) and where applicable (11a), shall be certified by the conformity assessment bodies referred to in paragraph 1, under relevant cybersecurity certification schemes pursuant to Regulation (EU) 2019/881 as they are referenced in accordance with paragraphs 4(a) and 4(aa).

3a. Certified European Digital Identity Wallets shall not be subject to the requirements referred to in Articles 7 and 9.

4. Within 6 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish:

a) a list of cybersecurity certification schemes pursuant to Regulation (EU) 2019/881, required for the certification of the European Digital Identity Wallets as referred to in paragraph 3;

aa) specifications, procedures and reference standards for their use under relevant cybersecurity certification schemes listed in accordance to point (a);

aaa) a list of specifications, procedures and reference standards establishing common certification requirements not covered by relevant cybersecurity certification schemes pursuant to Regulation (EU) 2019/881 for the purpose of certification referred to in paragraph 1 aiming to demonstrate that a European Digital Identity Wallet meets the requirements as referred to in paragraph 1;

b) technical, procedural, organisational and operational specifications for the designation of conformity assessment bodies referred to in paragraph 1, and, for what regards the certification requirements established pursuant to point (aaa), for the monitoring and review of the certification schemes and related-evaluation methods these bodies use and the certificates and certification reports they issue;

5. Member States shall communicate to the Commission the names and addresses of the public or private bodies referred to in paragraph 1. The Commission shall make that information available to Member States.

6. Implementing acts referred to in paragraph 4 shall be adopted in accordance with the examination procedure referred to in Article 48(2).

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 provided pursuant to Article 6a and certified by the bodies referred to in Article 6c paragraph 1. They shall also inform the Commission, without undue delay where the certification is cancelled.

2. On the basis of the information received, the Commission shall establish, publish and update a machine-readable list of certified European Digital Identity Wallets.

3. Within 6 months of the entering into force of this Regulation, the Commission shall define formats and procedures applicable for the purposes of paragraph 1 and 2 by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(11). This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 6da

Security breach of the European Digital Identity Wallets

1. Where European Digital Identity Wallets provided pursuant to Article 6a or the validation mechanisms referred to in Article 6a(5) points (a), (d) or (e) are breached or partly compromised in a manner that affects their reliability or the reliability of other European Digital Identity Wallets, the issuer of the concerned wallets shall, without undue delay, suspend the issuance and the use of the European Digital Identity Wallet. The Member State where concerned Wallets were provided shall inform the Member States and the Commission without undue delay. The issuer of the concerned Wallets or Member state shall inform relying parties and the users accordingly.

2. Where the breach or compromise referred to in paragraph 1 is remedied, the issuer of the Wallet shall re-establish the issuance and the use of the European Digital Identity Wallet. The Member State where concerned Wallets were provided shall inform Member States and the Commission without undue delay. The issuer of the concerned Wallets or Member state shall inform relying parties and the users without undue delay.

3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension, the Member State concerned shall withdraw the European Digital Identity Wallet concerned and inform the other Member States and the Commission accordingly. Where it is justified by the severity of the breach, the European Digital Identity Wallet concerned shall be withdrawn without undue delay.

4. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 6d without undue delay.

5. Within 6 months of the entering into force of this Regulation, the Commission shall further specify the measures referred to in paragraphs 1, 2 and 3 by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(11). This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 6db

Cross-border reliance on European Digital Identity Wallets

1. Where Member States require an electronic identification using an electronic identification means and authentication to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets provided in compliance with this Regulation for authentication of the user.

2. Where private relying parties providing services, with the exception of microenterprises and small enterprises as defined in Commission Recommendation 2003/361/EC, are required by national or Union law to use strong user authentication for online identification, or where strong user authentication is required by contractual obligation, including in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, private relying parties shall, no later than 12 months after the date of provision of European Digital Identity Wallets pursuant to Article 6a(1) and strictly upon voluntary request of the user, also accept the use of European Digital Identity Wallets provided in accordance with this Regulation in respect of the minimum data necessary for the specific online service for which authentication of the user is requested.

3. Where very large online platforms as defined in Article 25(1) of Regulation [reference to DSA Regulation] require users to authenticate to access online services, they shall also accept the use of European Digital Identity Wallets provided in accordance with this Regulation for authentication of the user strictly upon voluntary request of the user and in respect of the minimum data necessary for the specific online service for which authentication is requested.

4. In cooperation with Member states the Commission shall encourage and facilitate the development of 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 facilitate 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.

5. The Commission shall make an assessment within 24 months after deployment of the European Digital Identity Wallets whether on the basis of evidence showing demand, availability and usability of the European Digital Identity Wallet, additional private online service providers shall be mandated to accept the use of the European Digital identity Wallet strictly upon voluntary request of the user. Criteria of assessment shall include extent of user base, cross-border presence of service providers, technological development, evolution in usage patterns, and consumer demand.

(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 which have not yet done so shall notify, within 24 months after the entry into force of the implementing acts referred to in Article 6a(11) and Article 6c(4) at least one electronic identification scheme including at least one identification means of level of assurance 'high'. An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) provided that all of the following conditions are met:';

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

'2. The Commission shall 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.';

(12) the following Article 11a is inserted:

'*Article 11a*

Record matching

1. When notified electronic identification means or European Digital Identity Wallets are used for authentication, Member States when acting as relying parties shall ensure record matching.

2. Member States shall, for the purposes of providing European Digital Identity Wallets, include in the minimum set of person identification data referred to in Article 12(4) point (d), at least one unique and persistent identifier in conformity with Union and national law, to identify the user upon their request in those cases where identification of the user is required by law.

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

2aa. Member States may provide, in accordance with national law, that the user of European Digital Identity Wallet shall be able to request that a unique and persistent Identifier included in the minimum set of person identification data and associated with the wallet in accordance with Article 6a(4)(e) is replaced by another unique and persistent identifier issued by the Member State.

3. Within 6 months of the entering into force of this Regulation, the Commission shall further specify the measures referred to in paragraph 1 by means of an implementing act. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).

3a Within 6 months of the entering into force of this Regulation, the Commission shall detail the measures referred to in paragraph 2 and 2aa by means of an implementing act. This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).

(13) Article 12 is amended as follows:

Cooperation and interoperability

(a) in paragraph 3, point (d) is deleted;

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

‘(d) a reference to a minimum set of person identification data necessary to uniquely and persistently represent a natural person, legal person or a natural person representing natural or legal persons;’;

(ba) in paragraph 5, point (c) is inserted:

‘(c) similar approach towards online services accepting the use of European Digital Identity Wallets provided in accordance with this Regulation;’;

(c) in paragraph 6, point (a) of is replaced by the following:

‘(a) the exchange of information, experience and good practice as regards electronic identification schemes and in particular technical requirements related to interoperability, record matching and assurance levels;’;

(ca) in paragraph 6, point (e) is inserted:

‘(e) the exchange of information, experience and good practises and the issuing of guidelines as regards how online services may be designed, developed and implemented for the purpose of relying on the European Digital Wallets’

(14) the following Article 12a and 12b are inserted:

'*Article 12a*

Certification of electronic identification schemes

1. Conformity of electronic identification schemes to be notified with the requirements laid down in this Regulation shall be certified to demonstrate compliance of such schemes or parts thereof with the requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes under a relevant cybersecurity certification scheme pursuant to Regulation (EU) 2019/881 or parts thereof, in so far as the cybersecurity certificate or parts thereof cover the requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes. The certification shall not exceed five years, conditional upon a regular two-year vulnerabilities assessment. Where vulnerabilities are identified and not remedied within three months, the certification shall be cancelled.

   The certification shall be carried out by accredited public or private conformity assessment bodies designated by Member States and in accordance with Regulation (EC) No 765/2008.

2. The peer-review of electronic identification schemes referred to in Article 12(6), point (c) shall not apply to electronic identification schemes or to part of such schemes certified in accordance with paragraph 1.

2a. Notwithstanding paragraph 2 of this Article, Member States may request additional information about electronic identification schemes or part thereof certified according to paragraph 2 of this Article from a notifying Member State.

3. Member States shall notify to the Commission the names and addresses of the public or private body referred to in paragraph 1. The Commission shall make that information available to Member States.';

‘Article 12b

Access to hardware and software features

Issuers of European Digital Identity Wallets and issuers of notified electronic identification means acting in a commercial or professional capacity and using core platform services as defined in Article 2(2) of Regulation (EU) 2022/1925 for the purpose of, or in the course of, providing European Digital Identity Wallet services and electronic identification means to end-users are business users in accordance with Art. 2(21) of Regulation (EU) 2022/1925.

(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’;

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

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

(18) Article 14 is replaced by the following:

'*Article 14*

International aspects

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

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

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

3. The implementing decisions referred to in paragraph 1 shall be adopted in accordance with the examination procedure referred to in Article 48(2).

(19) Article 15 is replaced by the following:

'*Article 15*

Accessibility for persons with disabilities

The provision of Trust services and end-user products used in the provision of those services shall be made accessible for persons with disabilities in accordance with the accessibility requirements of Directive 2019/882 on the accessibility requirements for products and services.';

(20) Article 17 is amended as follows:

(a) paragraph 4 is amended as follows:

(1) point (c) of paragraph 4 is replaced by the following:

'(c) 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. Where the significant breach of security or loss of integrity concerns other Member States, the supervisory body shall inform the single point of contact of the Member State concerned designated pursuant to Directive (EU) XXXX/XXXX (NIS2) and the supervisory bodies designated pursuant to Article 17 of this Regulation in the other Member States concerned. The notified supervisory body shall inform the public or require the trust service provider to do so where it determines that disclosure of the breach of security or loss of integrity is in the public interest;';

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

‘(f) to cooperate with competent supervisory authorities established under Regulation (EU) 2016/679, in particular, by informing them without undue delay if personal data protection rules appear to have been breached and about security breaches which appear to constitute personal data breaches;’;

(b) paragraph 6 is replaced by the following:

‘6. By 31 March each year, each supervisory body shall submit to the Commission a report on its main activities during the previous calendar year.’;

(c) paragraph 8 is replaced by the following:

‘8. Within 12 months of the entering into force of this Regulation, the Commission shall adopt guidelines on the exercise by the Supervisory bodies of the tasks referred to in paragraph 4, and, by means of implementing acts adopted in accordance with the examination procedure referred to in Article 48(2), define the formats and procedures for the report referred to in paragraph 6.’;

(21) Article 18 is amended as follows:

(a) the title of Article 18 is replaced by the following:

‘Mutual assistance and cooperation’;

(b) paragraph 1 is replaced by the following:

‘1. Supervisory bodies shall cooperate with a view to exchanging good practice and information regarding the provision of trust services.’;

(c) the following paragraphs 4 and 5 are added:

‘4. Supervisory bodies and national competent authorities under Directive (EU) XXXX/XXXX of the European Parliament and of the Council [NIS2] shall cooperate and assist each other to ensure that trust service providers comply with the requirements laid down in this Regulation and in Directive (EU) XXXX/XXXX [NIS2]. Supervisory bodies shall request national competent authorities under Directive XXXX/XXXX [NIS2] to carry out supervisory actions to verify compliance of the trust service providers with the requirements under Directive XXXX/XXXX (NIS2), to require the trust service providers to remedy any failure to comply with those requirements, to provide timely the results of any supervisory activities linked to trust service providers and to inform the supervisory bodies about relevant incidents notified in accordance with Directive XXXX/XXXX [NIS2].

5. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Supervisory Authorities referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(21a) The following Article 19a is inserted:

'Requirements for non-qualified trust service providers'

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

(a) have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the provision of the non-qualified trust service. 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.

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

2. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, specify the technical characteristics of the measures referred to in paragraph 1(a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

(22) Article 20 is amended as follows:

(a) paragraph 1 is replaced by the following

‘1. Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The audit shall confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation and in Article 18 of Directive (EU) XXXX/XXXX [NIS2]. Qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within three working days of receipt.’;

(aa) the following paragraph is inserted:

1a. Member States may provide that qualified trust service providers shall inform in advance the supervisory body about planned audits and allow for the participation of the supervisory body as an observer upon request.

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

‘Where personal data protection rules appear to have been breached, the supervisory body shall, without undue delay, inform the competent supervisory authorities under Regulation (EU) 2016/679.’;

(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, 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, may withdraw the qualified status of that provider or of the affected service it provides.

3a. Where the supervisory body is informed by the national competent authorities under Directive (EU) XXXX/XXXX [NIS2] that the qualified trust service provider fails to fulfil any of the requirements set out by Article 18 of Directive (EU) XXXX/XXXX [NIS2], the supervisory body, taking into account in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides.

3b. Where the supervisory body is informed by the supervisory authorities under Regulation (EU) 2016/679 that the qualified trust service provider fails to fulfil any of the requirements set out by Regulation (EU) 2016/679, the supervisory body, taking into account in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides.

3c. The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned. The supervisory body shall inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1) and the national competent authority referred to in Dir XXXX [NIS2].

4. Within 12 months of the entering into force of this regulation, the Commission shall, by means of implementing acts, establish technical specifications and reference numbers of standards for the following:

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

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

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

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

(23) Article 21 is amended as follows:

‘1. Where trust service providers intend to start providing a qualified trust service, they shall submit to the supervisory body a notification of their intention together with a conformity assessment report issued by a conformity assessment body confirming the fulfilment of the requirements laid down in this Regulation and in Article 18 of Directive (EU) XXXX/XXXX [NIS2].’;

(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 without undue delay, and no later than two months from the receipt of this request by the competent authorities referred to in Dir XXXX [NIS2]. If the verification is not concluded within two months of the notification, the competent authorities referred to in Dir XXXX [NIS2] shall inform the supervisory body specifying the reasons for the delay and the period within which the verification is to be concluded.

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

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

(b) paragraph 4 is replaced with the following:

'4. Within 12 months of the entering into force of this 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. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(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, a qualified trust service provider shall verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of attributes will be 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 the European Digital Identity Wallet or 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 qualified electronic attestations of attributes or a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a), (c) or (d);

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

(d) through the physical presence of the natural person or of an authorised representative of the legal person by appropriate procedures and in accordance with national laws.’;

(b) the following paragraph 1a is inserted:

‘1a. Within 12 months after the entry into force of this Regulation, the Commission shall by means of implementing acts, set out minimum technical specifications, standards and procedures with respect to the verification of identity and attributes in accordance with paragraph 1, point c. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).’;

(c) paragraph 2 is amended as follows:

(0) point (a) is amended as follows:

‘(a) inform the supervisory body at least one month before implementing any change in the provision of its qualified trust services or at least three months in case of an intention to cease those activities. The supervisory body may request additional information or the result of a conformity assessment before granting the permission to implement the intended changes to the qualified trust services. If the verification is not concluded within three months of notification, the supervisory body shall inform the trust service provider, specifying the reasons for the delay and the period within which the verification is to be concluded.

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

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

‘(e) use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them, including using suitable cryptographic algorithms, key lengths and hash functions in the systems, products and in the processes supported by them;’;

(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, the identifiable affected individuals, other relevant competent bodies where applicable and, at the request of the supervisory body, the public if it is of public interest, of any breaches or disruptions in the provision of the service or the implementation of the measures referred to in paragraph (fa), points (i), (ii) and, (iii) that have a significant impact on the trust service provided or on the personal data maintained therein, without undue delay and in any case no later than 24 hours after the incident.’;

(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 qualified electronic attestations of attributes.’;

(e) paragraph 5 is replaced by the following:

‘5. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish technical specifications, procedures and reference numbers of standards for the requirements referred to in paragraph 2. Compliance with the requirements laid down in this Article shall be presumed, where those technical specifications, procedures and standards are met. 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 implementing acts specifying the technical characteristics of the measures referred to in paragraph 2(fa).’;

(25a) Article 26 is amended as follows:

2. Within 12 months after the entry into force of this Regulation, the Commission shall, by means of implementing acts, establish technical specifications and reference numbers of standards for advanced electronic signatures. Compliance with the requirements for advanced electronic signatures shall be presumed when an advanced electronic signature meets those specifications and standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

(25b) Article 27 is amended as follows:

Paragraph 4 is deleted.

(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 technical specifications and 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 specifications and 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 electronic signature creation data on behalf of the signatory or duplicating such signature creation data for back-up purposes may only be done by a qualified trust service provider providing a qualified trust service for the management of a remote qualified electronic signature creation device.’;

(28) The following Article 29a is inserted:

‘*Article 29a*

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

1. The management of remote qualified electronic signature creation devices as a qualified service 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, may duplicate 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. Within 12 months of the entering into force of this 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 validity of a certification referred to in paragraph 1 shall not exceed 5 years, conditional upon a regular 2 year vulnerabilities assessment. Where vulnerabilities are identified and not remedied, the certification shall be cancelled.';

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

‘3. Within 12 months of the entering into force of this 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 specifications and standards referred to in paragraph 3.’;

(b) paragraph 3 is replaced by the following:

‘3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, provide specifications and 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).’;

(31a) The following Article 32a is inserted:

Requirements for the validation of advanced electronic signatures based on qualified certificates

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

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

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

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

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

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

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

(g) the requirements provided for in Article 26 were met at the time of signing. Compliance with the requirements laid down in the first sub-paragraph shall be presumed where the validation of advanced electronic signatures based on qualified certificates meet the specifications and standards referred to in paragraph 3.

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

3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, provide specifications and reference numbers of standards for the validation of advanced electronic signatures based on qualified certificates. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).'

(31b) Article 33 is amended as follows:

‘1. A qualified validation service for qualified electronic signatures may only be provided by a qualified trust service provider who:’;

‘2. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish technical specifications and reference numbers of standards for qualified validation service referred to in paragraph 1. Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation service for a qualified electronic signature meets those specifications and standards. 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 specifications and standards referred to in paragraph 3.

3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish technical specifications and 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).’;

(32a) In Article 36 a new paragraph 2 is added:

2. Within 12 months after the entry into force of this Regulation, the Commission shall, by means of implementing acts, establish technical specifications and reference numbers of standards for advanced electronic seals.

Compliance with the requirements for advanced electronic seals shall be presumed when an advanced electronic seal meets those specifications and standards. 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:

Paragraph 4 is deleted.

(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 specifications and standards referred to in paragraph 6.’;

(b) paragraph 6 is replaced by the following:

‘6. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish technical specifications and 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 39a is inserted:

'*Article 39a*

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

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

(35a) the following Article 40a is inserted:

'*Article 40a*

Requirements for the validation of advanced electronic seals based on qualified certificates

(1) Article 32a shall apply mutatis mutandis to the validation of advanced electronic seals based on qualified certificates.';

(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 specifications and standards referred to in paragraph 2.';

(b) paragraph 2 is replaced by the following

'2. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish technical specifications and 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).';

(36a) In Article 43 a new paragraph 3 is added:

2a. A qualified electronic registered delivery service in one Member State shall be recognised as a qualified electronic registered delivery service in any other Member State.';

(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 specifications and standards referred to in paragraph 2.';

(b) paragraph 2 is replaced by the following:

'2. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, establish technical specifications and 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).';

(c) the following paragraph 3 and 4 are inserted:

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

‘4. The Commission may, by means of implementing act, establish technical specifications and reference numbers of standards in order to facilitate the transfer of data between two or more qualified trust service providers. The technical specifications and content of standards shall be cost-effective and proportionate. The implementing act 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 meet the requirements laid down in Annex IV. Evaluation of compliance with the requirements laid down in Annex IV shall be carried out in accordance with the specifications and standards referred to in paragraph 4.

2. Qualified certificates for website authentication referred to in paragraph 1 shall be recognised by web-browsers. For those purposes web-browsers shall ensure that the identity data provided using any of the methods is displayed in a user friendly manner. 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.

4. Within 12 months of the entering into force of this 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.

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

3. 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.

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

Article 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. In such a case, qualified electronic attestation of attributes from other Member States shall also be accepted.

Article 45c

Requirements for qualified electronic attestation of attributes

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

1a. Evaluation of compliance with the requirements laid down in Annex V shall be carried out in accordance with the specifications and standards referred to in paragraph 4.

2. Qualified electronic attestations of attributes shall not be subject to any mandatory 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.

4. Within 6 months of the entering into force of this Regulation, the Commission shall establish technical specifications and 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 within 24 months after entry into force of the implementing acts referred to in Article 6a(11) and Article 6c(4) 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 these attributes by electronic means at the request of the user and in accordance with national or Union law.

2. Within 6 months of the entering into force of this Regulation, taking into account relevant international standards, the Commission shall 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).

Article 45da

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

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

a) the requirements set out in Annex VII;

b) the qualified certificate supporting the qualified electronic signature or qualified electronic seal of the public sector body referred to in Article 3 (45a) identified as the issuer referred to in point (b) of Annex VII, shall contain a specific set of certified attributes in a form suitable for automated processing:

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

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

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

2. The Member State where the public sector bodies referred to in Article 3(45a) are established shall ensure that the public sector bodies that issue electronic attestations of attributes meet the equivalent level of reliability as qualified trust service providers in accordance with Article 24.

2a. Member States shall notify the public sector bodies referred to in Article 3 (45a) to the Commission. This notification shall include a conformity assessment report issued by a conformity assessment body confirming that the requirements set out in paragraphs 1, 2 and 6 of this Article are met. The Commission shall make available to the public, through a secure channel, the list of the public sector bodies referred to in Article 3 (45a) in electronically signed or sealed form suitable for automated processing.

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

4. An electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source shall be deemed compliant with the requirements laid down in paragraph (1) of this Article, where it meets the standards referred to in paragraph (5).

5. Within 6 months of the entering into force of this Regulation, the Commission shall establish technical specifications and reference numbers of standards for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source, by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(11).

5a. Within 6 months of the entering into force of this Regulation, the Commission shall define formats, procedures, specifications and standards for the purposes of paragraph 2a by means of an implementing act on the implementation of European Digital Identity Wallets as referred to in Article 6a(11).

6. Public sector bodies referred to in Article 3(45a) issuing electronic attestation of attributes shall provide an interface with the European Digital Identity Wallets provided in accordance with Article 6a.

Article 45e

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

Providers of qualified electronic attestations of attributes shall provide an interface with the European Digital Identity Wallets provided in accordance in Article 6a.

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 or their commercial partners.

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

4. Providers of qualified electronic attestation of attributes' services shall implement functional separation for providing such services.

SECTION 10

ELECTRONIC ARCHIVING SERVICES

Article 45g

Legal effect of an electronic archiving service

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

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

3. A qualified electronic archiving service in one Member State shall be recognised as a qualified electronic archiving service in any other Member State.

Article 45ga

Requirements for qualified electronic archiving services

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

   (a) They are provided by qualified trust service providers

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

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

(d) They shall allow authorised relying parties to receive a report in an automated manner that confirms that an electronic data retrieved from a qualified electronic archive enjoys the presumption of integrity of the data from the beginning of the preservation period to the moment of retrieval. This report shall be provided in a reliable and efficient way and it shall bear the qualified electronic signature or qualified electronic seal of the provider of the qualified electronic archiving service;

2. Within 12 months after the entry into force of this Regulation, the Commission shall, by means of implementing acts, establish technical specifications and reference numbers of standards for qualified electronic archiving services. Compliance with the requirements for qualified electronic archive services shall be presumed when a qualified electronic archive service meets those specifications and standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 11

ELECTRONIC LEDGERS

Article 45h

Legal effects of electronic ledgers

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

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

3. A qualified electronic ledger in one Member State shall be recognised as a qualified electronic ledger in any other Member State.

Article 45i

Requirements for qualified electronic ledgers

1. Qualified electronic ledgers shall meet the following requirements:

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

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

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

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

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

3. The Commission shall, by means of implementing acts, establish technical specifications and reference numbers of standards for the creation and operation of a qualified electronic ledger. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

(40) The following Article 48a 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 once they are provided on their territory.

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

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

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

   (c) summary report including data on incidents preventing the use of the European Digital Identity Wallet.

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

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

(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 within 36 months after its entering into force. The Commission shall evaluate in particular the scope of Article 6 and Article 6db and 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 customer demand, 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 and usability of the 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 the European Digital Identity Wallets.

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 36 months 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 24 months following the entry into force of this Regulation.'.

2a. The management of remote qualified electronic signature and seal creation devices by qualified trust service providers other than qualified trust service providers providing qualified trust services for the management of remote qualified electronic signature and seal creation devices in accordance with Articles 29a and 39a shall continue to be considered without the need to obtain the qualified status for the provision of these management services until 24 months following the entry into force of this Regulation.

2b. Qualified trust service providers that have been granted their qualified status under this Regulation before [date of entry into force of the amending Regulation], using methods for identity verification for the issuance of qualified certificates in compliance with Article 24(1), shall submit a conformity assessment report to the supervisory body proving compliance with Article 24(1) as soon as possible but not later than 30 months after entry into force of the amending Regulation. Until the submission of such a conformity assessment report and the completion of its assessment by the supervisory body, the qualified trust service provider may continue to rely on the use of the methods for identity verification set out in Article 24(1) of Regulation (EU) No 910/2014.

(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 52

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 Brussels,

For the European Parliament	For the Council
The President	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;’.

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:

   (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;’.

ANNEX IV

In Annex IV, 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:

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

(f) 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;

(g) 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;

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

(i) details of the beginning and end of the attestation’s period of validity;

(j) 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;

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

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

(m) 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 national or Union law and in cases where these attributes rely on authentic sources within the public sector:

1. Address;
2. Age;
3. Gender;
4. Civil status;
5. Family composition;
6. Nationality or citizenship;
7. Educational qualifications, titles and licenses;
8. Professional qualifications, titles and licenses;
9. Public permits and licenses;
10. Financial and company data.

ANNEX VII

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

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

a) an indication, at least in a form suitable for automated processing, that the attestation has been issued as an electronic attestation of attributes issued by or on behalf of a public body responsible for an authentic source;
b) a set of data unambiguously representing the public body issuing the electronic attestation of attributes, including at least, the Member State in which that public body is established and its name and, where applicable, its registration number as stated in the official records;
c) a set of data unambiguously representing the entity 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 issuing public body 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 body;
h) the location where the certificate supporting the qualified electronic signature or qualified electronic seal referred to in point (g) is available free of charge;
i) the information or location of the services that can be used to enquire about the validity status of the attestation.

_____