Council of the European Union

Brussels, 20 September 2022
(OR. en)

12532/22

Interinstitutional File:
2021/0136(COD)

LIMITE

TELECOM 370
COMPET 711
MI 666
DATAPROTECT 255
JAI 1191
CODEC 1313

NOTE

From:	Presidency
To:	Delegations
No. prev. doc.:	11713/22
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 – Fourth compromise proposal

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.

2. Discussions were initiated by the PT Presidency during the meeting of 17 June 2021, with the first reading being successfully completed under the SI Presidency on 15 November 2021.

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

3. The FR Presidency presented its first compromise proposal on 15 February and 5 April, with a second one being discussed on 23 May and 9 June.

4. Further to a third round of comments from delegations and the policy orientation debate on 19 July, the CZ Presidency presented a third compromise proposal during the WP TELECOM meetings of 5 and 8 September.

5. The fourth compromise proposal, to be found in the annex of this document, stems from additional comments and drafting suggestions received from delegations in September. The CZ Presidency invites the delegations to **discuss the proposed changes** to the EU eID proposal during the WP TELECOM meeting of **28 September**.

6. The changes in the document compared to the third compromise proposal are underlined: additions are marked with **bold text**, deletions with ~~strikethrough~~. Elements that require further discussion are marked with **[square brackets]**. Previous changes, thus compared to the original Commission's proposal or previous compromise proposals, are still marked as described above but are no longer underlined.

II. MAIN CHANGES

7. Fees

   A minor addition has been inserted in **Recital (9)**, stating that the list of examples of subsequent use of the Wallet that may incur costs is non-exhaustive. The reference to 'sole' use of the Wallet has been removed from **Article 6**, as this term was deemed confusing.

8. Selective disclosure

   Recital (29) has been expanded to elaborate on the concept of selective disclosure of data and to acknowledge that selectively disclosed attributes, including when originally part of distinct electronic attestations, may be subsequently combined and presented to relying parties, thereby contributing to the protection of personal data by data minimization — it should be possible to share and combine attributes from several attestations of attributes in order not to share more attributes than what is required for the provision of particular service.

9. Certification of qualified electronic sign/seal creation device

It was suggested to clarify in **Recital (31a)** that public or private bodies that have certified qualified electronic signature creation devices could temporarily extend the validity of certification in specific cases, when the recertification of the same device could not be performed within the time-frame. The proposal is intended for discussion.

10. Ledgers

Based on remarks made by Member States, **Recitals (34)** and **(35)** have been complemented with examples of use of electronic ledgers in public digital services and an explanation of the relationship with the Transfer of Funds Regulation.

11. State-of-the-art cryptographic algorithms

Based on suggestion of some Member States, **Recital (36d)** has been added in order to reflect that qualified trust service providers issuing qualified certificates should support state-of-the-art cryptographic algorithms. The proposal is intended for discussion.

12. Definitions of 'user' and 'electronic identification means'

The definition of 'user' in **Article 3(5a)** no longer includes the reference to European Digital Wallets, which was only kept in the definition of 'electronic identification means' (**Article 3(2)**) and of the EDIW itself (**Article 3(42)**) for clarity and consistency.

13. Definition of 'European Digital Identity Wallet'

The CZ Presidency has proposed minor corrections in the definition of 'European Digital Identity Wallet' in **Article 3(42)**. It is now clarified that Wallets should allow the user to store as well as retrieve identity data and electronic attestation of attributes. The definition was also aligned with **Article 6a(3)(b)** with regard to allowing of signing / sealing.

14. Archiving

Minor adjustments have been proposed in relation to electronic archiving in **Recital (33)** and **Article 3(47)** at the request of delegations. The CZ Presidency would like to clarify that the Regulation does not by any means mandate national public archives and memory institutions to become a qualified trust service provider. Similarly, the CZ Presidency is of the view that the above mentioned institutions may benefit from the exemption from scope under **Article 2(2)**,

thus they should not be considered as non-qualified trust service providers when providing their services to another public body within closed systems resulting from national law.

15. Strong user authentication

The definition of 'strong user authentication' in **Article 3(50)** was previously aligned with a corresponding definition in PSD2 Directive. Given a number of request from delegations to clarify that strong user authentication should be performed by using at least two different authentication factors belonging to distinct categories of knowledge, possession and inherence, the CZ Presidency has amended the definition accordingly. Further adjustments have been made in **Recital (11a)** in relation to processing of biometric data as an authentication factor.

16. Management of trusted lists of relying parties

Given a number of questions on how the evidence of eligible relying parties will be maintained, the CZ Presidency has proposed to introduce new paragraph 7a under **Article 6a**. According to the provision, Member States should notify to the Commission information about the list of eligible relying parties. The Commission subsequently would make that information available to the public through a secure channel and in a form suitable for automated processing.

17. Clarification of **Article 6a(11a)** and relation to certification

The wording of **Article 6a(11a)** on the remote on-boarding procedures has been slightly adjusted and references to this provision have been added to **Article 6c(1)** and **(3)**. The aim of this change is to establish a clear link between certification of Wallets and methods of on-boarding used for identity proofing that meet the requirements of level of assurance 'high'.

18. Deletion of **Article 6a(5)(e)**

In order not to impose an excessive burden on Member States, the obligation to ensure consistency of the use of European Digital Identity Wallets with the intended use notified under **Article 6b** by relying parties has been deleted.

19. Registration of relying parties & Recital (8)

Following the exchange of views in WP TELE meeting on September 5 and Member States written suggestions, the Presidency has proposed to further amend the provisions of **Article 6b** and **Recital (8)**, now referring to notification procedure instead of to registration. It has been clarified that the notification process is meant to be driven by sectoral Union or national laws to

accommodate various use cases differing in terms of registration requirements, of mode of online/offline operation, or in terms of the requirement to authenticate devices. Furthermore, Member States should decide on eligibility of the notifying party that intends to rely on European Digital Identity Wallets. The aim of the new wording is provide for a balanced approach to notification and consequently, to approval of relying parties, while allowing for reflection of specific requirements of individual use cases. For instance, the notification of all law enforcement forces and officers may rely on the existing registration of all law enforcement forces and may be ensured at legislation level. Relying on existing registers in the public sector should be fully sufficient as reference. Delegations are kindly invited to share their views on the new text, notably should the wording not be acceptable.

20. Exemption from notification of offline use

The safeguarding of exemption of offline use of the Wallet from the notification procedure under **Article 6b(1)** has been amended. The definitions of 'offline use of European Digital Identity Wallets' in **Article 3(55c)** and 'fully offline use of European Digital Identity Wallets' in **Article 3(55d)** have been renamed to 'hybrid use of European Digital Identity Wallets' and 'offline use of European Digital Identity Wallets' respectively, and modified based on the written suggestions. Furthermore, **Recital (8a)** now clarifies that a minimum set of information about the relying party and the devices used should be obtained and maintained also in case of an offline use of the Wallet, where possible in an automated or semi-automated manner, to allow intervention of a competent body when needed. Due to the changes made in **Article 6b(1)** and **Recital (8)**, the CZ Presidency is of the view that a specific requirements of offline use of the Wallet may be already covered by the general provision on notification procedures, thereby an exemption for offline use case may become unnecessary. Nonetheless, given a prevailing support of the exemption by Member States, the CZ Presidency has decided to place **Article 6b(1a)** and **Recital (8a)** into square brackets and to invite delegations to kindly express their opinion as to whether this wording should be kept or deleted. Throughout the text, the CZ Presidency has suggested to use 'where appropriate' when referring to offline use cases of Wallets. The reasoning provided by some Member States is that many services may not benefit from offline use of Wallets, hence the wording should not create the impression that Wallets must be usable offline in all cases. The definition of electronic identification means has been changed accordingly.

21. Changes to certification provisions under **Article 6c**

Following advice of the Commission, the CZ Presidency has proposed to amend **Article 6c(2)**. The purpose of certification of European Digital Identity Wallets is to ensure a common level of trust in their implementation by Member States. This certification is meant to include privacy requirements set out in **Article 6a(7)**, which will be further specified in implementing act under **Article 6a(11)** and conformity assessment bodies will have to assess conformity of European Digital Identity Wallets with the requirements laid down in the eIDAS framework. This system will ensure that privacy principles are directly set under the eIDAS Regulation on Wallets issuers without overlap with GDPR requirements that already apply. The CZ Presidency is of the view that GDPR certification under Article 42 GDPR should not be referenced, as it does not bear the same legal consequences as the certification of Wallets established in the proposal. In fact, GDPR certification following under Article 42 GDPR does not provide for a presumption of conformity. In addition, the process would add considerable burden to Member States with the involvement of national DPAs and courts. Additional changes have been made to **Article 6c**. As the CZ Presidency has received only a limited number of responses on period of certification under **Article 6c(1)**, the provision remains in square brackets and delegations are kindly invited to express their views on keeping it.

22. Streamlining of record matching

References to administrative practice have been removed throughout **Article 11a** on record matching. The reference to accordance with Union and national law has been deleted from **Article 11a(1)** as the necessity to comply by a Member State acting in its capacity as a relying party was considered to be self-evident. Safeguarding in **Article 11a(2a)** has been slightly reworded based on suggestions from delegations. Empowerment in **Art 6a(3)** has been modified to be more general and not aimed only for implementation of Wallets since paragraph 1 of the Article refers to notified electronic identification means or the European Digital Identity Wallets. Only minor changes have been proposed in **Recital (17a)**.

23. **Article 12 & Recital (17aa)**

As suggested in a non-paper by a Member State, the CZ Presidency has proposed to extend the scope of **Article 12** by including non-binding guidelines on exchanging information, experience and good practices as regards the design, development and implementation of online services where European Digital Identity Wallets should be accepted. Although the CZ Presidency considers the addition beneficial, respective provisions under **Article 12** and the

newly added **Recital (17aa)** are put in square brackets due to the fact that there has not been a proper discussion on this subject in WP so far.

24. Certification of eID schemes under **Article 12a**

The wording of **Article 12a** has been improved to clarify that compliance with the requirements regarding assurance levels of electronic identity schemes may be certified. Such compliance may be demonstrated via a relevant cybersecurity certification scheme pursuant to Regulation (EU) 2019/881, in so far as the cybersecurity certificate covers the requirements regarding assurance levels, or by other relevant national certification schemes. To the extent conformity is demonstrated by certification, the peer-review mechanism under **Article 12(6)** does not apply.

25. **Articles 26** & **36** ("may" v. "shall")

The empowerment for the Commission to establish reference numbers of standards for advanced electronic signatures and advanced electronic seals in **Articles 26** and **36** has been made mandatory based on Member States' preferences.

26. Commission empowerment

Article 32(3) on empowerment was slightly broadened in order to reflect the possibility to specify, for example, how to establish a time moment of proof of existence of qualified electronic signature used for the validation process of qualified electronic signature.

27. Parallel system to qualified electronic attestation of attributes (QEEA)

Based on comments made by multiple Members States, the CZ Presidency has decided to adjust provisions related to electronic attestation of attributes issued by a public sector body responsible for an authentic source, also known as an alternate system to QEEA. First, in order to allow for designation of a public body issuing electronic attestation on behalf of a body responsible for the authentic source at national level and, at the same time, to retain a relatively concise text of respective Articles, a new definition of 'electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source' has been introduced in **Article 3(45a)**. **Articles 45a**, **45da** and **Annex VII** have been amended accordingly. Secondly, the CZ Presidency has proposed a more generic wording of **Article 45da(2)** that does not change its meaning. Lastly, Article **45da(2a)** has been added to pre-condition the issuance of electronic attestation of attributes with the specified legal effect to Wallets by

approval of a supervisory body based on a conformity assessment report issued by the conformity assessment body. Delegations are kindly invited to intervene, should they not be in a position to accept the changes proposed, and in such a case, to provide the CZ Presidency with guidance on how to resolve the matter.

28. Commission empowerment to issue implementing acts in the area of trust services

    Based on comments from Member States, CZ Presidency has proposed to modify the empowerment of the Commission to issue implementing acts with regard to particular trust services.

29. Several modifications and adjustments with a view to improving the accuracy and readability of the text are also found in the Annex below.

30. The CZ Presidency would like to invite delegations to **discuss this new compromise** proposal during the next WP meeting of **28 September**.

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.

(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

---

3 OJ C , , p. .

4 COM/2020/67 final

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

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 eID 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) 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 issued, thus benefiting from a harmonised European approach to trust, security and interoperability. Users and service providers alike should be able to benefit from the same legal value provided to electronic attestations of attributes across the Union.

(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.

(7) It is necessary to set out the harmonised conditions for the establishment of a framework for European Digital Identity Wallets to be ~~issued~~ **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, user convenience and wide usability. Member States should ensure equal access to digital identification to all their nationals and residents.

(8) In order to ensure compliance with~~in~~ **sectoral** Union law or national law compliant with Union law, ~~service providers~~ **relying parties** should **notify** ~~communicate~~ **their intent to rely on the European Digital Identity Wallets** ~~to~~ **be subject to registration** **in** **the** Member State~~s~~ **where they are established ~~and~~. These notifications ~~They~~ should specify the intended use of the Wallet~~, including a list of~~ and a description of the~~ir~~ services for which the Wallet will be used ~~that will rely on the Wallet~~. The Wallet should ~~be able~~ enable the user to validate the identity of the relying parties and that they are authorized ~~allowed~~ by Member States to provide specific services**. That will allow Member States to protect users from fraud and prevent the unlawful use of identity data and electronic attestations of attributes as well as to ensure that the processing of sensitive data, like health data, can be verified by relying parties in accordance with Union law or national law. **Nonetheless, the extent to which the European Digital Identity**

[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.

Wallet allows for validation of identity of relying parties is dependent on specific use cases and requirements thereof. Typically, in in-person scenarios the user is able to identify the relying party thanks to the context, such as when interacting with a ~~police officer,~~ car rental clerk or pharmacist. Where automated validation of identity of the relying party through the European Digital Identity Wallet is not a requirement ~~possible~~, the European Digital Identity Wallet should at least display a notice to the user explaining that validation of the relying party may be conducted by the user offline by requesting the relying party to present a physical proof of identity, for instance a physical and legitimate ID ~~by requesting a law enforcement officer to present their badge~~. In all cases, the notification ~~registration~~ requirements should be cost-effective and proportionate to risk, consider existing notification or registration requirements applicable to specific categories of relying parties, such as public sector bodies, and how the European Digital Identity Wallet will enable ~~ensure~~ the user to obtain and validate ~~the provision and validation of~~ identity data and attestations of attributes depending on the various use cases. 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. All relying parties should nevertheless notify and be authorised to rely on the use of the European Digital Identity Wallet, to be enabled to authenticate themselves or their services to be authenticated towards the Wallet or the user as appropriate. The verification of the consistency between the notified intended use and the effective 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.

[(8a) An ~~fully~~ offline use of European Digital Identity Wallets usually poses a lower risk to protection of personal data as compared to other use cases. Typically, such situations comprise a ~~mere~~ presentation of ~~a QR code~~ information by the user through their European Digital Identity Wallet using a QR code or a location-based technology such as NFC, BLE or WifiAware and respective processing of that information by the relying party at a ~~its~~ physical location, whereas no data is transmitted to remote servers for the purpose of the interaction. Due to the local nature of such use of European Digital Identity Wallets, the relying party should be exempted from the registration obligation, provided that additional safeguards stipulated in this Regulation are met. However, in order to allow for the participation of a relying party in the Wallet ecosystem and to ensure that competent bodies can intervene in cases of security incidents or fraudulent use of the Wallet reported by users, a minimum set of information about the relying party and the devices used should be obtained and maintained also in case of an offline use of the Wallet, where possible in an automated or semi-automated manner.]

(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 of European Digital Identity Wallets shall be free of charge to natural persons, whereas subsequent use of the Wallet might imply costs occuring from the individual use of, for instance, authentication, unless this is supported by relying parties themselves, or from the issuance of the electronic attestations of attributes to the Wallet ~~or from the use of revocation services~~.**

(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, including solutions operable in cross-border regions. 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. Furthermore, the abovementioned additional functionalities should not benefit from measures aiming at cross-border reliance on European Digital Identity Wallets, unless such recognition is agreed on by Member States on a bilateral or multilateral basis.

(10) In order to achieve a high level of **data protection,** security and trustworthiness, this Regulation establishes the requirements for European Digital Identity Wallets. The conformity of European Digital Identity Wallets with those requirements should be certified by accredited public or private sector bodies designated by Member States. Relying on a certification scheme based on the availability of commonly agreed standards with Member States should ensure a high level of trust and interoperability. Certification should in particular rely on the relevant European cybersecurity certifications schemes established pursuant to Regulation (EU) 2019/881[8]. Such certification should be without prejudice to certification as regards personal data processing pursuant to Regulation (EC) 2016/679.

[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

(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 easy to utilize by the users and build 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 should be set out in implementing acts.

(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. ~~Using biometrics~~ **The processing of biometric data as an authentication factor in strong user authentication** ~~to authenticate~~ 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~~s~~ **data** represents a unique characteristic of a person, the ~~use~~ **processing** of biometric~~s~~ **data is only allowed under the exceptions of Article 9(2) of Regulation (EU) 2016/679 and** requires ~~organisational and security measures~~ **appropriate safeguards**, commensurate to the risk that such processing may entail to the rights and freedoms of natural persons ~~and in accordance with Regulation 2016/679~~.

(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

---

technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), OJ L 151, 7.6.2019, p. 15

[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).

notification as national electronic ~~identity card~~ **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 or voluntary ICT security certification schemes, such as certification schemes to be established at Union level under Regulation (EU) 2019/881, to support their claims on the alignment of the schemes or of parts thereof with the requirements of the Regulation on the interoperability and the security of the notified electronic identification schemes.

(17) ~~Service providers use the identity data provided by the set of person identification data available from electronic identification schemes pursuant to Regulation (EU) No 910/2014 in order to match users from another Member State with the legal identity of that user. However, despite the use of the eIDAS data set, in many cases ensuring an accurate match requires additional information about the user and specific unique identification procedures at national level. To further support the usability of electronic identification means, this Regulation should require Member States to take specific measures to ensure a correct identity match in the process of electronic identification. For the same purpose, this Regulation should also extend the mandatory minimum data set and require the use of a unique and persistent electronic identifier in conformity with Union law in those cases where it is necessary to legally identify the user upon his/her request in a unique and persistent way.~~

(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 ~~or according to administrative practice~~, 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 ~~the unique and persistent identifier~~ 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 ~~not~~ required by national or Union law ~~or according to administrative practice~~. 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 design, develop and implement online services in a similar manner 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 ~~considered~~ ensured, as well as the use of trusted lists as essential elements to build trust.**

(21) This Regulation should build on Union acts ensuring contestable and fair markets in the digital sector. In particular, it builds on the Regulation XXX/XXXX [Digital Markets Act], 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(1)(f) of the Regulation XXX/XXXX [Digital Markets Act] 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 [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

[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).

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** ~~and~~ 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 ~~recipients is ensured with a higher level of confidence than~~ **addressee while a high level of confidence would suffice as regard to** the identification of the sender.

(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**,** ~~and~~ financial**, payment and e-money** 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 for online identification is required by national or Union law or by contractual obligation. 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 18 months of their deployment and revise the provisions to ensure their acceptance by means of delegated acts in the light of this assessment.

(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 relying party to obtain only data 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 ~~protection~~ including **data** minimisation ~~of processing of personal data~~.

(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 meachnisms 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 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**~~, as users will have confidence in a website that has been authenticated~~. The use of website authentication services by websites **should be** ~~is~~ voluntary. However, in order for website authentication to become a means to increase~~ing~~ trust, providing a better experience for the user and furthering growth in the internal market, this Regulation **should** lays 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 ~~Q~~**q**ualified certificates for website authentication pursuant to Regulation (EU) No 910/2014. They should recognise ~~and display~~ ~~Q~~**q**ualified 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** ~~provide a high level of assurance, allowing website owners to assert their identity as owners of a website and users to identify the website owners with a high degree of certainty~~. **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 justified concerns related to breach of security and loss of integrity of certificates, thus contributing to the online security of end-users.** To further promote their usage, public authorities in Member States should consider incorporating ~~Q~~**q**ualified 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 ~~pre~~**con**servation of electronic documents and associated trust services. To ensure legal certainty**,** ~~and~~ trust **and harmonization across Member states**, ~~it is essential to provide~~ a legal framework ~~to facilitate the cross border recognition of~~ **for** qualified electronic archiving services **should be established,** ~~**that is**~~ **inspired by the framework of the other trust services** ~~**of**~~ **set out in this Regulation** ~~**by,**~~**. This framework should offer** ~~**offering**~~ **trust service providers and users** ~~**with**~~ **an efficient toolbox that includes functional requirements for the electronic archiving service, as well as** ~~**sets out**~~ **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** ~~**turned electronic**~~ **digitised**. **When required, these provisions should allow for the conserved electronic documents to be ported on different media or formats for the purpose of extending their durability and legibility beyond the technological validity period, while minimising loss and alteration to the greatest extent possible. When electronic documents 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 conservation period of such documents, possibly relying on the use of other qualified electronic trust services established by this Regulation. For creating archival evidence where electronic signatures, electronic seals or electronic timestamps are used, qualified electronic trust services should be used.** ~~That framework could also open new market opportunities for Union trust service providers.~~ ~~**Qualified preservation of qualified electronic signatures and qualified electronic seals can take place without the need to store the signed/sealed data and without requiring the use of a qualified electronic archiving services. Furthermore, the use of qualified electronic archiving services may not be sufficient to preserve the trustworthiness of qualified electronic signatures and qualified electronic seals beyond their technological validity period. Moreover the use**~~

~~of qualified electronic signatures and qualified electronic seals may only ensure the integrity of data for a limited period of time, hence the use of qualified electronic archiving services may be required to extend the data integrity beyond the technological validity period of those electronic signatures/seals, and/or to retrieve the data unaltered after a longer period of time.~~ **As far as ~~the~~ electronic archiving services are not ~~fully~~ 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.**

(34) ~~Qualified electronic ledgers record data in a manner that ensures the uniqueness, authenticity and correct sequencing of data entries in a tamper proof manner. An electronic ledger combines the effect of time stamping of data with certainty about the data originator similar to e-signing and has the additional benefit of enabling more decentralised governance models that are suitable for multi-party co-operations.~~ **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 ~~like~~ such as electricity. They can also provide solutions for ~~digital credentials and support~~** more **efficient and transformative public services <u>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</u>. Qualified electronic ledgers create a legal presumption for the unique and accurate sequential chronological ordering and integrity of the data records in the ledger.** ~~For example, it creates a reliable audit trail for the provenance of commodities in cross-border trade, supports the protection of intellectual property rights, enables flexibility markets in electricity, provides the basis for advanced solutions for self-sovereign identity and supports more efficient and transformative public services. To prevent fragmentation of the internal market, it is important to define a pan-European legal framework that allows for the cross-border recognition of trust services for the recording of data in electronic ledgers.~~ ~~**Data records contained in a qualified electronic ledger have a unique sequential chronological order, safeguards the integrity of the data entries. By creating a unique sequential chronological order of data records, t The qualified electronic ledger, for example, guarantees that an entity holding a solves the "double spending problem" for digital records of ownership and thereby differs**~~ **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.** ~~**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 like electricity. They can also provide solutions for digital credentials and support more efficient and transformative public services.**~~ **Namely, neither the time stamping of digital documents, nor their transfer by means of electronic registered delivery services could 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).**

~~**Common to all is that the creation of an electronic ledger presupposes both software and hardware components.**~~

(35) ~~The certification as qualified trust service providers should provide legal certainty for use cases that build on electronic ledgers. This trust service for electronic ledgers and qualified electronic ledgers and the certification as qualified trust service provider for electronic ledgers should be notwithstanding the need for use cases to comply with Union law or national law in compliance with Union law. Use cases that involve the processing of personal data must comply with Regulation (EU) 2016/679. Use cases that involve crypto assets should be compatible with all applicable financial rules for example with the Markets in Financial Instruments Directive[9], the Payment Services Directive[10] and the future Markets in Crypto Assets Regulation[11].~~ **To prevent fragmentation of the internal market~~, it is important to define~~ a pan-European legal framework should be established ~~that~~ allowing~~s~~ for the cross-border recognition of trust services for the recording of data in qualified electronic ledgers. ~~The granting of a qualified status to trust service providers for electronic ledgers and their auditing (Section 2) supervision should provide legal certainty to actors in the public and private sector for the reliability of electronic ledgers. Trust service providers for electronic ledgers should not be mandated to identify the parties sending data to the ledger, nor the authenticity of the data sent. The compliance of qualified trust service providers with this~~ Trust service providers for electronic ledgers should ~~not~~ be mandated to ascertain network integrity ~~to identify the natural/or and legal persons sending data to an electronic ledger, nor the "authenticity" of data sent, because these are not technical tasks related to ledger integrity but require legal verifications and anti-money laundering assessments entrusted to other entities such as crypto asset service providers~~. This Regulation is notwithstanding any legal obligations that ~~the~~ 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 ~~must~~ should comply with Regulation (EU) 2016/679. Use cases that involve crypto assets ~~shall~~ 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 ~~the future~~ Markets in Crypto Assets ~~Regulation~~[14] and with anti-money laundering rules which could be included in the Transfer of Funds Regulation[15]~~.~~, and could require crypto asset service providers to verify the identity of

---

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 24.9.2020 for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937, COM/2020/593 final.~~

15 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.

users of blockchains in order to comply with international anti-money laundering standards.

(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][16] 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) This Regulation ~~does~~ should not prevent Member ~~s~~States ~~should~~ from laying down rules on penalties for infringements ~~of this regulation~~ such as direct or indirect practices ~~creating~~ 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.

(36b) This ~~r~~Regulation should ensure a~~n~~ harmonized level of quality, trustworthiness and security of qualified trust services, regardless of the place where the operations are conducted. Thus, the provision of a qualified trust service by a qualified trust service provider outsourcing any of its operations outside of the Union should provide the guarantees, ensuring that supervisory activities and audits can be enforced as if these operations were carried out~~n~~ in the Union. When the compliance with the Regulation cannot be fully assured, the supervisory bodies should be able to ~~may~~ 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) Qualified trust service providers should use, when issuing a qualified certificate, state-of-the-art cypher suites in order to ensure security of issued qualified certificates and sufficient time period resistance thereof.]

[16] [insert reference once adopted]

(36e) This Regulation should set out an obligation for qualified trust service providers to verifythe 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 acting in a commercial or professional capacity using core platform services for the purpose of or in the course of providing goods and services to end-users are business users in accordance with Art. 2(21) DMA.

(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[17].

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

HAVE ADOPTED THIS REGULATION:

Article 1

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

(1) Article 1 is replaced by the following:

'This Regulations 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:

~~(a)~~**(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;

~~(d)~~**(ab)** lays down the conditions **under which Member States shall provide and recognise** ~~for the issuing of~~ European Digital Identity Wallets ~~by Member States.'~~;

(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 and electronic attestation of attributes,

[17] 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).

the management of remote **qualified** electronic signature and seal creation devices, and electronic ledgers;

~~(d) lays down the conditions for the issuing of European Digital Identity Wallets by Member States.';~~

(2) Article 2 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. This Regulation applies to electronic identification schemes that have been notified by a Member State, European Digital Identity Wallets ~~issued~~ ~~**made available**~~ **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** ~~as regards form with underlying legal effects~~.';

(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** ~~or ID cards following Regulation 2019/1157,~~ 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) 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~~,~~ ~~and~~ or electronic identification means, ~~and~~ ~~or~~ ~~including European Digital Identity Wallets,~~ provided according to this Regulation;

(c) point (14) is replaced by the following:

'(14) 'certificate for electronic signature' means an electronic attestation ~~or set of attestations~~ which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person;';

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

'(16) 'trust service' means an electronic service normally provided ~~against payment~~ **for remuneration** which consists of:

~~(a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services, electronic attestation of attributes and certificates related to those services;~~

~~(b) the creation, verification and validation of certificates for website authentication;~~

~~(c) the preservation of electronic signatures, seals or certificates related to those services;~~

~~(d) the electronic archiving of electronic documents;~~

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

~~(f) the recording of electronic data into an electronic ledger.';~~

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

(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; ~~or~~

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

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

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

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

(f) the issuing of electronic attestations of attributes ; ~~or~~

(fa) the validation of electronic attestation of attributes; ~~or~~

(g) the creation of electronic timestamps ; ~~or~~

(ga) the validation of electronic timestamps; ~~or~~

(g~~a~~b) the ~~[creation of]~~ provision of electronic registered delivery services; ~~or~~

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

(h) the electronic archiving of electronic documents; or

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

~~(j) any combination of the above services'~~

~~(da) the following point (10a) is inserted:~~

~~(10a) 'remote electronic signatures' means an electronic signature where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory;~~

(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 ~~where~~ **managed by** a qualified trust service provider ~~generates, manages or duplicates the electronic signature creation data~~ on behalf of a signatory;

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

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

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

~~'(32a) 'remote qualified **electronic** seal creation device' means a qualified electronic seal creation device where **managed by** a qualified trust service provider generates, manages or duplicates the electronic signature creation data on behalf of a seal creator;';~~

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

'(41) 'validation' means the process of verifying and confirming that ~~an electronic signature or a seal or person identification data, or an electronic attestations of attributes is~~ **data in electronic form are** valid **according to the requirements of this Regulation**';

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

'(42) 'European Digital Identity Wallet' is an electronic identification means that allows the user to store <u>and retrieve</u> identity data, electronic attestations of attributes linked to ~~her/his~~ <u>their</u> identity, to provide them to relying parties on request and to use them for authentication, online and<u>, where appropriate,</u> offline, for a service in accordance with Article 6a; and to ~~create~~ <u>sign by means of</u> qualified electronic signatures and <u>seal by means of qualified electronic</u> seals;';

~~'European Digital Identity Wallet' is a material or immaterial unit that allows, in accordance with Article 6a, the user to:~~

- **~~present personal identification data and electronic attestations of attributes to relying parties on request~~**
- **~~perform electronic identification and authentication for a service~~**
- **~~create qualified electronic signatures and or seals;~~**

(43) 'attribute' ~~is~~ **represents** ~~a feature,~~ **the** characteristic**,** ~~or~~ quality**, ~~[~~right or permission~~]~~** of a natural or legal person or of an ~~entity~~ **object**~~, in electronic form~~;

(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;

<u>(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;</u>

(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 ~~**in accordance with national law**~~ to be ~~the~~ **a** primary source of that information or recognised as authentic ~~in national law~~ **in accordance with Union or national law, including administrative practice**;

(47) 'electronic archiving' means a service ensuring the **receipt, storage,** ~~**transmission**~~ **retrieval and deletion of electronic documents in order to guarantee their durability and legibility as well as to preserve their integrity, confidentiality and** ~~**correctness of origin of their content**~~ **throughout the conservation period** ~~receipt, storage, deletion and transmission of electronic data or documents in order to guarantee their integrity, the accuracy of their origin and legal features throughout the conservation period~~ ~~**long term electronic storage and preservation of electronic documents**~~;

(48) 'qualified electronic archiving service' means a**n electronic archiving** service that meets the requirements laid down in Article 45g**a**;

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

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

~~(51) 'user account' means a mechanism that allows a user to access public or private services on the terms and conditions established by the service provider;~~

~~(52) 'credential' means a proof of a person's abilities, experience, right or permission;~~

(53) 'electronic ledger' means a **sequence of** ~~tamper proof~~ electronic **data** record**s** ~~of data~~, **which ensures** ~~providing authenticity and~~ **their integrity** ~~of the data it contains,~~ **and the** accuracy of their ~~date and time, and 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) '~~unique identification~~ **record matching**' means a process where person identification data, ~~or~~ person identification means**,** ~~**or**~~ **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, regional or sectoral identification data, is associated with a single user within a given system and persistent in time;

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

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

(55d) '~~fully~~ offline use of European Digital Identity Wallets' means an interaction between a user and a relying party at a physical location ~~of the relying party~~, whereby neither the Wallet ~~user~~ nor the relying party is required to ~~exchange data~~ 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 ~~replaced by the following~~ **inserted before Article 6a**:

'SECTION I

~~**ELECTRONIC IDENTIFICATION**'~~ **European Digital Identity Wallet**;

~~**(6) Article 6 is deleted**~~

(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 ~~cross-border~~ public and private services, **each Member State shall ensure that a European Digital Identity**

Wallet is ~~issued~~ provided ~~each Member State shall issue a European Digital Identity Wallet~~ within 12 months after the entry into force of this Regulation.

2. European Digital Identity Wallets shall be ~~issued~~ **provided**:

   (a) by a Member State; ~~**or**~~

   (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, ~~obtain, store, select, combine and share, in a manner that is transparent to and traceable by the user, the necessary legal person identification data and electronic attestation of attributes~~ **select, combine, store, delete and present electronic attestation of attributes and person identification data ~~and present~~ to relying parties, ~~while ensuring that selective disclosure is possible~~ including to authenticate online and offline in order to use ~~online~~ public and private services, while ensuring that selective disclosure of data is possible**;

   ~~(ab) perform electronic identification and authentication of the user to public and private services, through the use of an notified electronic identification means;~~

   (b) sign by means of qualified electronic signatures **~~or~~ and ~~create~~ seal by means of qualified electronic seals**.

4. **European** Digital Identity Wallets shall, in particular:

   (a) provide a common **set of** interface**s**:

      (1) **for issuance of person identification data,** ~~to qualified and non-qualified trust service providers issuing~~ qualified and non-qualified electronic attestations of attributes or ~~other~~ qualified and non-qualified certificates ~~for the purpose of issuing such attestations and certificates~~ to the European Digital Identity Wallet;

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

      (3) for the presentation to relying parties of person identification data~~,~~ **or** electronic attestation of attributes ~~or other data such as credentials, in local mode not requiring internet access for the wallet~~ **online and, where technically feasible, 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) ensure that trust service providers of ~~qualified~~ **electronic** attestations of attributes cannot receive any information about the use of these attributes **after their issuance ~~[, beyond what is strictly necessary for service provisioning of a service requested by the user]~~**;

(ba) Ensure that the identity of relying parties ~~is~~ can be validated by implementing ~~a common~~ authentication mechanism in accordance with Article 6b(1);

(c) meet the requirements set out in Article 8 with regards to assurance level ~~[~~'high'~~][or substantial] [~~**applicable mutatis mutandis to the management and use of person identification data through the Wallet, including electronic identification and authentication**~~]~~ ~~, in particular as applied to the requirements for identity proofing and verification, and electronic identification means management and authentication~~;

~~(d) provide a mechanism to ensure that the relying party is able to authenticate the user and to receive electronic attestations of attributes;~~

(e) ensure that the person identification data referred to in Articles 12(4), point (d) uniquely and persistently represent the natural **person,** ~~or~~ legal person **or the natural person representing the natural or legal person, who** is associated with ~~it~~ **the ~~w~~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, including of personal identification data and electronic attestations of attributes.

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

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

~~(b) to allow relying parties to verify that the attestations of attributes are valid;~~

~~(c) to allow relying parties and qualified trust service providers to verify the authenticity and validity of attributed person identification data.~~

(d) to allow the user to authenticate relying parties in accordance with Article 6b(1);

~~[(e) to ensure that the use of the European Digital Identity Wallet by relying parties is consistent with the intended use as registered in accordance with Article 6b(1).]~~

6. The European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance 'high' **~~[or substantial]~~**. The **issuance and ~~sole~~** use of the European Digital Identity Wallets shall be free of charge to natural persons.

[6a 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 user**s** shall be in full control of the **use of the** European Digital Identity Wallet **and of the~~ir~~ 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~~ **gives** expressly ~~requested~~ **consent to** it **as defined in Article 4 (11) of Regulation (EU) No 2016/679**. Personal data relating to the provision of European Digital Identity Wallets shall be kept ~~physically and~~ 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 ~~1~~**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 are eligible to rely on the European Digital Identity Wallets in accordance with Article 6b(2);

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

(c) the body 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 eligible 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** ~~Member States issuing~~ the European Digital Identity Wallets.

10. The European Digital Identity Wallet shall be made accessible for persons with disabilities in accordance with the accessibility requirements of ~~Annex I to~~ Directive 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**,** ~~and~~ 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' ~~or 'high'~~ 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 ~~issued~~ **provided** in accordance with this Regulation, they shall ~~communicate~~ **be subject to registration in notify** it to the Member State where ~~the relying party is~~ **the relying parties are** established ~~to~~**. The notification shall in particular include a description of the intended use of the European Digital Idenity Wallet and the services for which the European Digital Idenity Wallet will be used. ~~Such registration~~ This requirement shall be without prejudice to notification and registration requirements in accordance with sectorial Union or national law, including applicable to public bodies. ~~Member States shall provide for~~ The notification procedure shall be cost-effective and proportionate-to-risk ~~registration procedures~~. ~~Relying parties and shall also inform the Member State about all their services in which the European Digital Identity Wallet may be used and about the intended use of the European Digital Identity Wallet in relation to these services~~. Member States shall, in accordance with national law, ~~check~~ ~~ensure compliance~~ provide for appropriate measures to verify and decide on eligibility** with **the** requirements set out in Union ~~law~~ or national law for the ~~**provision**~~ **reliance on the use of the European Digital Identity** ~~of specific services **through the w**~~**Wallet**. ~~When communicating their intention to rely on European Digital Identity wallets, they shall also inform about the intended use of the European Digital Identity Wallet.~~ **Relying parties shall inform without delay the Member State about any subsequent change in the information ~~communicated for their initial registration~~ initially provided, including the cease of provided services.**

[1a. Where relying parties that provide private or public services ~~intend to~~ rely upon an ~~fully~~ offline use of European Digital Identity Wallets ~~issued~~ provided in accordance with this Regulation, they shall be exempted from the ~~obligation to register~~ notification procedure laid down in paragraph 1, provided that:

(i) the relying party does not obtain access to special categories of personal data as set out in Regulation (EU) 2016/679; ~~and~~

(ii) any personal data obtained by the relying party is erased or made anonymous when it is no longer needed to fulfil the purpose of the ~~fully~~ offline use of the European Digital Identity Wallet; and

(iii) the collected personal data shall not be used for any other purpose than for the purpose for which it was collected.]

2. ~~Member States shall implement a common mechanism for the authentication of relying parties.~~ **Relying parties shall ~~implement measures that~~ ensure the implementation of common authentication mechanisms referred to in Article 6a(4)(ba).**

3. Relying parties shall be responsible for carrying out the procedure for ~~authenticating~~ **validating** person identification data and 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**,** ~~and~~ 2 **and 3** by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(1**~~0~~**). **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. ~~European Digital Identity Wallets that have been certified or for which a statement of conformity has been issued under a cybersecurity scheme pursuant to Regulation (EU) 2019/881 and the references of which have been published in the Official Journal of the European Union shall be presumed to be compliant with the cybersecurity relevant requirements set out in Article 6a paragraphs 3, 4 and 5 in so far as the cybersecurity certificate or statement of conformity or parts thereof cover those requirements.~~ **The conformity of European Digital Identity Wallets with the requirements laid down in article 6a(3), (4), (5), ~~and~~ (7) and where applicable (11a), shall be certified by accredited public or private bodies designated by Member States. [The certification shall be valid for 2 years, and include a vulnerabilities assessment. Where vulnerabilities are identified and not remedied, the certification shall be cancelled.]**

2. ~~Compliance with~~ **Without prejudice to Regulation (EU) 2016/679 applying to them, ~~and especially~~ compliance with** the requirements set out in paragraphs 3, 4**,** ~~and~~ 5 **and 7** of Article 6a related to the personal data processing operations carried out by the issuer of the European Digital Identity Wallets shall be ~~certified~~ **~~pursuant to Article 42 of Regulation (EU) 2016/679~~ confirmed as part of the certification referred to in paragraph 1**.

3. ~~The conformity of European Digital Identity Wallets with the requirements laid down in article 6a paragraphs 3, 4 and 5 shall be certified by accredited public or private bodies designated by Member States~~. **European Digital Identity Wallets, or parts thereof, that have been certified ~~or for which a statement of conformity~~**

~~has been issued~~ **under a** relevant **cybersecurity certification scheme pursuant to Regulation (EU) 2019/881,** ~~and~~ **the references of which have been published in the Official Journal of the European Union, shall be presumed to be compliant with the cybersecurity relevant requirements set out in Article 6a(3), (4), (5),** ~~and~~ **(7)** and where applicable (11a), **in so far as the cybersecurity certificate** ~~or statement of conformity~~ **or parts thereof cover those requirements.**

3a. ~~For the purposes of this Article,~~ 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 **specifications and reference** standards **required** for the certification of the European Digital Identity Wallets referred to in paragraph ~~3.~~**1, 2 and 3; and**

b) technical, procedural, organisational and operational specifications for the designation, monitoring and review of accredited public and private bodies referred to in paragraph 1, including the certification schemes and related evaluation methods they use to conduct certification of the European Digital Identity Wallets and the certificates and certification reports underlying them. ~~This~~ These implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

5. Member States shall communicate to the Commission the names and addresses of the public or private bodies referred to in paragraph ~~3~~ **1**. The Commission shall make that information available to Member States.

6. The Commission shall ~~be empowered to~~**, by means of implementing acts,** ~~adopt delegated acts in accordance with Article 47 supplementing this Article by concerning the~~ establish**~~ingment of~~** specific criteria to be met by the designated bodies referred to in paragraph ~~3~~ **1** **in order to demonstrate that they have an appropriate level of independence and expertise**.

Article 6d

Publication of a list of certified European Digital Identity Wallets

1. Member States shall inform the Commission without undue delay of the European Digital Identity Wallets that have been ~~issued~~ **provided** pursuant to Article 6a and certified by the bodies referred to in Article 6c paragraph ~~3~~ **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 ~~maintain~~ **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(1**~~0~~**). **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 ~~issued~~ **provided** pursuant to Article 6a ~~and~~ **or** the validation mechanisms referred to in Article 6a(5) points (a), (**~~b~~d**) ~~and~~ **or** (**~~c~~e)** are breached or partly compromised in a manner that affects their reliability or the reliability of ~~the~~ other European Digital Identity Wallets, ~~the issuing Member State~~ **the issuer of the concerned wallets** shall, without **undue** delay, suspend the issuance and ~~revoke~~ the ~~validity~~ **use** of the European Digital Identity Wallet**. The Member State where concerned Wallets were** ~~issued~~ **provided** ~~and~~ **shall** inform the ~~other~~ Member States **and the Commission without undue delay~~,~~. The issuer of the concerned Wallets or Member state shall inform relying parties~~,~~ and the users ~~and the Commission~~** accordingly.

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

3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension ~~or revocation~~, the Member State concerned shall withdraw the European Digital **Identity** Wallet concerned and inform the other Member States and the Commission ~~on the withdrawal~~ accordingly. Where it is justified by the severity of the breach, the European Digital Identity Wallet concerned shall be withdrawn without **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(1**~~0~~0**). **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 ~~under national law or by administrative practice~~ to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets ~~issued~~ **provided** in compliance with this Regulation **for authentication of the user**.

2. Where private relying parties providing services 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**,** ~~and~~ financial**, payment and e-money** services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, private relying parties shall**, strictly upon voluntary request of the user,** also accept the use of European Digital Identity Wallets ~~issued~~ **provided** in accordance with ~~Article 6a~~ **this Regulation ~~[strictly upon voluntary request of the user and]~~ in respect of the minimum ~~attributes~~ 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 ~~issued~~ **provided** in accordance with ~~Article 6a~~ **this Regulation for authentication of the user** strictly upon voluntary request of the user and in respect of the minimum ~~attributes~~ **data** necessary for the specific online service for which authentication is requested~~, such as proof of age~~.

4. **In cooperation with Member states t**~~T~~he Commission shall encourage and facilitate the development of ~~self-regulatory~~ codes of conduct ~~at Union level ('codes of conduct')~~, in order to contribute to wide availability and usability of European Digital Identity Wallets within the scope of this Regulation. These codes of conduct shall ~~ensure~~ **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 18 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 ~~may include~~ **shall ~~be~~ include** extent of user base, cross-border presence of service providers, technological development, evolution in usage patterns**, and consumer demand**. **[**The Commission shall be empowered to adopt delegated acts **in accordance with Article 47** based on this assessment~~, regarding a revision of the requirements for recognition of the European Digital Identity wallet under points 1 to 4 of this article~~ **amending paragraph 2]**.

~~6. For the purposes of this Article, European Digital Identity Wallets shall not be subject to the requirements referred to in articles 7 and 9.~~

(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~~ **amended as follows**:

'Pursuant to Article 9(1) Member States **which have not yet done so** shall notify, within 12 months after the entry into force of this Regulation at least one electronic identification scheme including at least one identification means **of level of assurance 'high' meeting all the following conditions**:';

(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.';

~~(11) the following Article 10a is inserted:~~

~~'*Article 10a*~~

~~**Security breach of the European Digital Identity Wallets**~~

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

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

~~3. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension or revocation, the Member State concerned shall withdraw the European Digital **Identity** Wallet concerned and inform the other Member States and the Commission on the withdrawal accordingly. Where it is justified by the severity of the breach, the European Digital Identity Wallet concerned shall be withdrawn without **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(1**10**). **This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2)**.~~

(12) the following Article 11a is inserted:

'*Article 11a*

~~Unique Identification~~ Record matching

1. When notified electronic identification means ~~and~~ **or** the European Digital Identity Wallets are used for authentication, Member States **when acting as relying parties** shall ensure ~~**unique identification**~~ **record matching~~, in accordance with Union law, national law and with administrative practice~~**.

2. Member States shall, for the purposes of this Regulation, include in the minimum set of person identification data referred to in Article 12(4) point (d), a**t 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 ~~**or is in accordance with administrative practice**~~].

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

3. Within 6 months of the entering into force of this Regulation, the Commission shall further specify the measures referred to in 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(1**10**)~~. **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 ~~and access to hardware and software features~~

(a) in paragraph 3, point~~s (c) and~~ (d) ~~are~~ **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,** ~~or~~ legal person **or a natural person representing natural or legal persons**;';

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

'(c) the interoperability of 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, ~~unique identification~~ **record matching** and assurance levels;';

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

'(e) the exchange of information, experience and good practises as regards to design, development and implementation of online services where the European Digital Wallet should be accepted, in particular agreeing on guidelines how such online services should be designed, developed and implemented.']

(14) the following Article 12a is inserted:

'*Article 12a*

Certification of electronic identification schemes

1. 1. Conformity of ~~notified~~ electronic identification schemes **to be notified** with the requirements laid down in **this Regulation** ~~Article 6a, Article 8 and Article 10~~ may 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 or 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 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** ~~**to demonstrate compliance of such schemes or parts of such schemes with the requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes. Member States may use a certificate or a Union statement of conformity issued** in accordance with paragraph 1. Member States may use a certificate or a Union statement of conformity issued in accordance with a relevant European cybersecurity certification scheme established pursuant to Regulation (EU) 2019/881 **to demonstrate compliance of such schemes or parts of such schemes with the requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes**. to demonstrate compliance of such schemes **or parts of such schemes** with the requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes.

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

3. Member States shall notify to the Commission ~~with~~ 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.';

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

~~'SECTION III~~

~~**CROSS-BORDER RELIANCE ON ELECTRONIC IDENTIFICATION MEANS**';~~

~~(16) the following Articles 12b and 12c are~~ **is** ~~inserted:~~

~~'Article 12b~~

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

~~2. Where private relying parties providing services 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~~**,** ~~and financial~~**, payment and e-money** ~~services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, private relying parties shall also accept the use of European Digital Identity Wallets issued in accordance with Article 6a~~ **this Regulation [strictly upon voluntary request of the user and] in respect of the minimum attributes necessary for the specific online service for which authentication 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 issued in accordance with Article 6a~~ **this Regulation for authentication** ~~strictly upon voluntary request of the user and in respect of the minimum attributes~~ **data** ~~necessary for the specific online service for which authentication is requested, such as proof of age.~~

~~4.~~ **In cooperation with Member states t**~~The Commission shall encourage and facilitate the development of self-regulatory codes of conduct at Union level ('codes of conduct'), in order to contribute to wide availability and usability of European Digital Identity Wallets within the scope of this Regulation. These codes of conduct shall ensure~~ **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 18 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 may include **shall be include** extent of user base, cross-border presence of service providers, technological development, evolution in usage patterns**, and consumer demand**. **[**The Commission shall be empowered to adopt delegated acts **in accordance with Article 47** based on this assessment, regarding a revision of the requirements for recognition of the European Digital Identity wallet under points 1 to 4 of this article **amending paragraph 2]**.~~

~~6. For the purposes of this Article, European Digital Identity Wallets shall not be subject to the requirements referred to in articles 7 and 9.~~

~~*Article 12c*~~

~~**Mutual recognition of other electronic identification means**~~

~~1. Where electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access an online service provided by a public sector body in a Member State, the electronic identification means, issued in another Member State shall be recognised in the first Member State for the purposes of cross-border authentication for that online service, provided that the following conditions are met:~~

~~(a) the electronic identification means is issued under an electronic identification scheme that is included in the list referred to in Article 9;~~

~~(b) the assurance level of the electronic identification means corresponds to an assurance level equal to or higher than the assurance level required by the relevant public sector body to access that online service in the Member State concerned, and in any case not lower than an assurance level 'substantial';~~

~~(c) the relevant public sector body in the Member State concerned uses the assurance level 'substantial' or 'high' in relation to accessing that online service.~~

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

~~2. An electronic identification means which is issued within the scope of an electronic identification scheme included in the list referred to in Article 9 and which corresponds to the assurance level 'low' may be recognised by public sector bodies for the purposes of cross-border authentication for the online service provided by those bodies.';~~

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

'1. Notwithstanding paragraph 2 of this Article, trust service providers shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation ~~and with the~~

~~cybersecurity risk management obligations under Article 18 of the Directive XXXX/XXXX [NIS2].~~';

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. ~~The Commission may adopt implementing acts, in accordance with Article 48(2), setting out the conditions under which the requirements of a third country applicable to the trust service providers established in its territory and to the trust services they provide can be considered equivalent to the requirements applicable to qualified trust service providers established in the Union and to the qualified trust services they provide.~~ **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 ~~in question~~ or ~~an~~ international organisation in accordance with Article 218 ~~TFEU~~ of the Treaty.**

2. ~~Where the Commission has adopted an implementing act pursuant to paragraph 1 or the Union has concluded an international agreement on the mutual recognition of trust services in accordance with Article 218 of the TFEUreaty, trust services provided by providers established in the third country concerned shall be considered equivalent to qualified trust services provided by qualified trust service providers established in the Union.~~'; **The implementing decisions and ~~the~~ agreements referred to in paragraph 1 shall ensure~~, in particular,~~ that~~: a.~~ the requirements applicable to qualified trust service providers established in the Union and the qualified trust services they provide are ~~essentially~~ met by the trust service providers in the third country or international organisations ~~with which the agreement is concluded,~~ and by the trust services they provide. ~~[In particular, compliance with the requirements set out in Article 24, effectiveness of the trust services supervision and compliance with the requirements applicable to trust service providers under NIS 2 (Directive XXX – reference to be included once the proposal adopted) shall be ensured].~~ 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 Commission may adopt implementing acts specifying the conditions and procedures under which the requirements applicable to the trust service providers established in a third country and to the trust services they provide can be considered equivalent to the requirements applicable to qualified trust service providers established in the Union and to the qualified trust services. The implementing acts will cover, in particular :~~

~~a) The Compliance with the requirements set out in article 24 if this regulation; and~~

~~b) The effectiveness of the trust services supervision and its and enforcement; and~~

~~c) The compliance with protection of the data processed under the REGULATION (EU) 2016/679 of the European Parliament and of the Council and~~

~~d) The compliance with the requirements applicable to trust service providers under NIS 2 (Directive XXX – reference to be included once the proposal adopted)~~

4. **Th~~o~~se implementing ~~acts~~ 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 ~~Annex I 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 ~~the present~~ 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~~, about the results of audits of qualified trust service providers, where~~ **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~~], by means of implementing acts, further specify the formats and procedures for the~~ tasks of **adopt guidelines on the exercise by** the Supervisory ~~Authorities~~ **bodies of the tasks** referred to in paragraph 4**,** and ~~**define the formats and procedures**~~**, 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. ~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).~~';

(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]. ~~The s~~**S**upervisory bod**ies**~~y~~ shall request ~~the~~ national competent authorit**ies**~~y~~ 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, ~~and, where applicable,~~ the public if it is of public interest and, where applicable, other relevant competent bodies ~~where applicable and the public if it is of public interest~~, of any ~~linked~~ 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 has~~ve~~ 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 [24/72] 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, ~~establish the additional~~ 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. **~~[Qualified trust service providers shall inform at least two weeks in advance the supervisory body about planned audits and avail allow for the participation of the supervisory body as observer upon request.]~~** ~~t~~**T**he 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]. ~~q~~**Q**ualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within three working days of receipt.';

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

'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 ~~of the results of its audits~~.';

(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.

~~w~~**W**here that provider does not provide a remedy ~~and~~, where applicable within the time limit set by the supervisory body, the supervisory body, taking into account in particular~~,~~ the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the **affected** service ~~concerned which~~ it provides ~~and, request it, where applicable within a set time limit, to comply with the requirements of Directive XXXX/XXXX[NIS2]. The supervisory body shall inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1)~~ **~~and the national competent authority referred to in Dir XXXX [NIS2].~~**

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 ~~national competent~~ 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 number**s of** ~~for the following~~ 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~~, carried out by the conformity assessment bodies~~;

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

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

(23) Article 21 is amended as follows:

'1. Where trust service providers~~, without qualified status~~ intend to start providing **a** qualified trust service~~s~~, 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 ~~in any case~~ no later than two months from the receipt of this request by the ~~NIS~~ competent authorities referred to in Dir XXXX [NIS2] ~~authority~~** ~~within three days from their completion~~. **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 ~~referred to in the first subparagraph~~ **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 ~~of this Article~~. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).';

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

~~'2a. Paragraphs 1 and 2 shall also apply to trust service providers established in third countries and to the services they provide, provided that they have been recognised in the Union in accordance with **an implementing act adopted pursuant to** Article 14.';~~

(25) Article 24 is amended as follows:

(a) paragraph 1 is replaced by the following:

'1. When issuing a qualified certificate or a qualified electronic attestation of attributes ~~for a trust service~~, ~~**or when recording data into a qualified electronic ledger,**~~ a qualified trust service provider shall verify the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of attribute**s** ~~is~~ **will be** issued~~**, or of the natural or legal person sending data to the qualified electronic ledger**~~.

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**s** ~~[~~'substantial' or~~]~~ '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 ~~natural~~ person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;

(d) through the physical presence of the natural person or of an authorised representative of the legal person by appropriate procedures and in accordance with national laws ~~if other means are not available~~.';

(b) the following paragraph 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 ~~of~~ **at least ~~two weeks~~ one month before implementing** any change in the provision of its qualified trust services **or at least three months in case of** ~~and~~ an intention to cease those activities~~;~~**. The supervisory body may ~~decide that a validation has to be granted before the trust service provider can implement any changes~~ request additional information or the result of a conformity assessment before granting the permission to implement the intended changes to the qualified trust services. ~~An absence of reply of the supervisory body within two weeks shall be considered as an implicit permission~~; 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) point (d) is replaced by the following:

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

(2) the new points (fa) and (fb) are inserted:

'(fa) have appropriate policies and take corresponding measures to manage legal, business, operational and other direct or indirect risks to the

provision of the qualified trust service. Notwithstanding the provisions of Article 18 of Directive EU XXXX/XXX [NIS2], those measures shall include at least the following:

(i) measures related to registration and on-boarding procedures to a service;

(ii) measures related to procedural or administrative checks;

(iii) measures related to the management and implementation of services.';

'(fb) notify the supervisory body**, 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 ~~l~~inked 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 has**ve** 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. ~~e~~**C**ompliance with the requirements laid down in this Article shall be presumed, where ~~trustworthy systems and products~~ ~~meet~~ 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 ~~delegated~~ **implementing** acts ~~regarding~~ **specifying the technical characteristics of** the ~~additional~~ measures referred to in paragraph 2(fa).';

(XX) Article 26 is amended as follows:

2. The Commission ~~[may/~~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 standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

(XX) Article 27 is amended as follows:

~~**2a. If a Member State requires qualified electronic signature to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise qualified electronic signatures in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.**~~

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 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 ~~qualified~~ 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. ~~**Within 12 months of the entering into force of this Regulation, t**~~ 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 **~~[according to the individual intent of the signatory, refraining the use of automated or bulk signing]~~;**

(b) notwithstanding point (1)(d) of Annex II, **ma**y duplicate~~s~~ the electronic signature creation data only for back-up purposes provided the following requirements are met:

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

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** ~~The~~ certification referred to in paragraph 1 ~~**must**~~ **shall not exceed** ~~shall be valid for~~ 5 years, conditional upon a regular 2 year vulnerabilities assessment. Where vulnerabilities are identified and not remedied, the certification shall be ~~withdrawn~~ **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 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, ~~establish~~ **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).';

~~[~~(XX) 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 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, ~~establish~~ 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).'~~]~~

(XX) Article 33 is amended as follows:

'1. ~~**Within 12 months of the entering into force of this Regulation a**~~ **A** qualified validation service for qualified electronic signatures **may ~~shall~~** only be provided by a qualified trust service provider who:';

'2. **Within 12 months of the entering into force of this Regulation,** The Commission ~~may~~ **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 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 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).';

(XX) **In** Article 36 ~~is amended as follows~~ **a new paragraph 2 is added**:

2. The Commission [~~may/~~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 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:

~~**'2a. If a Member State requires qualified electronic seal to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise qualified electronic seals in at least the formats or using methods defined in the implementing acts referred to in paragraph 5.**~~

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 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.';

[(XX) 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 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).';

(XX) 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 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).';

(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** ~~Qualified certificates for website authentication shall be deemed compliant~~ with the requirements laid down in Annex IV **shall be carried out in accordance with** ~~where they meet~~ the standards referred to in paragraph ~~3~~ **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.

~~3. **Compliance with the requirements laid down in paragraphs 1 and 2 shall be presumed where a qualified certificates for website authentication meets the standards referred to in paragraph 4.**~~

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

Article 45c

Requirements for qualified electronic attestation of attributes

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

1a. Evaluation of compliance ~~A qualified electronic attestation of attributes shall be deemed to be compliant~~ with the requirements laid down in Annex V~~, where it meets~~ **shall be carried out in accordance with** the 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(1**0**).

Article 45d

Verification of attributes against authentic sources

1. Member States shall ensure that, at least for the attributes listed in Annex VI, wherever these attributes rely on authentic sources within the public sector, measures are taken to allow qualified providers of electronic attestations of attributes to verify **these attributes** by electronic means at the request of the user **and in accordance with national or Union law**, ~~the authenticity of the attribute directly against the relevant authentic source at national level or via designated intermediaries recognised at national level in accordance with 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(1**0**).

Article 45da

Requirements for ~~E~~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 ~~responsible for the authentic source~~ 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 following articles shall apply mutatis mutandis to the public sector bodies responsible for an authentic source issuing the electronic attestation of attributes: Articles 24(1), 24(1a), 24(2) points (b), (c), (d), (e), (f), (fa), (fb), (g) and (h), 24(4a), 24(5) and 24(6).~~ 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 same level of reliability as qualified trust service providers in accordance with Article 24.

2a. Prior to issuing the attestations of attributes to European Digital Identity Wallets, the public sector body referred to in Article 3(45a), shall provide to the competent supervisory body, a conformity assessment report issued by a conformity assessment body confirming that they meet the requirements set out in paragraphs 1, 2 and 6 of this Article. After the approval by the supervisory body, the public sector body may proceed with issuing the attestations of attributes to European Digital Identity Wallets.

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).

6. Public sector bodies ~~responsible for an authentic source~~ referred to in Article 3(45a) issuing electronic attestation of attributes shall provide an interface with the European Digital Identity Wallets issued 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 ~~issued~~ **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**.

~~3. Personal data relating to the provision of qualified electronic attestation of attributes services shall be kept physically and logically separate from any other data held **by the provider of electronic attestation of attributes**.~~

4. Providers of qualified electronic attestation of attributes' services shall **implement [functional~~/legal~~] separation for** provid**eing** such services ~~under a separate legal entity~~.

SECTION 10

~~QUALIFIED~~ ELECTRONIC ARCHIVING SERVICES

Article 45g

Legal effect of an electronic archiving service

1. Electronic documents 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 documents stored using a qualified electronic archiving service shall enjoy the presumption of their integrity and ~~of correctness~~ of their origin for the duration of the ~~pre~~conservation 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.

~~**Qualified electronic archiving services**~~

~~A qualified electronic archiving service for electronic documents may only be provided by a qualified trust service provider that uses procedures and technologies capable of extending the trustworthiness of the electronic document beyond the technological validity period.~~

~~Within 12 months after the entry into force of this Regulation, the Commission shall, by means of implementing acts, establish reference numbers of standards for electronic archiving services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).~~

Article 45ga

Requirements for qualified electronic archiving services

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

(a) They are provided by qualified trust service providers

(b) They use procedures and technologies ~~that guarantee the integrity of the electronic documents for the duration of the preservation period by the~~

~~qualified trust service providers~~ capable of extending the durability and legibility of the electronic document beyond the technological validity period and at least throughout the legal or contractual conservation period, while maintaining their integrity and ~~the correctness of~~ their origin;

(c) They ensure that the ~~data~~ electronic documents ~~is preserved~~ are stored in such a way that ~~it is~~ they are safeguarded against loss and alteration, except for changes concerning ~~its~~ 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 document retrieved from a qualified electronic archive enjoys the presumption of integrity of the data from the moment of archiving to the moment of retrieval ~~at the moment of retrieval~~. This report shall be provided in a reliable and efficient way~~, which report is reliable, efficient~~ and it shall bears ~~the advanced~~ qualified electronic signature or ~~advanced~~ qualified electronic seal of the provider of the qualified electronic archiving service;

~~(e) When electronic documents submitted to the archival service contain one or more qualified electronic signatures or qualified electronic seals, the requirements of article 34 shall apply correspondingly.~~

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 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 the**ir** unique~~ness~~ **and accurate sequential chronological ordering and of their integrity**~~, the correctness of their origin, and authenticity of the data it contains, of the accuracy of their date and time of recording, and of their sequential chronological ordering within the ledger~~.

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 ~~correctly~~ establish the origin of data records ~~ensure the uniqueness, authenticity and correct sequencing of data entries recorded~~ **in the ledger;**

   (c) they ensure the **unique** ~~correct~~ sequential chronological ordering of data **records** in the ledger ~~and the accuracy of the date and time of their recording data entry;~~

   (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 standards referred to in paragraph 3.

3. The Commission ~~may~~ **shall**, by means of implementing acts, establish **technical specifications and** reference numbers of standards for ~~the processes of execution and registration of a set of data into, and the creation, of~~ **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 issued on their territory** ~~and the qualified trust services~~.

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

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

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

   (c) **summary report including data on** incidents ~~and down time of the infrastructure at national level~~ preventing the use of **the European** Digital Identity Wallet ~~Apps~~.

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 ~~24~~ **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 ~~identification means including~~ European Digital Identity Wallets in scope of this Regulation and assess whether all online private service providers relying on third party electronic identification services for users authentication, shall be mandated to accept the use of ~~notified electronic identification means and~~ **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 ~~12~~ **36 months following the entry into force of this Regulation**. ~~[date – OJ please insert period of four years following the entry into force of this Regulation].~~

2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall continue to be considered as qualified certificates for electronic signatures under this Regulation until ~~12~~ **24 months following the entry into force of this Regulation**. ~~[date – PO please insert a period of four years 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.

(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;’.

~~The following point is added:~~

~~‘(x) Qualified certificates for electronic signatures may contain an indication, in a form suitable for automated processing, and for the sole purpose of demonstrating conformity with the requirements of article 24.1.b), of the identity verification method listed in paragraph 1 of Article 24 used during issuance of the certificate.~~

ANNEX II

REQUIREMENTS FOR QUALIFIED ELECTRONIC SIGNATURE CREATION DEVICES

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

   (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;’.

~~The following point is added:~~

~~‘(x) Qualified certificates for electronic seals may contain an indication, in a form suitable for automated processing, and for the sole purpose of demonstrating conformity with the requirements of article 24.1.b), of the identity verification method listed in paragraph 1 of Article 24 used during issuance of the 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 ~~advanced~~ **qualified** electronic signature or ~~advanced~~ **qualified** electronic seal of the issuing qualified trust service provider;

(l) the location where the certificate supporting the ~~advanced~~ **qualified** electronic signature or ~~advanced~~ **qualified** electronic seal referred to in point (~~f~~**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 ~~responsible for an authentic source~~ 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.**