Analysis of the consolidated eID (eIDAS2) draft Regulation

Version: 1.0

2024-01-12

Contents

Introduction

At the end of 2023 the draft regulation of eID (the eIDAS2 legislation) was published. The amending draft was identified as document 15149/23 from the Council of the European Union.

This draft Regulation was an amending regulation and was not published in a consolidated form.
In order to make the draft eID Regulation more readable, the eIDAS and the new draft eID Regulation have been merged by Microsec:

- The original text is the text of eIDAS, while the parts modified with change tracking are taken from the draft eID (eIDAS2) Regulation.
- The number and the title of the Articles have been merged into a single line so that the table of contents can index them.

This document does not only contain the consolidated version of the text, but also examines other aspects of the draft, and thus consists of the following sections:

- Executive summary
  In this section, the most important information about the draft eID regulation were summarized.
- The changes
  In this section the changes have been examined, identifying the sections that have changed and those that have not. For the sections that have changed, the change is also described.
- The error lists
  In this section, the errors in the draft amendment, be they typing errors, problems of understanding, technical problems, etc., have been identified.
- The deadlines
  This section collects the new deadlines scattered throughout the draft amending act.
- The consolidated eID draft
  The draft merged manually with track changes.

The utmost care has been taken in the preparation of this document. If you find any errors, please report them to viktor.varga@microsec.com.

Executive summary

The draft eID Regulation has been amended to make it compatible with eIDAS as follows:

1. eIDAS originally consists of 52 Articles.
2. Of these, 37 are not or minimally modified, 3 have been deleted and 12 have been significantly modified.
3. The new draft regulation adds 33 new Articles, so in the end the draft eID regulation has 82 Articles.

The requirements for new services are covered in 2/3 of the new parts. The new services are:

- **EDIW (European Digital Identity Wallet)**

  The EDIW is a mobile Wallet service that allows you to share your identity (to identify, authenticate yourself) and other attributes, from your mobile phone, primarily for public administration and connected services. It is planned to be used for both online and offline transactions. Such a Wallet is required to be developed in all EU Member States.

  The requirements will cover the following areas: requirements for the Wallet itself, requirements for Relying parties where we can use EDIW, requirements for certification, requirements for the Wallet Trust List and mandatory acceptance at EU level.

- **attribute attestation service**

  A qualified attribute service certifies our attributes, its electronic attestation (attribute attestation) is legally equivalent to its paper form.

  This means that we can obtain a valid electronic attestation from a qualified service provider, for example, about our personal data, education, age, marital status, driving licence, identity cards, etc.

  A special case of attribute services is the Public Sector Body attribute service, which is an attribute service provided by an administrative manager of a given authentic data source (e.g. a government agency), which returns the data it manages in the form of an attribute attestation. The attestation issued is legally equivalent to a qualified attribute attestation, and its technical security requirements are as strong as required for a QTSP.

- **archiving**

  This differs from preservation in that it is no longer just digitally signed data that can be accepted for archiving, but anything. (The Preservation Service, on the other hand, is the preservation of digitally signed data.)

- **ledger**

The ledger service verifies the chronological order and integrity of the data entered.

In terms of amendments to the previous text, the most significant changes are:

- Managed Remote Qualified Signature Creation Device (RQSCD) is now a separate service.
- Requirements are introduced for non-qualified trust services.
- Qualified trust services are also supervised by the NIS2 supervisory body, NIS2 requirements must be met.
- The identification and verification requirements for qualified certificate issuance are changed:
    - EDIW is introduced as a possible identification method.
    - For remote identification, a high-level identification solution is required, but it is not necessary for the solution to be recognized at national level.
    - A certificate issued with remote identification becomes eligible for a certificate with qualified signature.
- Depending on the results of assessment by the Commission, it is possible that there will be implementation regulation from the Commission on the standard for advanced electronic signatures (in 24 months)
- The validity of the certification of Qualified Signature Creation Device (QSCD) devices should not exceed 5 years and a vulnerability assessment is required every 2 years.
- There will be regulation of the verification of advanced signatures based on QSCD.
- Planned changes at a QTSP must be approved by Supervisory Body of Trust services.
- Devices with SSCD certification can be used only for 36 months after the Regulation enters into force.
- RQSCD services already in operation at the date of entry into force of the eID Regulation can be considered compliant without a compliance assessment for 24 months.
- Identifications according to eIDAS Article 24 may be used for 24 months after the Regulation enters into force.
- Member States have 24 months to give qualified service providers access to a credible source of the data listed in Annex VI.
- In the 6th month after entry into force 10 and in the 12th month 22 Articles are expected to be referenced to a standard or process in the framework of a Commission implementing regulation.

The proposed amendment contains errors, perhaps the most disturbing of these:

- In Article 24, the regulation does not allow attributes to be verified using the Public Sector Body attribute attestation, because it is missing from the list.
- For QWAC, service certification for the new specifications is only possible after the publication of the Commission implementing regulation.

The changes

The changes to the draft eID Regulation compared to eIDAS2 are summarized below.

The changes can be grouped into the following categories:

- unchanged articles,
- minimal changes that do not change the interpretation,
- articles updated with the deadline for Commission legislation,
- articles updated with the new trust services,
- articles completely deleted,
- completely new articles or significantly changed articles.

Unchanged articles

The following articles were unchanged:

- Article 4, 6, 7, 10, 11, 22, 23, 39, 40, 43, 46, 48, 50

Minimal changes that do not change the interpretation

The following articles have been slightly modified, but without changing the meaning:

- Article 5, 8, 9, 12, 13, 14, 25, 27, 28, 35, 37, 41, Annex IV

Articles updated with the deadline for Commission legislation

Deadlines for Commission legislation have been added to the following articles:

- Article 31, 32, 33, 34, 36, 38, 42, 44

Articles updated with the new trust services

New trust services have been added in the following articles:

- Article 1, 2, 3, 47

Articles completely deleted

- Article 17, 18, 19
  The articles on the supervisory body, mutual assistance and security requirements of the TSP have been deleted and the relevant provisions are reflected in other articles.

Articles completely new or significantly changed

- Preamble paragraphs
  Since the Court of Justice of the European Communities has ruled that the preamble to a Community act does not has binding legal force[1], so we will not describe the changes.
- Article 6a
  EDIW requirements.
- Article 6b
  EDIW relying party requirements.
- Article 6c
  EDIW certification requirements.
- Article 6d
  Publication of EDIW "trust list"
- Article 6da
  Security breach response requirements of EDIWs.
- Article 6db
  Mandatory acceptance of EDIWs in public services for electronic identification.
- Article 11a
  Mandatory acceptance of EDIWs in cross border electronic identification.
- Article 12a
  Certification requirements of electronic identification schemes.
- Article 12b
  Gatekeepers shall allow EDIWs.
- Article 15
  Accessibility requirements: trust services should be aligned with the requirements set out Annex I of Directive 2019/882.
- Article 16
  Penalties; the maximum penalty is 5m € or 1% total worldwide turnover, whichever is higher.
- Article 19a
  Non-qualified trust services requirements.
- Article 20
  Supervision of qualified TSPs:
  - The Supervisory Body (SB) shall be notified about the planned audits of TSP, and the SB can participate on the audit.
  - Member states shall notify the Commission about the CABs carrying out conformity assessments and the Commission shall publish a list of them. CABs to the Commission, and the Commission shall publish a list of them.
    Please note: these CABs do not have to be designated.
- Article 21
  Initiation of a qualified trust service: NIS2 Supervisory Body action is mandatory.

[1] The Court of Justice of The European Union (1998, November 19) C-162/97 - Nilsson and Others - Judgment of the Court https://curia.europa.eu/juris/liste.jsf?language=en&num=C-162/97

- Article 24
  - paragraph 1 -
    - The order of identification methods were shifted (a->d; b->a; c->b; d->c).
    - Wallet was added as identification means.
    - Remote identification shall be carried out on level “high”
    - There is no need for national recognition of the remote identification method.
    - A certificate issued with remote authentication can now be used to request a certificate with an electronic signature.
    - A new option for verifying the data to be included in the certificate has been added: the use of qualified attribute attestation.
    - **Important: attribute attestations issued by a PSB CANNOT be used.**
  - paragraph 2
    - The qualified provider must obtain authorization from the supervisory body one month before implementing any change.
- Article 24a
  EU wide recognition of qualified services and devices. The previous recognition sentences in eIDAS are collected in this Article.
- Article 26
  Advanced signatures; The Commission may draw up a list of standards and procedures in the light of experience.
- Article 29
  QSCD requirement; the managed RQSCD requirements were added here.
- Article 29a
  RQSCD detailed requirements
- Article 30
  QSCD certification; certificate shall be only valid for 5 years. In every 2 years vulnerability assessment is mandatory.
- Article 32a
  Requirements for the validation of advanced electronic signatures based on qualified certificates.
- Article 39a
  RQSCD for seals; Article 29a apply mutatis mutandis.
- Article 40a
  Requirements for advanced electronic seals based on qualified certificates: Article 32a apply mutatis mutandis.

- Article 45
  Requirement for QWACs
  - QWACs shall be recognized by web browsers.
  - The assessment can only be made on the basis of a standard list to be established by the Committee, i.e. only after this implementing regulation is created and in force. Compared with the terminology in force for other services, the difference and the problem with the wording is apparent:

    Evaluation of compliance with those requirements shall be carried out in accordance with the standards and the specifications referred to in paragraph x.
    VS
    Compliance with the requirements laid down in paragraph x/Annex x shall be presumed where <service> meets those standards.

- Article 45a-1
  Cybersecurity precautionary measures.
- Article 45a
  Legal effect of attribute attestation; legal effect cannot be denied, qualified and PSB attribute attestations shall have the same legal effect as the lawfully issued attestation in paper form.
- Article 45b
  Qualified attribute attestation only usable for authentication for a public service, if the Member State allows it. If allowed in a Member State, then qualified attributes from other Member States shall be also accepted.
- Article 45c
  Requirements for qualified electronic attestation of attributes;
  - References the Annex V.
  - The assessment can only be made on the basis of a standard list to be established by the Committee, i.e. only after this implementing regulation is created and in force. Compared with the terminology in force for other services, the difference and the problem with the wording is apparent:

    Evaluation of compliance with those requirements shall be carried out in accordance with the standards and the specifications referred to in paragraph x.
    VS
    Compliance with the requirements laid down in paragraph x/Annex x shall be presumed where <service> meets those standards.

- Article 45d
  Verification of attributes against authentic sources:
  - Members State shall ensure access to trust services for authentic data.
  - The Commission shall have an implementing act to define catalogue of attributes and schemes.

- Article 45da
  PSB attribute attestation requirements:
  - The qualified seal of PSB shall include special data.
  - The reliability and security of PSB shall be the same as the QTSP.
  - Member State shall notify the PSBs to the EU.
- Article 45e
  Issuing attestation to Wallet: EDIW user shall have the possibility to access and manage attributes. For qualified attribute attestations, implementing the EDIW interface is mandatory.
- Article 45f
  Additional rules for attribute attestation:
  - The data shall not be combined with data from other services, shall kept logically separate and the functionally shall be separated from other services.
- Article 45g
  Legal effect of archiving services.
- Article 45ga
  Requirements for qualified electronic archiving services.
- Article 45h
  Legal effect of ledger services.
- Article 45i
  Requirements for qualified electronic ledger services.
- Article 46a
  Supervision of the EDIW framework.
- Article 46b
  Supervision of trust services
  Please note: in the Chapter III Section 2 and 3 also about supervision (Article 19a, 20, 21)
- Article 46c
  Single points of contact
- Article 46d
  Mutual assistance
- Article 46e
  The European Digital Identity Cooperation Group
- Article 48a
  Member State reporting requirements
- Article 49
  Review of the Regulation 24 months after its entry into force.
- Article 52
  Entry into force:
  - SSCD certified under the Directive can only be accepted for 36 months from the date of entry into force.
  - Qualified certificates issued under the Directive are only valid for 24 months from the date of entry into force.
  - Qualified remote signature services already in operation may continue to operate without a compliance assessment for 24 months from the date of entry into force.

Please note: This Article can be found on the error list too.

- Annex I
  Point (i) has been modified so that revocation information can include information not just path (e.g., NoRevAvail extension for validity assured short time certificates).
- Annex II
  Requirements of managed remote QSCD services were removed. (There is a dedicated Article for this purpose.)
- Annex III
  Point (i) has been modified so that revocation information can include information not just path (e.g., NoRevAvail extension for validity assured short time certificates).
- Annex V
  Requirements of qualified attribute attestation; requirements are similar to Annex I, with one exception, the attribute attestation shall have qualified signature or seal in it.
- Annex VI
  Minimum list of attributes; Member States shall provide access to authentic data sources for QTSPs for the attributes listed in this Annex.
- Annex Via
  Requirements of attribute attestation for Public sector Bodies (PSB); requirements are similar to Annex V, except no QCStatements required.

The error lists

The published version of the draft eID (eIDAS2) Regulation contains various bugs, which we have collected here, grouped into different categories.

These categories are:

- Inconsistent, wrong numbering
  They may be repeated, incorrect numbering, gaps in the numbering, their correction in most of the cases is either not necessary or not a problem.
- Formatting errors
  These are poor formatting, such as incorrect indentation, duplicate or missing headings, etc. Do not interfere with understanding.
- Typos
  A few typos. Do not interfere with understanding.
- Unrepealed paragraphs of the eIDAS
  Following the merger, in the case of Articles 50, 51 and 52, the amendment has not repealed the parts which still affect the Directive. These parts do not make sense, they should be addressed in the draft amendment so that they are not included in the final eID Regulation.
- Other inconsistencies
  In the draft, the legal formula used is sometimes inappropriate. In these cases, the correct terminology may be to change or replace rather than insert. It does not interfere with understanding, but from a legal technical point of view, it is necessary to correct them in the final eID Regulation.

Inconsistent, wrong numbering of items

There are many places where the numbering during drafting is not consistent.

These are:

- Paragraphs with the same number.
  The following paragraph numbers were assigned multiple times (twice or more):
  - preamble paragraph (9a)
  - preamble paragraph (31a)

- Gap in the numbering.
  These are the gaps in the numbering of the items:
  - preamble paragraph (11b), (17a), (36a), (36b), (36f)
  - preamble paragraph (21) (draft deleted this paragraph)
  - Article 3 point (51), (52), (55a)
  - Article 6a paragraph 3 (a) point (i)
  - Article 6a paragraph 3 (ab)
  - Article 6a paragraph 4 point (a): (4b), (4f), (4g),
  - Article 6a paragraph 4 (d), (ea), (eb),
  - Article 6a paragraph 5 (b), (c)
  - Article 6a paragraph 5b

- Article 6b paragraph 1c, 1f
- Article 6c paragraph 5 (draft added an empty paragraph, which is omitted)
- Article 11a paragraph 2.
- Article 12 paragraph 7.
- Article 17-19 (draft deleted these)
- Article 24 paragraph 2 point j
- Article 27 paragraph 4
- Article 37 paragraph 4
- Article 45 paragraph 2a
- Article 45a paragraph 3
- Article 45f paragraph 3

- Mistake in the numbering.
  These were wrong and **corrected:**
  - Article 19a paragraph 1 (a) - Numbered as (cc), corrected to (a).
  - Article 19a paragraph 1 (a) point (i) - The numbering was missing, added.
  - Article 26 paragraph 1 - The numbering was missing, added.
  - Article 36 paragraph 1 - The numbering was missing, added.
  - Article 44 paragraph 2b – Numbered as (2b) corrected to 2b.

Formatting errors

There are few places where the formatting of the draft is wrong. These and the activity carried out on them are:

- preamble paragraph (21) – Adds a deleted paragraph. **Omitted.** Also added to the gaps in numbering list.
- Article 6a paragraph 3 - Single item list. **Untouched.**
- Article 6a paragraph 4a, 4b, 5a, 5c - The indentation of the paragraphs was incorrect. **Corrected.**
- Article 6c paragraph 5 - The draft adds a blank paragraph. **Omitted.** Also added to the gaps in numbering list.
- Article 19a - The article has not been given a title. **Untouched.**
- Annex Via – The title was duplicated. The **second instance was omitted.**

Typos

The wording contains typos in some places. These are:

- Article 6a paragraph 6 - 'a' instead of 'an'. **Untouched.**

  > *6. The European Digital Identity Wallets shall be provided under a**n** electronic identification scheme of level of assurance 'high'.*

- Article 20 paragraph 1a - 'at the latest' instead of 'at least'. **Untouched.**

1a. Qualified trust service providers shall inform the supervisory body at ~~the latest~~ least one month in advance about planned audits and allow for the participation of the supervisory body as an observer upon request.

- The paragraph 1 of the Article 21 was repeated before Article 24 modification without any context. This second appearance was **omitted.**

Unrepealed paragraphs of the eIDAS Regulation that apply to the Directive

These are the provisions relating to the Directive. Since the directive was repealed a long time ago, these remaining sections make no sense.

These sentences, paragraphs are colored to **purple in the consolidated text:**

- Article 50
- Article 51 paragraph 3, 4
- Article 52 paragraph 2, 3, 4
  The draft inserts the Article 52, but there is already an Article 52. The inserted text is identical with the first paragraph of Article 52 of eIDAS.

Other inconsistencies

There are few other inconsistencies in the wording of draft:

- The wording says, that the Article 24 paragraph 2 point *„point (g) and (h) are replaced*". But also, the point (i) was replaced. This amendment to point (i) has also been included.
- The wording says *"Article 33 is amended as follows:"* but the amended paragraphs are already exists, and paragraph 2 of Article 33 shall be replaced.

The deadlines

Legislative tasks for the Commission within 6 months of the entry into force of the eID Regulation

The following table lists the implementing rules to be established by the Commission for which the deadline is 6 months.

Article	Task
Article 6a paragraph 11	Implementing act about the standards and/or procedures for EDIWs.
Article 6b paragraph 4	Implementing act about the standards and/or procedures for EDIW Relying parties.
Article 6c paragraph 4	Implementing act about the certification of the European Digital Identity Wallets.
Article 6d paragraph 3	Implementing act about the formats and/or procedures of EDIW list publishing.
Article 6da paragraph 5	Implementing act about the standards and/or procedures for Reaction on an EDIW Security breach.
Article 11a paragraph 3	Implementing act about the standards and/or procedures when Member States act as relying parties for cross border services.
Article 45c paragraph 4	Implementing act about the standards and/or procedures for qualified electronic attribute attestation.
Article 45d paragraph 2	Implementing act about the standards and/or procedures for the catalogue of attributes and schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes.
Article 45da paragraph 6	Implementing act about the standards and/or procedures for PSB electronic attribute attestation.
Article 45da paragraph 7	Implementing act about the standards and/or procedures for notification of PSBs to the Commission.

Legislative tasks for the Commission within 12 months of the entry into force of the eID Regulation

The following table lists the implementing rules to be established by the Commission for which the deadline is 12 months.

Article	Task
Article 19a paragraph 2	Implementing act about the standards and/or procedures for TSPs providing non-qualified services.
Article 20 paragraph 4	Implementing act about the standards and/or procedures for: - accreditation of CABs - QTSP conformity assessment requirements
Article 21 paragraph 4	Implementing act about the standards and/or procedures for the initiation of a qualified trust service.
Article 24 paragraph 1a	Implementing act about the standards and/or procedures for the verification of identities and attributes.
Article 24 paragraph 5	Implementing act about the standards and/or procedures for the requirements for QTSPs.
Article 28 paragraph 6	Implementing act about the standards and/or procedures for qualified certificates for electronic signature.
Article 29a paragraph 2	Implementing act about the requirements for a qualified service for the management of remote qualified electronic signature creation devices
Article 31 paragraph 3	Implementing act about the formats and/or procedures of QSCD.
Article 32 paragraph 3	Implementing act about the standards and/or procedures for QSCD list publishing
Article 32a paragraph 3	Implementing act about the standards and/or procedures for requirements for validation of advanced signatures based on qualified certificates.
Article 32a paragraph 4	Implementing act about the standards and/or procedures for requirements for validation of qualified signature.
Article 33 paragraph 2	Implementing act about the standards and/or procedures for requirements for qualified validation service.
Article 34 paragraph 3	Implementing act about the standards and/or procedures for requirements for qualified preservation service.
Article 38 paragraph 6	Implementing act about the standards and/or procedures for qualified certificates for electronic seals.
Article 42 paragraph 2	Implementing act about the standards and/or procedures for qualified electronic time stamps.
Article 44 paragraph 2	Implementing act about the standards and/or procedures for qualified electronic registered delivery services.
Article 45 paragraph 3	Implementing act about the standards and/or procedures for qualified web site authentication.
Article 45ga paragraph 2	Implementing act about the standards and/or procedures for qualified electronic archiving services.
Article 45i paragraph 3	Implementing act about the standards and/or procedures for qualified electronic ledgers.
Article 46a paragraph 8	Implementing act about the formats and/or procedures of the supervisory report.

Article	Task
Article 46b paragraph 8	Implementing act about the guideline of supervisory practice.
Article 46e paragraph 7	Implementing act about the necessary procedural arrangements to facilitate the cooperation between the Member States

Tasks for the Commission within 24 months of the entry into force of the eID Regulation

The following table lists the implementing rules to be established by the Commission for which the deadline is 24 months.

Article	Task
Article 26 paragraph 2	Commission shall carry out an assessment on whether it is necessary to adopt an implementing act, establishing a list of reference standards and when necessary, establishing specifications and procedures for advanced electronic signatures.
Article 36 paragraph 2	Commission shall carry out an assessment on whether it is necessary to adopt an implementing act, establishing a list of reference standards and when necessary, establishing specifications and procedures for advanced electronic seals.
Article 49 paragraph 1	The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council .

Other deadlines starting from the entry into force of the eID Regulation

The following table lists the other deadlines found in the eID regulation.

Article	Task	Months
Article 51 paragraph 1	SSCD devices can only considered as QSCD device. (After this date only QSCD is allowed to use.)	36
Article 51 paragraph 2a	The already running remote qualified electronic signature services are considered valid, without conformity assessment.	24
Article 51 paragraph 2b	The already running remote qualified trust services are considered valid, without conformity assessment, and the eIDAS Art. 24 identification are still usable.	24

Deadlines starting from the publication of the implementing regulation under Art. 6a paragraph 11 and Art. 6c (4)

The following table lists the other deadlines and their subjects starting from the publication of the implementing regulation under Art. 6a paragraph 11 and Art. 6c (4).

Article	Subject	Task	Months
Article 6a paragraph 1	Member State	Member State shall provide at least one European Digital Identity Wallet.	24
Article 6db paragraph 2	EDIW Relying parties	If strong authentication required by a EU or national law or by contractual obligations, relying parties shall accept the EDIWs.	36
Article 45d paragraph 1	Member State	Member State shall provide access to authentic sources for attributes detailed in Annex VI.	24

Deadlines that start from another event or legal act or with different subject

The following table lists the other deadlines found in the eID regulation.

Article	Subject	Task	Months	Condition
Article 6a paragraph 1	Member State	Member State, if electronic identification is used for public services shall recognize other Member States electronic identification.	24	after the Commission published it on the list
Article 6db paragraph 5	Commission	Commission shall carry out an assessment on demand, availability and usability of the European Digital Identity Wallets	24	after deployment of the European Digital Identity Wallets
Article 45d paragraph 1	EDICG	EDICG shall publish guideline on the organizational aspects and procedures for the mutual assistance.	24	after entry into force of the eID Regulation

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,

Acting in accordance with the ordinary legislative procedure,

Whereas:

(PREAMBLE PARAGRAPHS)

(1) The Commission Communication of 19 February 2020, entitled "Shaping Europe's Digital Future" announces a revision of Regulation (EU) No 910/2014 of the European Parliament and of the Council 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, the European Council called on the Commission to propose the development of a Union-wide framework for secure public electronic identification, including interoperable digital signatures, to provide people with control over their online identity and data as well as to enable access to public, private and cross-border digital services.

(2a) The Digital Decade Policy Programme 2030, established by Decision (EU) 2022/2481 of the European Parliament and of the Council, sets the objectives and digital targets of a Union framework which, by 2030, leads to wide deployment of a trusted, voluntary, user-controlled digital identity, recognised throughout the Union and allowing each user to control their data in online interactions.

(3a) The interinstitutional Declaration entitled "European Declaration on Digital Rights and Principles for the Digital Decade", signed by the European Parliament, the Council and the Commission on 15 December 2022 (the 'Declaration'), underlines every citizen's right to

access digital technologies, products and services that are safe, secure, and privacy-protective by design. This includes ensuring that all people living in the Union are offered an accessible, secure and trusted digital identity that enables access to a broad range of online and offline services, protected against all cyberthreats, including identity theft or manipulation. The Declaration also states that everyone has the right to the protection of their personal data online. That right encompasses the control on how the data is used and with whom it is shared.

(3b) Union citizens should have the right to a digital identity that is under their sole control and that enables them to exercise their rights as citizens in the digital environment and to participate in the digital economy. To achieve this aim, a European digital identity framework should be established allowing Union citizens to access public and private online and offline services throughout the Union.

(3c) A harmonised digital identity framework should contribute to the creation of a more digitally integrated Union by reducing digital barriers between Member States and by empowering Union citizens and residents to enjoy the benefits of digitalisation, while increasing transparency and the protection of their rights.

(4) A more harmonised approach to digital identification should reduce the risks and costs of the current fragmentation due to the use of divergent national solutions ***or, in some Member States, the absence of such electronic identification solutions. Such an approach should*** strengthen the Single Market by allowing citizens, other residents as defined by national law and businesses to identify ***and authenticate*** online ***and offline in a safe, trustworthy, user friendly,*** convenient***, accessible and harmonised way,*** across the Union. ***The European Digital Identity Wallet should provide natural and legal persons across the Union with a harmonised electronic identification means enabling the authentication and sharing of 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 ***electronic*** attestations of attributes, such as ***academic qualifications,*** university ***degrees or other educational or professional entitlements***. The framework for a European Digital Identity ***should*** achieve a shift from the reliance on national digital identity solutions only, to the provision of electronic attestations of attributes valid ***and legally recognised across the Union***. Providers of electronic attestations of attributes should benefit from a clear and uniform set of rules***, while*** public administrations should be able to rely on electronic documents in a given format.

(4a) Several Member States have implemented and largely use electronic identification means that nowadays are accepted by service providers in the Union. Additionally, investments were made into both national and cross-border solutions on the basis of Regulation (EU) No 910/2014 of the European Parliament and of the Council, including the interoperability of notified electronic identification schemes (eIDAS) pursuant to that Regulation. In order to guarantee the complementarity and a fast adoption of European Digital Identity Wallets by current users of notified electronic identification means and to minimise the impacts on existing service providers, European Digital Identity Wallets are expected to benefit from building on the experience with existing electronic identification means and taking advantage of the deployed eIDAS infrastructure at Union and national levels.

(4b) Regulation (EU) 2016/679 and, where relevant, Directive 2002/58/EC should apply to all personal data processing activities under this amending Regulation. The solutions under the interoperability framework provided in this amending Regulation should also comply with these rules. EU data protection law provides for data protection principles, such as the data minimisation and purpose limitation principle and obligations, such as data protection by design and by default. The implementation of this amending Regulation should comply with these data protection principles and obligations.

(5) To support the competitiveness of European businesses, ***both*** online ***and offline*** service providers should be able to rely on digital identity solutions recognised across the Union, irrespective of the Member State in which they have been ***provided***, thus benefiting from a harmonised European approach to trust, security and interoperability. ***Both*** users and service providers should be able to benefit from the same legal value provided to electronic attestations of attributes across the Union.

A harmonised digital identity framework should create economic value by providing easier access to goods and services and by significantly reducing operational costs linked to identification and authentication procedures, for instance during the on-boarding of new customers, by reducing the potential for cybercrimes, such as identity theft, data theft and online fraud, thus promoting efficiency gains and the secure digital transformation of Union's micro, small and medium sized enterprises (SMEs).

(5b) The European Digital Identity Wallet (EDIW) should facilitate the application of the 'once only' principle, thus reducing administrative burden and supporting cross-border mobility of citizens and businesses across the Union and fostering the development of interoperable e-government services across the Union.

(6) ***Regulations*** (EU) No 2016/679[1] ***and (EU) 2018/1725***[2] ***and Directive 2002/58/EC***[3] ***apply*** to the processing of personal data in the implementation of this ***amending*** Regulation. Therefore, this ***amending*** 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 ***processed to provide*** the services falling within the scope of this ***amending*** Regulation. ***Personal data related to the provision of European Digital Identity Wallets should be kept logically separate from any other data held by the provider. This amending Regulation should not prevent providers of European Digital Identity Wallets to apply additional technical measures contributing to protection of personal data, such as physical separation of personal data relating to the provision of Wallets from any other data held by the provider. Without prejudice to Regulation (EU) 2016/679, this amending Regulation further specifies the application of principles of purpose limitation, data minimisation, and data protection by design and by default.***

(6a) EDIWs should have the function of a common dashboard embedded into the design, in order to ensure a higher degree of transparency, privacy and control of the users over their data. This function should provide an easy, user friendly interface with an overview of all relying parties with whom the user has shared data, including attributes, and the type of data shared with each relying party. It should allow the user to track all transactions executed through EDIWs, with at least the following data: the time and date of the transaction, the counterpart identification, the data requested and the data shared. That information should be stored

even if the transaction was not concluded. It should not be possible to repudiate the authenticity of the information contained in the transaction history. Such a function should be active by default. It should allow users to easily request to a relying party the immediate deletion of personal data pursuant Article 17 of Regulation (EU) 2016/679 and to easily report to the competent national authority where a relying party is established if an unlawful or inappropriate request of data is received without leaving the EDIW.

(6b) Member States should integrate different privacy-preserving technologies, such as zero knowledge proof, into the EDIW. These cryptographic methods should allow a relying party to validate that a given statement based on the person's identification data and attestation of attributes is true, without revealing any data this statement is based on, thereby ensuring the privacy of the user.

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

(7a) Member States should rely on the possibilities offered by this Regulation to provide, under their responsibility, European Digital Identity Wallets for use by the natural and legal persons residing on their territory. To offer Member States flexibility and leverage the technological state of the art, this Regulation should enable provision of EDIWs directly by a Member State, under a mandate from a Member State, or independently of a Member State, but recognised by that Member State.

(8) ***For the purposes of registration, relying parties should provide the information necessary to allow for their identification and authentication towards the European Digital Identity Wallets. When declaring their intended use of the EUDIW, relying parties should provide information regarding the data that they will request, if any,*** in order to ***provide their services and the reason for the request. Relying party registration should facilitate Member States' verifications related to the lawfulness of the activities of the relying parties in accordance*** with Union law***.***

The obligation to register should ***be without prejudice to obligations laid down in other Union or national law, such as the information to be provided to the data subjects pursuant to the Regulation (EU) 2016/679.***

Relying parties should comply with the safeguards offered by Articles 35 and 36 of Regulation (EU) 2016/679, in particular by performing data protection impact assessments and by consulting the competent data protection authorities prior to data processing where data protection impact assessments indicate that the processing ***would result in a high risk. Such safeguards should support the lawful processing of personal data by relying parties, in particular when special categories of data are at stake, such as health data. The registration of*** relying parties ***should enhance transparency and trust in the use of the European Digital Identity Wallet. Registration should be cost-effective and proportionate to the related risks in order to ensure the uptake by service providers. In this context, registration should provide for the use of automated procedures, including the reliance on and the use of existing registers by Member States, and not entail a pre-authorisation process.***

The registration process should enable a variety of use-cases that may differ in terms of mode of operation (online/offline), or in terms of the requirement to authenticate devices for the purposes of interfacing with the European Digital Identity Wallet. Registration should exclusively apply to relying parties providing services by means of digital interaction.

(8a) Safeguarding citizens against unauthorised or fraudulent use of the wallet is of high importance for ensuring trust in and for the wide uptake of the European Digital Identity Wallets. Users should be provided with effective protection against such misuse. In particular, when facts that form the basis for a fraudulent or otherwise illegal use of the wallet are established by a national judicial authority in the context of another procedure, supervisory bodies of the wallet issuers should upon notification take the necessary measures to ensure that the registration of the relying party and the inclusion of relying parties in the authentication mechanism is withdrawn or suspended until the notifying authority confirms that the identified irregularities have been remedied.

(9) All *EDIWs* should ***enable*** users to electronically identify and authenticate online and offline across borders ***to access*** a wide range of public and private services. Without prejudice to Member States' prerogatives as regards the identification of their nationals and residents, ***EDIWs*** can also serve the institutional needs of public administrations, international organisations and the Union's institutions, bodies, offices and agencies. Offline use would be important in many sectors, including in the health sector where services are often provided through face-to-face interaction and ePrescriptions should be able to rely on QR-codes or similar technologies to verify authenticity. Relying on the level of assurance "high", ***EDIWs*** 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. ***When on-boarding into EDIWs, natural persons should be able to sign with qualified electronic signatures, free of charge and by default, without having to go through any additional administrative procedures. This should enable users to sign or seal self-claimed assertions or attributes.*** To achieve simplification and cost reduction benefits to persons and businesses across the ***Union***, including by enabling powers of representation and e-mandates, Member States should ***provide*** *EDIWs* relying on common standards ***and technical specifications*** to ensure seamless interoperability and ***to adequately increase the IT security, strengthen robustness against cyber-attacks and thus significantly***

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

(9a) *The use of qualified electronic signature should be free of charge to all natural persons for* ***non-professional purposes. Member States may provide for measures to prevent the free-of-charge use of qualified electronic signatures by natural persons for professional purposes, ensuring that any such measures are proportionate to identified risks and are justified.***

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

(9a) *EDIWs* ***should include a functionality to generate user chosen and managed pseudonyms, to authenticate when accessing online services.***

(10a) In order to avoid divergent approaches and harmonize the implementation of the requirements laid down by this Regulation, European Digital Identity Wallets should be certified according to common specifications, procedures and reference standards adopted by the Commission according to this Regulation for the purpose of expressing detailed technical specifications of those requirements. For as long and as far as the certification of the conformity of European Digital Identity Wallet with relevant cybersecurity requirements are not covered by cybersecurity certification schemes that are available and referenced in this Regulation, and for as far as non-cybersecurity requirements relevant to the European Digital Identity Wallet are concerned, Member States should establish national certification schemes following the harmonized requirements set out in this Regulation.

(10b) Certification of conformity with the cybersecurity requirements established in this Regulation should, where available, rely on the relevant European cybersecurity certifications schemes

established pursuant to Regulation (EU) 2019/881 which establishes a voluntary European cybersecurity certification framework for ICT products, processes and services.

(10c) In order to continuously assess and mitigate risks linked to security, certified European Digital Identity Wallet should be subject to regular vulnerability assessments aiming at detecting any vulnerability of the certified product, process, and service related components of the European Digital Identity Wallet.

(10d) By protecting users and companies from cybersecurity risks, the essential cybersecurity requirements laid down in this Regulation, are also to contribute to enhancing the protection of personal data and privacy of individuals. Synergies on both standardisation and certification on cybersecurity aspects should be considered through the cooperation between the Commission, the European Standardisation Organisations, the European Union Agency for Cybersecurity (ENISA), the European Data Protection Board (EDPB) established by Regulation (EU) 2016/679, and the national data protection supervisory authorities.

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

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

(11) European Digital Identity Wallets should ensure the highest level of ***data protection and*** security for the ***purposes of authentication and identification to facilitate access to public***

and private services, irrespective of whether such data is stored locally or on cloud-based solutions, taking ***due*** account ***of*** the different levels of risk.

(11a) EDIWs should be secure-by-design and implement advanced security features to protect against identity and other data theft, denial of service and any other cyber threat. This should include state of-the-art encryption and storage methods that are only accessible to and can be decrypted exclusively by the user and rely on end-to-end encrypted communication with other EDIWs and relying parties. Additionally, EDIWs should require secure explicit, and active users' confirmation for the operations performed via the EDIWs.

(11c) The use of the wallet free of charge should not result in the processing of data beyond what is necessary for the provision of wallet services. This Regulation should not allow processing of personal data stored in or resulting from the use of the European Digital Identity Wallet by the provider of the European Digital Identity Wallet for other purposes than the provision of wallet services. To ensure privacy, EDIW providers should ensure unobservability by not collecting data and not having insight into the transactions of the users of the Wallet. This means that the providers should not be able to see the details of the transactions made by the user. However, in specific cases based on the previous explicit consent of users for each of those specific cases, and in full accordance with GDPR, providers of EDIW could be granted access to the information necessary for the provision of a particular service related to the Wallet.

(11d) *The transparency of EDIWs and accountability of their providers are key elements to create social trust and trigger acceptance of the framework. The functioning of European Digital Identity Wallets should therefore be transparent and, in particular, allow for verifiable processing of personal data. To achieve this, Member States should disclose the source code of the user application software components of European Digital Identity Wallets, including those that are related to processing of personal data and data of legal persons. The publication of this source code under an open-source licence should enable society, including users and developers, to understand its operation, audit and review the code. This would increase users' trust in the Wallet ecosystem and contribute to the security of EDIWs by enabling anyone to report vulnerabilities and errors in the code. Overall, this should incentivise suppliers to deliver and maintain a highly secure product.* ***However, there are cases where the disclosure of the source code for the libraries used, communication channel or other elements that are not hosted on user device, could be limited by Member States, for duly justified reasons, especially for public security purposes.***

(11e) The use of the EDIWs as well as the discontinuation of their use should be the exclusive right and choice of users. Member States should develop simple and secure procedures for the users to request immediate revocation of validity of EDIWs, including in case of loss or theft. Upon the death of the user or the cessation of activity by a legal person, a mechanism should be established to enable the authority responsible for settling the succession of the natural person or assets of the legal person to request the immediate termination of EDIWs.

(11f) In order to promote uptake of the EDIWs and wider use of digital identities, Member States should not only show the benefits of the relevant services, but also, in cooperation with the private sector, researchers and academia, develop training programmes aiming to strengthen the digital skills of their citizens and residents, in particular for vulnerable groups

such as persons with disabilities and older persons. *Member States should also raise awareness about the benefits and risks of the European Digital Identity Wallet by means of communication campaigns.*

(12) To ensure that the European Digital Identity framework is open to innovation, technological development and future-proof, Member States ***are*** encouraged to ***jointly set up*** sandboxes to test innovative solutions in a controlled and secure environment in particular to improve the functionality, protection of personal data, security and interoperability of the solutions and to inform future updates of technical references and legal requirements. This environment should foster the inclusion of European ***SMEs, start-ups and individual innovators and researchers, as well as relevant industry stakeholders. Such initiatives should contribute to and strengthen the regulatory compliance and technical robustness of the EDIWs to be provided to the citizens, thus preventing the development of solutions non-compliant with Union law on data protection or open to security vulnerabilities***.

(13) Regulation (EU) No 2019/1157 strengthens the security of identity cards with enhanced security features by August 2021. Member States should consider the feasibility of notifying them under electronic identification schemes to extend the cross-border availability of electronic identification means.

(14) The process of notification of electronic identification schemes should be simplified and accelerated to promote the access to convenient, trusted, secure and innovative authentication and identification solutions and, where relevant, to encourage private identity providers to offer electronic identification schemes to Member State's authorities for notification as national electronic ***identification*** schemes under Regulation 910/2014.

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

(16) Member States should benefit from new, flexible tools to ensure compliance with the requirements of this Regulation and of the relevant implementing acts. This Regulation should allow Member States to use reports and assessments**,** performed by accredited conformity assessment bodies***, as provided for in the context of*** certification schemes to be established at Union level under Regulation (EU) 2019/881, to support their claims on the alignment of the schemes or of parts thereof with the requirements of the Regulation on the interoperability and the security of the notified electronic identification schemes.

(17) ***Public*** service providers use the person identification data available from electronic identification ***means*** pursuant to Regulation (EU) No 910/2014 ***to match the electronic identity of the users from other Member States with the person identification data provided to those*** users ***in the*** Member State ***performing the cross-border*** identity ***matching process***. However, ***in many cases,*** despite the use of the eIDAS ***minimum*** data set, ***ensuring accurate identity matching when Member States act as relying parties require*** additional information about the user and specific ***complementary*** unique identification procedures ***to be performed*** at

national level. To further support the usability of electronic identification means, ***provide better online public services and increase legal certainty in relation to the*** electronic ***identity of the users***, this Regulation should require ***Member States to take specific online measures to ensure unequivocal identity matching when users intend to access cross-border public services online***.

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

(18) In ***accordance*** with Directive (EU) 2019/882, 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.

(18a) In order to ensure effective enforcement of the obligations laid down in this Regulation, a minimum for the maximum of administrative fines for both qualified and non-qualified trust service providers should be established. Member States should implement penalties regimes providing for effective, proportionate and dissuasive sanctions. When determining the penalties, the size of the affected entities, their business models and the severity of the breaches should be duly taken into consideration.

(18b) Member States should lay down rules on penalties for infringements such as direct or indirect practices leading to confusion between non-qualified and qualified trust services or to the abusive use of the EU trust mark by non-qualified trust service providers. The EU trust mark should not be used under conditions which, directly or indirectly, lead to the belief that any non-qualified trust services offered by these providers are qualified.

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

(20) The provision and use of trust services ***and the benefits brought in terms of convenience and legal certainty in the context of cross-border transactions, in particular when qualified trust services are used,*** are becoming increasingly important for international trade and cooperation. International partners of the EU are establishing trust frameworks inspired by Regulation (EU) No 910/2014. In order to facilitate the recognition of ***qualified trust*** 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***. Such an approach should*** complement the possibility ***for*** 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 (EU) 2022/2555 and Regulation (EU) 2016/679 should also be ensured, as well as the use of trusted lists as essential elements to build trust.***

(21a) This Regulation should foster choice and the possibility of switching between EDIWs, where a Member State has endorsed more than one EDIW solution on its territory. In order to avoid lock-in effects in such situations, where technically feasible, the providers of EDIWs should ensure the effective portability of data at the request of EDIW users, and should not be allowed to use contractual, economic or technical barriers to prevent or to discourage effective switching between different EDIWs.

(21b) To ensure the proper functioning of the European Digital Identity Wallets, 'wallet' providers need effective interoperability and fair, reasonable and non-discriminatory conditions for the 'wallet' to access specific hardware and software features of mobile devices. These components may include in particular but not exclusively, Near Field Communication antennas and secure elements (including Universal Integrated Circuit Cards, embedded secure elements, microSD cards and Bluetooth Low Energy). The access to these components may be under the control of mobile network operators and equipment manufacturers. Therefore, whenever needed to provide the services of the European Digital Identity Wallets, original equipment manufacturers of mobile devices or providers of electronic communication services should not refuse access to such components. In addition, the undertakings that are designated gatekeepers for enumerated core platform services by the European Commission under Regulation (EU) 2022/1925, should remain subject to the specific provisions of such Regulation, building on Article 6(7) of the Regulation (EU) 2022/1925 of the European Parliament and of the Council.

(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 ***EU 2022/2555***, trust services are required to take appropriate technical and organisational measures pursuant to Directive ***EU 2022/2555***, 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 ***EU 2022/2555***. 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 ***EU 2022/2555*** 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 ***EU 2022/2555***. 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 ***(EU) 2022/2555***, 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 ***(EU) 2022/2555***. In particular, the supervisory bodies under this Regulation should be entitled to request the competent authority under Directive ***(EU) 2022/2555*** 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 ***Directive (EU) 2022/2555*** or require them to remedy non-compliance.

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

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

(26) It should be possible to issue and handle trustworthy ***electronic*** 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 ***issues attested attributes in electronic form*** such as diplomas, ***licenses, birth*** certificates ***or powers and mandates to represent or act on behalf of natural or legal persons*** should ***be considered as a trust service provider of electronic attestation of attributes***. An electronic attestation of attributes should not be denied legal effect on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic attestation of attributes***. Relying parties should be able to use the electronic attestations of attributes as equivalent to attestations in paper format***. 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) ***The*** wide availability and usability of ***EDIWs should rely on*** their acceptance ***and trust by both private individuals and*** private service providers. ***Therefore,*** private relying parties providing services ***such as*** in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, ***telecommunications or education*** should accept the use of ***EDIWs*** for the provision of services where strong user authentication for online identification is required by ***Union or national*** law or by contractual obligation. ***The request for information to the EUDIW user*** should be ***necessary and proportionate with the intended use case and in line with*** the principle of data minimisation ***and ensure transparency over which data is shared and for what purposes***. ***To facilitate the use and*** acceptance of ***the*** European Digital Identity Wallets***, widely accepted industry standards and specifications*** should be ***taken into account in*** their deployment.

(28a) Where very large online platforms as defined in Article 25(1) of Regulation (EU) 2022/2065 require users to authenticate to access online services, those platforms should be mandated to accept the use of EDIWs upon voluntary request of the user. Users should be under no obligation to use EDIWs to access private services and should not be restricted or hindered in their access to services on the grounds that they do not use an EDIW. However, if users wish to do so, very large online platforms should accept EDIWs for this purpose while respecting the principle of data minimisation and the right of the users to use freely chosen pseudonyms. Given the importance of very large online platforms, due to their reach, in particular as expressed in number of recipients of the service and economic transactions this is necessary to increase the protection of users from fraud and secure a high level of data protection.

(28b) Codes of conduct at Union level should be developed in order to contribute to wide availability and usability of electronic identification means, including EDIWs within the scope of this Regulation. The codes of conduct should facilitate wide acceptance of electronic identification means including EDIWs by those service providers which do not qualify as very large platforms and which rely on third party electronic identification services for user authentication.

(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 such information that is necessary for the provision of a service requested by a user.*** The European Digital Identity Wallet should technically enable the selective disclosure of attributes to relying parties. ***Such selectively disclosed attributes, including when originally parts of multiple distinct electronic attestations, may be subsequently combined and presented to relying parties by the user.*** This feature should become a basic design feature ***of EDIWs*** thereby reinforcing convenience and ***the*** protection ***of personal data, including data minimization***.

(29a) Unless specific rules of Union or national law require users to identify themselves, accessing services by using a pseudonym should not be prohibited.

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

(31) Secure electronic identification and the provision of attestation of attributes should offer additional flexibility and solutions for the financial services sector to allow identification of customers and the exchange of specific attributes necessary to comply with, for example, customer due diligence requirements under the Anti Money Laundering Regulation, [reference to be added after the adoption of the proposal], with suitability requirements stemming from investor protection legislation, or to support the fulfilment of strong customer authentication requirements for ***online identification for the purposes of*** account login and ***of*** initiation of transactions in the field of payment services.

(31a) This Regulation should establish the principle that the legal effect of an electronic signature cannot be challenged on the grounds that it is in an electronic form or that it does not meet the requirements of the qualified electronic signature. However, it is for national law to define the legal effect of electronic signatures, except for the requirements provided for in this Regulation according to which the legal effect of a qualified electronic signature it is to be equivalent to that of a handwritten signature. In determining the legal effects of electronic signatures Member States should take into account the principle of proportionality between the judicial value of a document to be signed and level of security and cost that an electronic signature requires. To increase the accessibility and use of electronic signatures, Member States are encouraged to consider the use of advanced electronic signatures in the day-to- day transactions for which they provide a sufficient level of security and confidence.

(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 the receiving Member States from allowing public or private bodies that have certified qualified electronic

signature creation devices to temporarily extend the recognition of the validity of certification when a recertification of the same device could not be performed within the legally defined time frame 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 assurance ***with a high level of confidence in the identity of the*** entity standing behind the website***, irrespective of the platform used to display it.*** Those services ***should*** contribute to the building of trust n conducting business online, as users ***would*** have confidence in a website that has been authenticated. The use of website authentication services by websites ***should be*** voluntary. In order for website authentication to become a means to ***increase*** trust, ***and to provide*** a better experience for the user and ***to foster*** growth in the internal market, this Regulation lays down ***a trust framework including*** minimal security and liability obligations for the providers of ***qualified*** website authentication services and ***requirements for the provision of*** their services. ***National trusted lists should confirm the qualified status of website authentication services and of their trust service providers, including their full compliance with the requirements of this Regulation with regards to the issuance of qualified certificates for website authentication. Recognition of QWACs means that the providers of web-browsers should not deny the authenticity of qualified certificates for website authentication for the sole purpose of attesting the link between the website domain name and the natural or legal person to whom the certificate is issued and confirming the identity of that person. Providers of web-browsers should display in a user-friendly manner the certified identity data and the other attested attributes to the end-user, in the browser environment, by relying on technical implementations of their choice.*** To that end, ***providers of*** web-browsers should ensure support and interoperability with qualified certificates for website authentication ***issued in full compliance with the requirement of this Regulation***. ***The obligation of recognition, interoperability and support of QWACs is not to affect the freedom of web-browser providers to ensure web security, domain*** authentication ***and the encryption of web traffic in the manner and with the technology they consider most appropriate. In order to contribute to the online security of end-users, providers of web-browsers should be able to take measures, in exceptional circumstances, that are both necessary and proportionate in reaction to substantiated concerns on breaches of security or loss of integrity of an identified certificate or set of certificates. In this case, while taking any such precautionary measures, web-browser providers should notify without undue delay the national supervisory body and the Commission, the entity to whom the certificate was issued and the qualified trust service provider that issued that certificate or set of certificates of any such concern of a security breach as well as the measures taken relating to a single certificate or a set of certificates. These measures, should be without prejudice to the obligation of the browsers to recognize qualified website authentication certificates in accordance with the national trusted lists.*** To further ***protect citizens and*** promote their usage, public authorities in Member States should consider incorporating qualified certificates for website authentication in their websites.

The measures put forward by this Regulation aiming to bring increased coherence between Member States' divergent approaches and practices related to supervisory procedures should contribute to improved trust and confidence in the security, quality and availability of Qualified Website Authentication Certificates (QWACs).

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

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

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

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

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

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

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

(36e) This Regulation should set out an obligation for qualified trust service providers to verify the identity of a natural or legal person to whom the qualified certificate or the qualified electronic attestation of attribute is issued based on various harmonized methods across the EU. To ensure that qualified certificates and qualified electronic attestations of attributes are issued to the person to whom they belong and that they attest the correct and unique set of data representing the identity of that person, qualified trust service providers issuing qualified certificates or issuing qualified electronic attestations of attributes should, at the

moment of their issuance, ensure with full certainty the identification of that person. Moreover, in addition to the mandatory verification of the identity of the person, if applicable for the issuance of qualified certificates and when issuing a qualified electronic attestation of attributes, qualified trust service providers should ensure with full certainty the correctness and accuracy of the attested attributes of the person to whom the qualified certificate or the qualified electronic attestation of attributes is issued. These obligations of result and full certainty in verifying the attested data should be supported by appropriate means, including by using one or, when required, a combination of specific methods prescribed by this Regulation. These methods may be combined to provide an appropriate basis for the verification of the identity of the person to whom the qualified certificate or a qualified electronic attestation of attributes is issued. Such a combination may include the reliance on electronic identification means which meet the requirements of level of assurance 'substantial' in combination with other supplementary means of identity verification which would allow the fulfillment of the harmonized requirements set out in this Regulation as regards level of assurance 'high' as part of additional harmonized remote procedures which ensures the identification of the person with a high level of confidence. Those methods should include the possibility for the qualified trust service provider issuing a qualified electronic attestation of attributes to verify the attributes to be attested by electronic means at the request of the user and in accordance with national or Union law, including against authentic sources.

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

(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.

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

HAVE ADOPTED THIS REGULATION:

~~REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL~~

~~of 23 July 2014~~

~~on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC~~

~~THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,~~

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

~~Having regard to the proposal from the European Commission,~~

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

Having regard to the opinion of the European Economic and Social Committee (1),

Acting in accordance with the ordinary legislative procedure (2),

Whereas:

(1)

Building trust in the online environment is key to economic and social development. Lack of trust, in particular because of a perceived lack of legal certainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically and to adopt new services.

(2)

This Regulation seeks to enhance trust in electronic transactions in the internal market by providing a common foundation for secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.

(3)

Directive 1999/93/EC of the European Parliament and of the Council (3), dealt with electronic signatures without delivering a comprehensive cross-border and cross-sector framework for secure, trustworthy and easy-to-use electronic transactions. This Regulation enhances and expands the acquis of that Directive.

(4)

The Commission communication of 26 August 2010 entitled 'A Digital Agenda for Europe' identified the fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy. In its EU Citizenship Report 2010, entitled 'Dismantling the obstacles to EU citizens' rights', the Commission further highlighted the need to solve the main problems that prevent Union citizens from enjoying the benefits of a digital single market and cross-border digital services.

(5)

In its conclusions of 4 February 2011 and of 23 October 2011, the European Council invited the Commission to create a digital single market by 2015, to make rapid progress in key areas of the digital economy and to promote a fully integrated digital single market by facilitating the cross-border use of online services, with particular attention to facilitating secure electronic identification and authentication.

(6)

In its conclusions of 27 May 2011, the Council invited the Commission to contribute to the digital single market by creating appropriate conditions for the mutual recognition of key enablers across borders, such as electronic identification, electronic documents, electronic signatures and electronic delivery services, and for interoperable e-government services across the European Union.

~~(7)~~

~~The European Parliament, in its resolution of 21 September 2010 on completing the internal market for e-commerce (4), stressed the importance of the security of electronic services, especially of electronic signatures, and of the need to create a public key infrastructure at pan-European level, and called on the Commission to set up a European validation authorities gateway to ensure the cross-border interoperability of electronic signatures and to increase the security of transactions carried out using the internet.~~

~~(8)~~

~~Directive 2006/123/EC of the European Parliament and of the Council (5) requires Member States to establish 'points of single contact' (PSCs) to ensure that all procedures and formalities relating to access to a service activity and to the exercise thereof can be easily completed, at a distance and by electronic means, through the appropriate PSC with the appropriate authorities. Many online services accessible through PSCs require electronic identification, authentication and signature.~~

~~(9)~~

~~In most cases, citizens cannot use their electronic identification to authenticate themselves in another Member State because the national electronic identification schemes in their country are not recognised in other Member States. That electronic barrier excludes service providers from enjoying the full benefits of the internal market. Mutually recognised electronic identification means will facilitate cross-border provision of numerous services in the internal market and enable businesses to operate on a cross-border basis without facing many obstacles in interactions with public authorities.~~

~~(10)~~

~~Directive 2011/24/EU of the European Parliament and of the Council (6) set up a network of national authorities responsible for e-health. To enhance the safety and the continuity of cross-border healthcare, the network is required to produce guidelines on cross-border access to electronic health data and services, including by supporting 'common identification and authentication measures to facilitate transferability of data in cross-border healthcare'. Mutual recognition of electronic identification and authentication is key to making cross-border healthcare for European citizens a reality. When people travel for treatment, their medical data need to be accessible in the country of treatment. That requires a solid, safe and trusted electronic identification framework.~~

~~(11)~~

~~This Regulation should be applied in full compliance with the principles relating to the protection of personal data provided for in Directive 95/46/EC of the European Parliament and of the Council (7). In this respect, having regard to the principle of mutual recognition established by this Regulation, authentication for an online service should concern processing of only those identification data that are adequate, relevant and not excessive to grant access to that service online. Furthermore, requirements under Directive 95/46/EC concerning confidentiality and security of processing should be respected by trust service providers and supervisory bodies.~~

~~(12)~~

~~One of the objectives of this Regulation is to remove existing barriers to the cross-border use of electronic identification means used in the Member States to authenticate, for at least public services. This Regulation does not aim to intervene with regard to electronic identity management systems and related infrastructures established in Member States. The aim of this Regulation is to ensure that for access to cross-border online services offered by Member States, secure electronic identification and authentication is possible.~~

~~(13)~~

~~Member States should remain free to use or to introduce means for the purposes of electronic identification for accessing online services. They should also be able to decide whether to involve the private sector in the provision of those means. Member States should not be obliged to notify their electronic identification schemes to the Commission. The choice to notify the Commission of all, some or none of the electronic identification schemes used at national level to access at least public online services or specific services is up to Member States.~~

~~(14)~~

~~Some conditions need to be set out in this Regulation with regard to which electronic identification means have to be recognised and how the electronic identification schemes should be notified. Those conditions should help Member States to build the necessary trust in each other's electronic identification schemes and to mutually recognise electronic identification means falling under their notified schemes. The principle of mutual recognition should apply if the notifying Member State's electronic identification scheme meets the conditions of notification and the notification was published in the Official Journal of the European Union. However, the principle of mutual recognition should only relate to authentication for an online service. The access to those online services and their final delivery to the applicant should be closely linked to the right to receive such services under the conditions set out in national legislation.~~

~~(15)~~

~~The obligation to recognise electronic identification means should relate only to those means the identity assurance level of which corresponds to the level equal to or higher than the level required for the online service in question. In addition, that obligation should only apply when the public sector body in question uses the assurance level 'substantial' or 'high' in relation to accessing that service online. Member States should remain free, in accordance with Union law, to recognise electronic identification means having lower identity assurance levels.~~

~~(16)~~

~~Assurance levels should characterise the degree of confidence in electronic identification means in establishing the identity of a person, thus providing assurance that the person claiming a particular identity is in fact the person to which that identity was assigned. The assurance level depends on the~~

~~degree of confidence that electronic identification means provides in claimed or asserted identity of a person taking into account processes (for example, identity proofing and verification, and authentication), management activities (for example, the entity issuing electronic identification means and the procedure to issue such means) and technical controls implemented. Various technical definitions and descriptions of assurance levels exist as the result of Union-funded Large-Scale Pilots, standardisation and international activities. In particular, the Large-Scale Pilot STORK and ISO 29115 refer, inter alia, to levels 2, 3 and 4, which should be taken into utmost account in establishing minimum technical requirements, standards and procedures for the assurances levels low, substantial and high within the meaning of this Regulation, while ensuring consistent application of this Regulation in particular with regard to assurance level high related to identity proofing for issuing qualified certificates. The requirements established should be technology neutral. It should be possible to achieve the necessary security requirements through different technologies.~~

~~(17)~~

~~Member States should encourage the private sector to voluntarily use electronic identification means under a notified scheme for identification purposes when needed for online services or electronic transactions. The possibility to use such electronic identification means would enable the private sector to rely on electronic identification and authentication already largely used in many Member States at least for public services and to make it easier for businesses and citizens to access their online services across borders. In order to facilitate the use of such electronic identification means across borders by the private sector, the authentication possibility provided by any Member State should be available to private sector relying parties established outside of the territory of that Member State under the same conditions as applied to private sector relying parties established within that Member State. Consequently, with regard to private sector relying parties, the notifying Member State may define terms of access to the authentication means. Such terms of access may inform whether the authentication means related to the notified scheme is presently available to private sector relying parties.~~

~~(18)~~

~~This Regulation should provide for the liability of the notifying Member State, the party issuing the electronic identification means and the party operating the authentication procedure for failure to comply with the relevant obligations under this Regulation. However, this Regulation should be applied in accordance with national rules on liability. Therefore, it does not affect those national rules on, for example, definition of damages or relevant applicable procedural rules, including the burden of proof.~~

~~(19)~~

~~The security of electronic identification schemes is key to trustworthy cross-border mutual recognition of electronic identification means. In this context, Member States should cooperate with regard to the security and interoperability of the electronic identification schemes at Union level. Whenever electronic identification schemes require specific hardware or software to be used by relying parties at the national level, cross-border interoperability calls for those Member States not to impose such requirements and related costs on relying parties established outside of their territory. In that case appropriate solutions should be discussed and developed within the scope of the interoperability framework. Nevertheless technical requirements stemming from the inherent specifications of~~

~~national electronic identification means and likely to affect the holders of such electronic means (e.g. smartcards), are unavoidable.~~

~~(20)~~

~~Cooperation by Member States should facilitate the technical interoperability of the notified electronic identification schemes with a view to fostering a high level of trust and security appropriate to the degree of risk. The exchange of information and the sharing of best practices between Member States with a view to their mutual recognition should help such cooperation.~~

~~(21)~~

~~This Regulation should also establish a general legal framework for the use of trust services. However, it should not create a general obligation to use them or to install an access point for all existing trust services. In particular, it should not cover the provision of services used exclusively within closed systems between a defined set of participants, which have no effect on third parties. For example, systems set up in businesses or public administrations to manage internal procedures making use of trust services should not be subject to the requirements of this Regulation. Only trust services provided to the public having effects on third parties should meet the requirements laid down in the Regulation. Neither should this Regulation 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.~~

~~(22)~~

~~In order to contribute to their general cross-border use, it should be possible to use trust services as evidence in legal proceedings in all Member States. It is for the national law to define the legal effect of trust services, except if otherwise provided in this Regulation.~~

~~(23)~~

~~To the extent that this Regulation creates an obligation to recognise a trust service, such a trust service may only be rejected if the addressee of the obligation is unable to read or verify it due to technical reasons lying outside the immediate control of the addressee. However, that obligation should not in itself require a public body to obtain the hardware and software necessary for the technical readability of all existing trust services.~~

~~(24)~~

~~Member States may maintain or introduce national provisions, in conformity with Union law, relating to trust services as far as those services are not fully harmonised by this Regulation. However, trust services that comply with this Regulation should circulate freely in the internal market.~~

~~(25)~~

~~Member States should remain free to define other types of trust services in addition to those making part of the closed list of trust services provided for in this Regulation, for the purpose of recognition at national level as qualified trust services.~~

~~(26)~~

~~Because of the pace of technological change, this Regulation should adopt an approach which is open to innovation.~~

~~(27)~~

~~This Regulation should be technology neutral. The legal effects it grants should be achievable by any technical means provided that the requirements of this Regulation are met.~~

~~(28)~~

~~To enhance in particular the trust of small and medium-sized enterprises (SMEs) and consumers in the internal market and to promote the use of trust services and products, the notions of qualified trust services and qualified trust service provider should be introduced with a view to indicating requirements and obligations that ensure high-level security of whatever qualified trust services and products are used or provided.~~

~~(29)~~

~~In line with the obligations under the United Nations Convention on the Rights of Persons with Disabilities, approved by Council Decision 2010/48/EC (8), in particular Article 9 of the Convention, persons with disabilities should be able to use trust services and end-user products used in the provision of those services on an equal basis with other consumers. Therefore, where feasible, trust services provided and end-user products used in the provision of those services should be made accessible for persons with disabilities. The feasibility assessment should include, inter alia, technical and economic considerations.~~

~~(30)~~

~~Member States should designate a supervisory body or supervisory bodies to carry out the supervisory activities under this Regulation. Member States should also be able to decide, upon a mutual agreement with another Member State, to designate a supervisory body in the territory of that other Member State.~~

~~(31)~~

~~Supervisory bodies should cooperate with data protection authorities, for example, by informing them about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached. The provision of information should in particular cover security incidents and personal data breaches.~~

~~(32)~~

~~It should be incumbent on all trust service providers to apply good security practice appropriate to the risks related to their activities so as to boost users' trust in the single market.~~

~~(33)~~

~~Provisions on the use of pseudonyms in certificates should not prevent Member States from requiring identification of persons pursuant to Union or national law.~~

~~(34)~~

All Member States should follow common essential supervision requirements to ensure a comparable security level of qualified trust services. To ease the consistent application of those requirements across the Union, Member States should adopt comparable procedures and should exchange information on their supervision activities and best practices in the field.

(35)

All trust service providers should be subject to the requirements of this Regulation, in particular those on security and liability to ensure due diligence, transparency and accountability of their operations and services. However, taking into account the type of services provided by trust service providers, it is appropriate to distinguish as far as those requirements are concerned between qualified and non-qualified trust service providers.

(36)

Establishing a supervisory regime for all trust service providers should ensure a level playing field for the security and accountability of their operations and services, thus contributing to the protection of users and to the functioning of the internal market. Non-qualified trust service providers should be subject to a light touch and reactive ex post supervisory activities justified by the nature of their services and operations. The supervisory body should therefore have no general obligation to supervise non-qualified service providers. The supervisory body should only take action when it is informed (for example, by the non-qualified trust service provider itself, by another supervisory body, by a notification from a user or a business partner or on the basis of its own investigation) that a non-qualified trust service provider does not comply with the requirements of this Regulation.

(37)

This Regulation should provide for the liability of all trust service providers. In particular, it establishes the liability regime under which all trust service providers should be liable for damage caused to any natural or legal person due to failure to comply with the obligations under this Regulation. In order to facilitate the assessment of financial risk that trust service providers might have to bear or that they should cover by insurance policies, this Regulation allows trust service providers to set limitations, under certain conditions, on the use of the services they provide and not to be liable for damages arising from the use of services exceeding such limitations. Customers should be duly informed about the limitations in advance. Those limitations should be recognisable by a third party, for example by including information about the limitations in the terms and conditions of the service provided or through other recognisable means. For the purposes of giving effect to those principles, this Regulation should be applied in accordance with national rules on liability. Therefore, this Regulation does not affect those national rules on, for example, definition of damages, intention, negligence, or relevant applicable procedural rules.

(38)

Notification of security breaches and security risk assessments is essential with a view to providing adequate information to concerned parties in the event of a breach of security or loss of integrity.

(39)

To enable the Commission and the Member States to assess the effectiveness of the breach notification mechanism introduced by this Regulation, supervisory bodies should be requested to

~~provide summary information to the Commission and to European Union Agency for Network and Information Security (ENISA).~~

~~(40)~~

~~To enable the Commission and the Member States to assess the effectiveness of the enhanced supervision mechanism introduced by this Regulation, supervisory bodies should be requested to report on their activities. This would be instrumental in facilitating the exchange of good practice between supervisory bodies and would ensure the verification of the consistent and efficient implementation of the essential supervision requirements in all Member States.~~

~~(41)~~

~~To ensure sustainability and durability of qualified trust services and to boost users' confidence in the continuity of qualified trust services, supervisory bodies should verify the existence and the correct application of provisions on termination plans in cases where qualified trust service providers cease their activities.~~

~~(42)~~

~~To facilitate the supervision of qualified trust service providers, for example, when a provider is providing its services in the territory of another Member State and is not subject to supervision there, or when the computers of a provider are located in the territory of a Member State other than the one where it is established, a mutual assistance system between supervisory bodies in the Member States should be established.~~

~~(43)~~

~~In order to ensure the compliance of qualified trust service providers and the services they provide with the requirements set out in this Regulation, a conformity assessment should be carried out by a conformity assessment body and the resulting conformity assessment reports should be submitted by the qualified trust service providers to the supervisory body. Whenever the supervisory body requires a qualified trust service provider to submit an ad hoc conformity assessment report, the supervisory body should respect, in particular, the principles of good administration, including the obligation to give reasons for its decisions, as well as the principle of proportionality. Therefore, the supervisory body should duly justify its decision to require an ad hoc conformity assessment.~~

~~(44)~~

~~This Regulation aims to ensure a coherent framework with a view to providing a high level of security and legal certainty of trust services. In this regard, when addressing the conformity assessment of products and services, the Commission should, where appropriate, seek synergies with existing relevant European and international schemes such as the Regulation (EC) No 765/2008 of the European Parliament and of the Council (9) which sets out the requirements for accreditation of conformity assessment bodies and market surveillance of products.~~

~~(45)~~

~~In order to allow an efficient initiation process, which should lead to the inclusion of qualified trust service providers and the qualified trust services they provide into trusted lists, preliminary interactions between prospective qualified trust service providers and the competent supervisory body should be encouraged with a view to facilitating the due diligence leading to the provisioning of qualified trust services.~~

~~(46)~~

~~Trusted lists are essential elements in the building of trust among market operators as they indicate the qualified status of the service provider at the time of supervision.~~

~~(47)~~

~~Confidence in and convenience of online services are essential for users to fully benefit and consciously rely on electronic services. To this end, an EU trust mark should be created to identify the qualified trust services provided by qualified trust service providers. Such an EU trust mark for qualified trust services would clearly differentiate qualified trust services from other trust services thus contributing to transparency in the market. The use of an EU trust mark by qualified trust service providers should be voluntary and should not lead to any requirement other than those provided for in this Regulation.~~

~~(48)~~

~~While a high level of security is needed to ensure mutual recognition of electronic signatures, in specific cases, such as in the context of Commission Decision 2009/767/EC (10), electronic signatures with a lower security assurance should also be accepted.~~

~~(49)~~

~~This Regulation should establish the principle that an electronic signature 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 signature. However, it is for national law to define the legal effect of electronic signatures, except for the requirements provided for in this Regulation according to which a qualified electronic signature should have the equivalent legal effect of a handwritten signature.~~

~~(50)~~

~~As competent authorities in the Member States currently use different formats of advanced electronic signatures to sign their documents electronically, it is necessary to ensure that at least a number of advanced electronic signature formats can be technically supported by Member States when they receive documents signed electronically. Similarly, when competent authorities in the Member States use advanced electronic seals, it would be necessary to ensure that they support at least a number of advanced electronic seal formats.~~

~~(51)~~

~~It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device.~~

~~(52)~~

~~The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust service provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to guarantee that the electronic signature creation environment is reliable and is used under the sole control of the signatory. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply.~~

~~(53)~~

~~The suspension of qualified certificates is an established operational practice of trust service providers in a number of Member States, which is different from revocation and entails the temporary loss of validity of a certificate. Legal certainty calls for the suspension status of a certificate to always be clearly indicated. To that end, trust service providers should have the responsibility to clearly indicate the status of the certificate and, if suspended, the precise period of time during which the certificate has been suspended. This Regulation should not impose the use of suspension on trust service providers or Member States, but should provide for transparency rules when and where such a practice is available.~~

~~(54)~~

~~Cross-border interoperability and recognition of qualified certificates is a precondition for cross-border recognition of qualified electronic signatures. Therefore, qualified certificates should not be subject to any mandatory requirements exceeding the requirements laid down in this Regulation. However, at national level, the inclusion of specific attributes, such as unique identifiers, in qualified certificates should be allowed, provided that such specific attributes do not hamper cross-border interoperability and recognition of qualified certificates and electronic signatures.~~

~~(55)~~

~~IT security certification based on international standards such as ISO 15408 and related evaluation methods and mutual recognition arrangements is an important tool for verifying the security of qualified electronic signature creation devices and should be promoted. However, innovative solutions and services such as mobile signing and cloud signing rely on technical and organisational solutions for qualified electronic signature creation devices for which security standards may not yet be available or for which the first IT security certification is ongoing. The level of security of such qualified electronic signature creation devices could be evaluated by using alternative processes only where such security standards are not available or where the first IT security certification is ongoing. Those processes should be comparable to the standards for IT security certification insofar as their security levels are equivalent. Those processes could be facilitated by a peer review.~~

~~(56)~~

~~This Regulation should lay down requirements for qualified electronic signature creation devices to ensure the functionality of advanced electronic signatures. This Regulation should not cover the entire system environment in which such devices operate. Therefore, the scope of the certification of~~

~~qualified signature creation devices should be limited to the hardware and system software used to manage and protect the signature creation data created, stored or processed in the signature creation device. As detailed in relevant standards, the scope of the certification obligation should exclude signature creation applications.~~

~~(57)~~

~~To ensure legal certainty as regards the validity of the signature, it is essential to specify the components of a qualified electronic signature, which should be assessed by the relying party carrying out the validation. Moreover, specifying the requirements for qualified trust service providers that can provide a qualified validation service to relying parties unwilling or unable to carry out the validation of qualified electronic signatures themselves, should stimulate the private and public sector to invest in such services. Both elements should make qualified electronic signature validation easy and convenient for all parties at Union level.~~

~~(58)~~

~~When a transaction requires a qualified electronic seal from a legal person, a qualified electronic signature from the authorised representative of the legal person should be equally acceptable.~~

~~(59)~~

~~Electronic seals should serve as evidence that an electronic document was issued by a legal person, ensuring certainty of the document's origin and integrity.~~

~~(60)~~

~~Trust service providers issuing qualified certificates for electronic seals should implement the necessary measures in order to be able to establish the identity of the natural person representing the legal person to whom the qualified certificate for the electronic seal is provided, when such identification is necessary at national level in the context of judicial or administrative proceedings.~~

~~(61)~~

~~This Regulation should ensure the long-term preservation of information, in order to ensure the legal validity of electronic signatures and electronic seals over extended periods of time and guarantee that they can be validated irrespective of future technological changes.~~

~~(62)~~

~~In order to ensure the security of qualified electronic time stamps, this Regulation should require the use of an advanced electronic seal or an advanced electronic signature or of other equivalent methods. It is foreseeable that innovation may lead to new technologies that may ensure an equivalent level of security for time stamps. Whenever a method other than an advanced electronic seal or an advanced electronic signature is used, it should be up to the qualified trust service provider to demonstrate, in the conformity assessment report, that such a method ensures an equivalent level of security and complies with the obligations set out in this Regulation.~~

~~(63)~~

~~Electronic documents are important for further development of cross-border electronic transactions in the internal market. This Regulation should establish the principle that an electronic document~~

~~should not be denied legal effect on the grounds that it is in an electronic form in order to ensure that an electronic transaction will not be rejected only on the grounds that a document is in electronic form.~~

~~(64)~~

~~When addressing formats of advanced electronic signatures and seals, the Commission should build on existing practices, standards and legislation, in particular Commission Decision 2011/130/EU (11).~~

~~(65)~~

~~In addition to authenticating the document issued by the legal person, electronic seals can be used to authenticate any digital asset of the legal person, such as software code or servers.~~

~~(66)~~

~~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.~~

~~(67)~~

~~Website authentication services provide a means by which a visitor to a website can be assured that there is a genuine and legitimate entity standing behind the website. Those services contribute to the building of trust and confidence in conducting business online, as users will have confidence in a website that has been authenticated. The provision and the use of website authentication services are entirely voluntary. However, in order for website authentication to become a means to boosting trust, providing a better experience for the user and furthering growth in the internal market, this Regulation should lay down minimal security and liability obligations for the providers and their services. To that end, the results of existing industry-led initiatives, for example the Certification Authorities/Browsers Forum — CA/B Forum, have been taken into account. In addition, this Regulation should not impede the use of other means or methods to authenticate a website not falling under this Regulation nor should it prevent third country providers of website authentication services from providing their services to customers in the Union. However, a third country provider should only have its website authentication services recognised as qualified in accordance with this Regulation, if an international agreement between the Union and the country of establishment of the provider has been concluded.~~

~~(68)~~

~~The concept of 'legal persons', according to the provisions of the Treaty on the Functioning of the European Union (TFEU) on establishment, leaves operators free to choose the legal form which they deem suitable for carrying out their activity. Accordingly, 'legal persons', within the meaning of the TFEU, means all entities constituted under, or governed by, the law of a Member State, irrespective of their legal form.~~

~~(69)~~

~~The Union institutions, bodies, offices and agencies are encouraged to recognise electronic identification and trust services covered by this Regulation for the purpose of administrative~~

~~cooperation capitalising, in particular, on existing good practices and the results of ongoing projects in the areas covered by this Regulation.~~

~~(70)~~

~~In order to complement certain detailed technical aspects of this Regulation in a flexible and rapid manner, the power to adopt acts in accordance with Article 290 TFEU should be delegated to the Commission in respect of criteria to be met by the bodies responsible for the certification of qualified electronic signature creation devices. It is of particular importance that the Commission carry out appropriate consultations during its preparatory work, including at expert level. The Commission, when preparing and drawing up delegated acts, should ensure a simultaneous, timely and appropriate transmission of relevant documents to the European Parliament and to the Council.~~

~~(71)~~

~~In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission, in particular for specifying reference numbers of standards the use of which would raise a presumption of compliance with certain requirements laid down in this Regulation. Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council (12).~~

~~(72)~~

~~When adopting delegated or implementing acts, the Commission should take due account of the standards and technical specifications drawn up by European and international standardisation organisations and bodies, in particular the European Committee for Standardisation (CEN), the European Telecommunications Standards Institute (ETSI), the International Organisation for Standardisation (ISO) and the International Telecommunication Union (ITU), with a view to ensuring a high level of security and interoperability of electronic identification and trust services.~~

~~(73)~~

~~For reasons of legal certainty and clarity, Directive 1999/93/EC should be repealed.~~

~~(74)~~

~~To ensure legal certainty for market operators already using qualified certificates issued to natural persons in compliance with Directive 1999/93/EC, it is necessary to provide for a sufficient period of time for transitional purposes. Similarly, transitional measures should be established for secure signature creation devices, the conformity of which has been determined in accordance with Directive 1999/93/EC, as well as for certification service providers issuing qualified certificates before 1 July 2016. Finally, it is also necessary to provide the Commission with the means to adopt the implementing acts and delegated acts before that date.~~

~~(75)~~

~~The application dates set out in this Regulation do not affect existing obligations that Member States already have under Union law, in particular under Directive 2006/123/EC.~~

~~(76)~~

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

~~(77)~~

~~The European Data Protection Supervisor was consulted in accordance with Article 28(2) of Regulation (EC) No 45/2001 of the European Parliament and of the Council (13) and delivered an opinion on 27 September 2012 (14),~~

CHAPTER I - GENERAL PROVISIONS

Article 1 - Subject matter

This ***Regulation*** aims at ensuring the proper functioning of the internal market and providing an adequate level of security of electronic identification means and trust services ***used across the Union in order to enable and to facilitate the exercise of the right to safely participate in the digital society and the access to online public and private services throughout the Union for any natural or legal person***. For these purposes this Regulation:

(a) lays down the conditions under which Member States shall provide and recognise electronic identification means of natural and legal persons, falling under a notified electronic identification scheme of another Member State;

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

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

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

Article 2 - Scope

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

2. This Regulation does not apply to the provision of trust services that are used exclusively within closed systems resulting from national law or from agreements between a defined set of participants.

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

3. 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***.

3a. This Regulation shall be without prejudice to Regulation (EU) 2016/679.

Article 3 - Definitions

For the purposes of this Regulation, the following definitions apply:

(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;

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

(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 a natural person representing a ***natural or*** legal person, to be established;

(4) 'electronic identification scheme' means a system for electronic identification under which electronic identification means are issued to natural or legal persons, or natural persons representing ***natural or*** legal persons;

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

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

(6) 'relying party' means a natural or legal person that relies upon an electronic identification***, European Digital Identity Wallets or other electronic identification means,*** or a trust service;

(7) 'public sector body' means a state, regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several such bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate;

(8) 'body governed by public law' means a body defined in point (4) of Article 2(1) of Directive 2014/24/EU of the European Parliament and of the Council (15);

(9) 'signatory' means a natural person who creates an electronic signature;

(10) 'electronic signature' means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

(11) 'advanced electronic signature' means an electronic signature which meets the requirements set out in Article 26;

(12) 'qualified electronic signature' means an advanced electronic signature that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures;

(13) 'electronic signature creation data' means unique data which is used by the signatory to create an electronic signature;

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

(15) 'qualified certificate for electronic signature' means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I;

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

(a) the ***issuing of certificates for*** electronic signatures, ***of certificates for*** electronic ***seals, of certificates for website authentication or of certificates for the provision of other trust*** services;~~the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those 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;

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

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

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

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

(f) the ***issuing*** of electronic ***attestations of attributes***;

(fa) the validation of electronic attestation of attributes;

(fb) the creation of electronic timestamps;

(fc) the validation of electronic timestamps;

(fd) the provision of electronic registered delivery services;

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

(ff) the electronic archiving of electronic data; or

(fg) the recording of electronic data into an electronic ledger;~~(b)~~

~~the creation, verification and validation of certificates for website authentication; or~~

~~(c)~~

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

(17) ‘qualified trust service’ means a trust service that meets the applicable requirements laid down in this Regulation;

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

(19) ‘trust service provider’ means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider;

(20) ‘qualified trust service provider’ means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body;

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

(22) ‘electronic signature creation device’ means configured software or hardware used to create an electronic signature;

(23) ‘qualified electronic signature creation device’ means an electronic signature creation device that meets the requirements laid down in Annex II;

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

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

(24) ‘creator of a seal’ means a legal person who creates an electronic seal;

(25) ‘electronic seal’ means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity;

(26) ‘advanced electronic seal’ means an electronic seal, which meets the requirements set out in Article 36;

(27) ‘qualified electronic seal’ means an advanced electronic seal, which is created by a qualified electronic seal creation device, and that is based on a qualified certificate for electronic seal;

(28) ‘electronic seal creation data’ means unique data, which is used by the creator of the electronic seal to create an electronic seal;

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

(30) ‘qualified certificate for electronic seal’ means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III;

(31) ‘electronic seal creation device’ means configured software or hardware used to create an electronic seal;

(32) ‘qualified electronic seal creation device’ means an electronic seal creation device that meets mutatis mutandis the requirements laid down in Annex II;

(33) ‘electronic time stamp’ means data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time;

(34) ‘qualified electronic time stamp’ means an electronic time stamp which meets the requirements laid down in Article 42;

(35) ‘electronic document’ means any content stored in electronic form, in particular text or sound, visual or audiovisual recording;

(36) ‘electronic registered delivery service’ means a service that makes it possible to transmit data between third parties by electronic means and provides evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and that protects transmitted data against the risk of loss, theft, damage or any unauthorised alterations;

(37) ‘qualified electronic registered delivery service’ means an electronic registered delivery service which meets the requirements laid down in Article 44;

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

(39) ‘qualified certificate for website authentication’ means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;

(40) ‘validation data’ means data that is used to validate an electronic signature or an electronic seal;

(41) ‘validation’ means the process of verifying and confirming that ***data in*** electronic ***form are valid according to the requirements of this Regulation*** ~~an electronic signature or a seal is valid.~~

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

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

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

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

(45a) ‘electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source’ means an electronic attestations of attributes issued by a public sector body

responsible for an authentic source or by a public sector body designated by the Member State to issue such attestations of attributes on behalf of the public sector bodies responsible for authentic sources in accordance with Article 45da and meeting the requirements laid down in Annex VIa;

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

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

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

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

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

(53) 'electronic ledger' means a ***sequence of*** electronic ***data records, ensuring their*** integrity ***and the*** accuracy of their chronological ordering';

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

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

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

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

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

Article 4 - Internal market principle

1. There shall be no restriction on the provision of trust services in the territory of a Member State by a trust service provider established in another Member State for reasons that fall within the fields covered by this Regulation.

2. Products and trust services that comply with this Regulation shall be permitted to circulate freely in the internal market.

~~**Article 5**~~

~~**Data processing and protection**~~

~~**1. Processing of personal data shall be carried out in accordance with Directive 95/46/EC.**~~

Article 5 - Pseudonyms in electronic transaction

Without prejudice to specific rules of Union or national law requiring users to identify themselves and w~~2. W~~ithout prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms***, chosen by the user,*** ~~in electronic transactions~~ shall not be prohibited.

CHAPTER II - ELECTRONIC IDENTIFICATION

Article 6 - Mutual recognition

1. When an electronic identification using an electronic identification means and authentication is required under national law or by administrative practice to access a service provided by a public sector body online in one 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 service online, 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 published by the Commission pursuant to 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 service online in the first Member State, provided that the assurance level of that electronic identification means corresponds to the assurance level substantial or high;

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

Such recognition shall take place no later than 12 months after the Commission publishes the list referred to in point (a) of the first subparagraph.

2. An electronic identification means which is issued under an electronic identification scheme included in the list published by the Commission pursuant to 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 service provided online by those bodies.

SECTION I - EUROPEAN DIGITAL IDENTITY WALLET

Article 6a - European Digital Identity Wallets

1. For the purpose of ensuring that all natural and legal persons in the Union have secure, trusted and seamless ***cross-border*** access to public and private services, ***while having full control over their data,*** each Member State shall ***provide at least one*** European Digital Identity Wallet within ***24*** months after the entry into force of ***the implementing acts referred to in paragraph 11 and Article 6c(4)***.

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

(a) ***directly*** by a Member State;

(b) under a mandate from a Member State;

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

2a. The source code of the application software components of the European Digital Identity Wallets shall be open-source licensed. Member States may provide that, for duly justified reasons, specific components other than those installed on user devices shall not be disclosed.

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

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

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

(iii) easily report to the national data protection authority where a relying party is established when an allegedly unlawful or suspicious request of data is received.

(ac) generate pseudonyms and store them encrypted and locally within it;

(ad) securely authenticate another person's European Digital Identity Wallet, and receive and share identity data and electronic attestations of attributes in a secured way between the two wallets.

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

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

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

(ba) download, to the extent technically feasible, users' data, electronic attestation of attributes and configurations;

(bb) exercise users' rights to data portability.

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

(a) ***support*** common ***protocols and interfaces***:

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

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

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

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

(4a) to securely on-board the user with the electronic identification means associated pursuant to Article 6a(11a);

(4c) for interaction with another person's European Digital Identity Wallet for the purpose of receiving, validating and sharing identity data and electronic attestations of attributes in a secured way between two wallets;

(4d) for authenticating relying parties by implementing authentication mechanisms in accordance with Article 6b;

(4e) for relying parties to verify the authenticity and validity of European Digital Identity Wallets;

(4h) for requesting to a relying party the deletion of personal data pursuant to Article 17 of the Regulation (EU) 2016/679);

(4i) for reporting to the national data protection authority where a relying party is established when an allegedly unlawful or suspicious request of data is received;

(4j) for the creation of qualified electronic signatures or seals by means of qualified signature or seal creation devices;

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

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

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

(ca) *in the case of electronic attestation of attributes with embedded disclosure policies,* ***implement the appropriate*** *mechanism to inform that the* ***requesting*** *relying party or the* ***requesting*** *user of European Digital Identity Wallets* ***have*** *the permission to access it;*

(e) ensure that the person identification data***, which is available from the electronic identification scheme under which the EUDIW is provided,*** uniquely ***represents the natural person, legal person or the natural person representing*** the natural or legal person***, and*** is associated with ***the Wallet;***

(ec) offer the ability to sign by means of qualified electronic signatures to all natural persons by default and free of charge. Member States may provide for proportionate measures to ensure that the free-of-charge use of qualified electronic signatures by natural persons is for non-professional purposes.

4a. Member State shall inform users, without delay, of any security breach that may have entirely or partially compromised their European Digital Identity Wallet or its content and in particular if their European Digital Identity Wallet has been suspended or revoked pursuant to Article 6da.

4b. 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. Those additional functionalities shall comply with the requirements of this Article.

5. Member States shall provide ***free-of-charge*** validation mechanisms ***to***:

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

(ca) allow European Digital Identity Wallet users to verify the authenticity and validity of the identity of relying parties registered in accordance with Article 6b.

5a. *Member States shall provide means to revoke the validity of the European Digital Identity Wallet*

(a) upon the explicit request of the user;

(b) when its security has been compromised;

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

5c. Providers of European Digital Identity Wallets shall ensure that users can easily request technical support and report technical problems or any other incidents having a negative impact on the provision of services of the European Digital Identity Wallet.

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

6a. European Digital Identity Wallets shall ensure security-by-design.

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

7. The ***users*** shall be in full control of the ***use of the European Digital Identity Wallet and of the data in their*** European Digital Identity Wallet. The ***provider*** 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 ***provider*** or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it. Personal data relating to the provision of European Digital Identity Wallets shall be kept logically separate from any other data held ***by the provider of European Digital Identity Wallets***. If the European Digital Identity Wallet is provided by private parties in accordance to paragraph ***2*** (b) and (c), the provisions of article 45f paragraph 4 shall apply mutatis mutandis.

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

7b. *The technical framework of the European Digital Identity Wallet shall:*

- ***(a)*** *not allow providers of electronic attestations of attributes or any other party, after the issuance of the attestation of attributes, to obtain data that allows for tracking, linking, correlating or otherwise obtain knowledge of transactions or user behaviour unless explicitly authorised by the user.*
- ***(b)*** *enable privacy preserving techniques which ensure unlinkability, where attestation of attributes do not require the identification of the user.*

7c. *Any processing of personal data carried out by the Member States or on their behalf by bodies or parties responsible for the provision of the European Digital Identity Wallets as electronic identification means shall implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with Regulation (EU) 2016/679. Member States shall be allowed to introduce national provisions to further specify the application of such rules.*

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

- ***(a) the body responsible for establishing and maintaining the list of registered relying parties that rely on the European Digital Identity Wallets in accordance with Article 6b(1e), and the location of such a list;***
- ***(b) the bodies responsible for the provision of the European Digital Identity Wallets in accordance with Article 6a(1);***
- ***(c) the bodies responsible for ensuring that the person identification data is associated with the Wallet in accordance with Article 6a(4)(e);***

(d) the mechanism allowing for the validation of the person identification data referred to in 6a(4)(e) and of the identity of the relying parties.

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

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 ***without prejudice to Art.6a(10a)***.

9. Article 24(2), points (b), ***(d), (e), (f), (fa), (fb),*** (g), and (h) shall apply mutatis mutandis to ***the providers of*** European Digital Identity Wallets.

10. The European Digital Identity Wallet shall be made accessible for ***use, in accordance with Directive 2019/882, by persons with disabilities, on an equal basis with other users***.

10a. For the purposes of the provision of the EUDIW, the EUDIW and the electronic identification schemes under which they are provided shall not be subject to the requirements referred to in Articles 7, 9, 10, 12 and 12a.

11. ***By … [***6 months ***after the date*** of the entering into force of this ***amending*** Regulation***]***, the Commission shall***, by means of implementing acts,*** establish ***a list of reference standards and when necessary, establish*** specifications and ***procedures*** for the requirements referred to in paragraphs 3, 4***, 5 and 7c*** on the implementation of the European Digital Identity Wallet. ***These*** implementing ***acts*** shall be adopted in accordance with the examination procedure referred to in Article 48(2).

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

Article 6b - European Digital Identity Wallets Relying Parties

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

1a. The registration process shall be cost-effective and proportionate-to-risk. Relying parties shall provide at least:

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

i) the Member State in which they are established and

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

b) contact details;

c) the intended use of the European Digital Identity Wallet, including the data to be requested.

1c. Relying parties shall not request any data beyond what they have registered for according to paragraphs 1 and 1a.

1d. Paragraphs 1 and 1a shall be without prejudice to requirements in accordance with Union or national law, applicable for the provision of specific services.

1e. Member States shall make the information referred to in paragraph 1a publicly available online in electronically signed or sealed form suitable for automated processing.

1g. Relying parties registered in accordance with this Article shall inform Member States without delay about any changes in to the information provided.

2. Member States shall ***provide*** a common mechanism for ***allowing the identification and*** authentication of relying parties***, as referred to in Article 6a(4)(ba) [GA].***

2a. Where relying parties intend to rely upon European Digital Identity Wallets issued in accordance with this Regulation, they shall identify themselves to the user of the European Digital Identity Wallet.

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

3a.Intermediaries acting on behalf of relying parties are to be considered relying parties and shall not store data about the content of the transaction.

4. ***By ... [***6 months ***after the date*** of the entering into force of this ***amending*** Regulation***]***, the Commission shall establish technical and operational specifications for the requirements referred to in paragraphs ***1a, 1e, 1g, 2, 2a and 3*** by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6***a(11). This implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).***

Article 6c - Certification of the European Digital Identity Wallets

1. ***The conformity of*** European Digital Identity Wallets ***and of the electronic identification scheme*** under ***which they are provided with the requirements laid down in Article 6a(3), (4), (5), with the requirement for logical separation laid down Article 6a(7) and, where applicable, in accordance with***

standards and technical specifications referred to in Article 6a***(11a), shall be certified by*** conformity ***assessment bodies designated by Member States***.

2. ***Certification of the conformity of European Digital Identity Wallets with cybersecurity relevant requirements referred to in paragraph 1, or parts thereof, shall be*** carried out ***in accordance with cybersecurity schemes adopted pursuant to Regulation (EU) 2019/881 and referenced in the implementing acts referred to in paragraph 4***.

2a. For those non-cybersecurity requirements referred to in paragraph1 and, for as long as cybersecurity certification schemes referred to in paragraph 2 do not or do not fully cover the relevant cybersecurity requirements, for those requirements, Member States shall establish national certification schemes following the requirements set out in the implementing acts referred to in paragraph 4. Member States shall transmit their draft national certification schemes to the EDICG, which may issue opinions and recommendations.

2b. The certification referred to in paragraph 1 shall be valid for not more than five years, conditional upon a regular two-year vulnerabilities assessment.

3. ***Compliance*** with the requirements ***set out*** in Article 6a ***related to the personal data processing operations may be certified pursuant to Regulation (EU) 2016/679***.

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

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

Article 6d - Publication of a list of certified European Digital Identity Wallets

1. Member States shall inform the Commission ***and the EDICG referred to in Art.46e*** without undue delay of the European Digital Identity Wallets that have been ***provided*** pursuant to Article 6a and certified by the ***conformity assessment*** bodies referred to in Article 6c paragraph ***1.*** They shall also inform the Commission ***and the EDICG referred to in Art.46e***, without undue delay where the certification is cancelled ***and state the reasons for such cancellation***.

1a. Without prejudice to Art.6a(7c), the information provided by Member States referred to in paragraph 1 shall include at least:

a) the certificate and certification assessment report of the certified EUDIW;

b) a description of the electronic identification scheme under which the EUDIW is provided;

c) the applicable supervisory regime and information on the liability regime with respect to the party providing the EUDIW;

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

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

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

2a. A Member State may submit to the Commission a request to remove an EUDIW and the electronic identification scheme under which it is provided from the list referred to in paragraph 2. A Member State shall submit updates to the provided information referred to in paragraph 1. The Commission shall publish in the list referred to in paragraph 2 the corresponding amendments to the list within one month from the date of receipt of the Member State's request or updated information.

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

Article 6da - Security breach of the European Digital Identity Wallets

1. Where European Digital Identity Wallets provided pursuant to Article 6a or the validation mechanisms referred to in Article 6a(5), or the electronic identification scheme under which the wallets are provided, are breached or partly compromised in a manner that affects their reliability or the reliability of other European Digital Identity Wallets, the providing Member State shall, without undue delay, suspend the provision and the use of the European Digital Identity Wallet. The Member States where concerned Wallets were provided shall inform the affected users, the single points of contact designated pursuant to Article 46c, the relying parties and the Commission accordingly.

2. If the breach or compromise referred to in paragraph 1 is not remedied within three months of the suspension, the Member State concerned shall withdraw the European Digital Identity Wallets concerned and have their validity revoked. Member States concerned shall inform the affected users, the single points of contact designated pursuant to Article 46c, the relying parties and the Commission of 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.

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

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

5. By … [6 months after the entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish the reference standards and when necessary, establish specifications and procedures for the measures referred to in paragraphs 1, 2 and 3. These implementing acts 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 and authentication to access an online service provided by a public sector body, they shall also accept European Digital Identity Wallets provided in accordance with this Regulation.

2. *Where private relying parties providing services,* ***with the exception of microenterprises and small enterprises as defined in Commission Recommendation 2003/361/EC****, are required by national or Union law to use strong user authentication for online identification or* ***where strong user authentication*** *for online identification* ***is required by contractual obligation,*** *including in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, private relying parties shall,* ***no later than 36 months after the entry into force of the implementing acts referred to in [Article 6a] paragraph 11 and Article 6c(4)] and strictly upon voluntary request of the user,*** *also accept the use of European Digital Identity Wallets provided in accordance with this Regulation.*

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

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

5. Within 24 months after deployment of the European Digital Identity Wallets, the Commission shall carry out an assessment on demand, availability and usability of the European Digital Identity Wallets, considering criteria such as users' take up, cross-border presence of service providers, technological developments, evolution in usage patterns and consumer demand.

SECTION II - ELECTRONIC IDENTIFICATION SCHEMES

Article 7 - Eligibility for notification of electronic identification schemes

An electronic identification scheme shall be eligible for notification pursuant to Article 9(1) provided that all of the following conditions are met:

(a) the electronic identification means under the electronic identification scheme are issued:

(i) by the notifying Member State;

(ii) under a mandate from the notifying Member State; or

(iii) independently of the notifying Member State and are recognised by that Member State;

(b) the electronic identification means under the electronic identification scheme can be used to access at least one service which is provided by a public sector body and which requires electronic identification in the notifying Member State;

(c) the electronic identification scheme and the electronic identification means issued thereunder meet the requirements of at least one of the assurance levels set out in the implementing act referred to in Article 8(3);

(d) the notifying Member State ensures that the person identification data uniquely representing the person in question is attributed, in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3), to the natural or legal person referred to in point 1 of Article 3 at the time the electronic identification means under that scheme is issued;

(e) the party issuing the electronic identification means under that scheme ensures that the electronic identification means is attributed to the person referred to in point (d) of this Article in accordance with the technical specifications, standards and procedures for the relevant assurance level set out in the implementing act referred to in Article 8(3);

(f) the notifying Member State ensures the availability of authentication online, so that any relying party established in the territory of another Member State is able to confirm the person identification data received in electronic form.

For relying parties other than public sector bodies the notifying Member State may define terms of access to that authentication. The cross-border authentication shall be provided free of charge when it is carried out in relation to a service online provided by a public sector body.

Member States shall not impose any specific disproportionate technical requirements on relying parties intending to carry out such authentication, where such requirements

prevent or significantly impede the interoperability of the notified electronic identification schemes;

(g) at least six months prior to the notification pursuant to Article 9(1), the notifying Member State provides the other Member States for the purposes of the obligation under Article 12(5) a description of that scheme in accordance with the procedural arrangements established by the implementing acts referred to in Article 12(~~7~~6);

(h) the electronic identification scheme meets the requirements set out in the implementing act referred to in Article 12(8).

Article 8 - Assurance levels of electronic identification schemes

1. An electronic identification scheme notified pursuant to Article 9(1) shall specify assurance levels low, substantial and/or high for electronic identification means issued under that scheme.

2. The assurance levels low, substantial and high shall meet respectively the following criteria:

(a) assurance level low shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a limited degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease the risk of misuse or alteration of the identity;

(b) assurance level substantial shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a substantial degree of confidence in the claimed or asserted identity of a person, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to decrease substantially the risk of misuse or alteration of the identity;

(c) assurance level high shall refer to an electronic identification means in the context of an electronic identification scheme, which provides a higher degree of confidence in the claimed or asserted identity of a person than electronic identification means with the assurance level substantial, and is characterised with reference to technical specifications, standards and procedures related thereto, including technical controls, the purpose of which is to prevent misuse or alteration of the identity.

3. By 18 September 2015, taking into account relevant international standards and subject to paragraph 2, the Commission shall, by means of implementing acts, set out minimum technical specifications, standards and procedures with reference to which assurance levels low, substantial and high are specified for electronic identification ~~means for the purposes of paragraph 1~~.

Those minimum technical specifications, standards and procedures shall be set out by reference to the reliability and quality of the following elements:

(a) the procedure to prove and verify the identity of natural or legal persons applying for the issuance of electronic identification means;

(b) the procedure for the issuance of the requested electronic identification means;

(c) the authentication mechanism, through which the natural or legal person uses the electronic identification means to confirm its identity to a relying party;

(d) the entity issuing the electronic identification means;

(e) any other body involved in the application for the issuance of the electronic identification means; and

(f) the technical and security specifications of the issued electronic identification means.

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

Article 9 - Notification

1. The notifying Member State shall notify to the Commission the following information and, without undue delay, any subsequent changes thereto:

(a) a description of the electronic identification scheme, including its assurance levels and the issuer or issuers of electronic identification means under the scheme;

(b) the applicable supervisory regime and information on the liability regime with respect to the following:

(i) the party issuing the electronic identification means; and

(ii) the party operating the authentication procedure;

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

(d) information on the entity or entities which manage the registration of the unique person identification data;

(e) a description of how the requirements set out in the implementing acts referred to in Article 12(8) are met;

(f) a description of the authentication referred to in point (f) of Article 7;

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

2. ~~One year from the date of application of the implementing acts referred to in Articles 8(3) and 12(8), the~~The Commission shall***, without undue delay,*** publish ~~in~~ 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. ~~If the~~ The Commission ~~receives a notification after the expiry of the period referred to in paragraph 2, it~~ shall publish in the Official Journal of the European Union the amendments to the list referred to in paragraph 2 within ~~two~~ one month~~s~~ from the date of receipt of that notification.

4. A Member State may submit to the Commission a request to remove an electronic identification scheme notified by that Member State from the list referred to in paragraph 2. The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list within one month from the date of receipt of the Member State's request.

5. The Commission may, by means of implementing acts, define the circumstances, formats and procedures of notifications under paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 10 - Security breach of electronic identification schemes

1. Where either the electronic identification scheme notified pursuant to Article 9(1) or the authentication referred to in point (f) of Article 7 is breached or partly compromised in a manner that affects the reliability of the cross-border authentication of that scheme, the notifying Member State shall, without delay, suspend or revoke that cross-border authentication or the compromised parts concerned, and shall inform other Member States and the Commission.

2. When the breach or compromise referred to in paragraph 1 is remedied, the notifying Member State shall re-establish the cross-border authentication and shall inform other Member States 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 notifying Member State shall notify other Member States and the Commission of the withdrawal of the electronic identification scheme.

The Commission shall publish in the Official Journal of the European Union the corresponding amendments to the list referred to in Article 9(2) without undue delay.

Article 11 - Liability

1. The notifying Member State shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with its obligations under points (d) and (f) of Article 7 in a cross-border transaction.

2. The party issuing the electronic identification means shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligation referred to in point (e) of Article 7 in a cross-border transaction.

3. The party operating the authentication procedure shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to ensure the correct operation of the authentication referred to in point (f) of Article 7 in a cross-border transaction.

4. Paragraphs 1, 2 and 3 shall be applied in accordance with national rules on liability.

5. Paragraphs 1, 2 and 3 are without prejudice to the liability under national law of parties to a transaction in which electronic identification means falling under the electronic identification scheme notified pursuant to Article 9(1) are used.

Article 11a - Cross-border identity matching

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

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

3. ***By … [***6 months ***after the date of entry*** into force of this ***amending*** Regulation***]***, the Commission shall ***establish the reference standards and when necessary, establish specifications and procedures for the requirements*** referred to in paragraph 1 by means of an implementing act***. That implementing act shall be adopted in accordance with the examination procedure*** referred to in Article ***48(2)***.

Article 12 - ~~i~~interoperability

1. The national electronic identification schemes notified pursuant to Article 9(1) shall be interoperable.

2. For the purposes of paragraph 1, an interoperability framework shall be established.

3. The interoperability framework shall meet the following criteria:

(a) it aims to be technology neutral and does not discriminate between any specific national technical solutions for electronic identification within a Member State;

(b) it follows European and international standards, where possible;

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

~~(d)~~

~~it ensures that personal data is processed in accordance with Directive 95/46/EC.~~

4. The interoperability framework shall consist of:

(a) a reference to minimum technical requirements related to the assurance levels under Article 8;

(b) a mapping of national assurance levels of notified electronic identification schemes to the assurance levels under Article 8;

(c) a reference to minimum technical requirements for interoperability;

(d) a reference to a minimum set of person identification data uniquely represent~~ing~~ a natural person, ~~or~~ legal person ***or*** a natural ***person representing natural*** or legal ***persons~~,~~*** which is available from electronic identification schemes;

(e) rules of procedure;

(f) arrangements for dispute resolution; and

(g) common operational security standards.

5. Member States shall carry out peer reviews of electronic identification schemes falling under this Regulation, to be notified pursuant to Article 9(1). ~~5. Member States shall cooperate with regard to the following:~~

~~(a)~~

~~the interoperability of the electronic identification schemes notified pursuant to Article 9(1) and the electronic identification schemes which Member States intend to notify; and~~

~~(b)~~

~~the security of the electronic identification schemes.~~

6. By 18 March 2025, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements for the peer reviews referred to in paragraph 5 with a view to fostering a high level of trust and security appropriate to the degree of risk. ~~6. The cooperation between Member States shall consist of:~~

~~(a)~~

~~the exchange of information, experience and good practice as regards electronic identification schemes and in particular technical requirements related to interoperability and assurance levels;~~

~~(b)~~

~~the exchange of information, experience and good practice as regards working with assurance levels of electronic identification schemes under Article 8;~~

~~(c)~~

~~peer review of electronic identification schemes falling under this Regulation; and~~

~~(d)~~

~~examination of relevant developments in the electronic identification sector.~~

~~7. By 18 March 2015, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in paragraphs 5 and 6 with a view to fostering a high level of trust and security appropriate to the degree of risk.~~

8. By 18 September ~~2015~~2025, for the purpose of setting uniform conditions for the implementation of the requirement under paragraph 1, the Commission shall, subject to the criteria set out in paragraph 3 and taking into account the results of the cooperation between Member States, adopt implementing acts on the interoperability framework as set out in paragraph 4.

9. The implementing acts referred to in paragraphs ~~7~~ 6 and 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 12a - Certification of electronic identification schemes

1. ***The*** conformity of electronic identification schemes ***to be notified with cybersecurity*** requirements laid down in ***this Regulation shall*** be certified by ***conformity assessment*** bodies designated by Member States.

2. ***Certification*** referred to in ***paragraph 1 including the conformity with cybersecurity relevant requirements set out in Article 8(2) regarding the assurance levels of electronic identification schemes shall be carried out 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 those cybersecurity requirements***.

2a. The certification referred to in paragraph 1 shall be valid for not more than five years, conditional upon a regular two-year vulnerabilities assessment. Where vulnerabilities are identified and not remedied within three months, the certification shall be cancelled.

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

2c. The peer-review of electronic identification schemes referred to in paragraph 5.c of Article 46e shall not apply to electronic identification schemes or part of such schemes certified in accordance with paragraph 1 of this Article. Member States may use a certificate or a statement of conformity, issued in accordance with a relevant certification scheme or parts of such schemes, with the non-cybersecurity requirements set out in Article 8(2) of this Regulation regarding the assurance levels of electronic identification schemes.

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

Article 12b - Access to hardware and software features

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

CHAPTER III - TRUST SERVICES

SECTION 1 - General provisions

Article 13 - Liability and burden of proof

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

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

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

2. Where trust service providers duly inform their customers in advance of the limitations on the use of the services they provide and where those limitations are recognisable to third parties, trust service providers shall not be liable for damages arising from the use of services exceeding the indicated limitations.

3. Paragraphs 1 and 2 shall be applied in accordance with national rules on liability.

Article 14 - International aspects

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

2. The implementing decisions and ~~A~~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 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. ***Third countries and international organisations shall in particular establish, maintain and publish a trusted list of recognised trust service providers***. ~~(b)~~

2a. ***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.

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

Article 15 - Accessibility for persons with disabilities *and special needs*

The provision of ***electronic identification means,*** trust services and end-user products used in the provision of those services shall be made ***available in plain and intelligible language and*** in accordance with the ***United Nations Convention on the Rights of Persons with Disabilities. Further, alignment with the requirements set out in*** Annex I of Directive ***(EU) 2019/882***[1]***, should also benefit persons who experience functional limitations, such as elderly people, and persons with limited access to digital technologies***.~~Where feasible, trust services provided and end-user products used in the provision of those services shall be made accessible for persons with disabilities.~~

Article 16 - Penalties

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

2. Member States shall ensure that infringements by qualified and non-qualified trust service providers of the obligations of this Regulation be subject to administrative fines of a maximum of at least EUR 5,000,000 when the trust service provider is a natural persons or EUR 5,000,000 or 1% of the total worldwide annual turnover of the undertaking to which the trust service provider belonged in the financial year preceding the year in which the infringement occurred, whichever is higher.

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

SECTION 2 - Supervision

~~**Article 17**~~

~~**Supervisory body**~~

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

~~Supervisory bodies shall be given the necessary powers and adequate resources for the exercise of their tasks.~~

~~2. Member States shall notify to the Commission the names and the addresses of their respective designated supervisory bodies.~~

~~3. The role of the supervisory body shall be the following:~~

~~(a)~~

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

~~(b)~~

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

~~4. For the purposes of paragraph 3 and subject to the limitations provided therein, the tasks of the supervisory body shall include in particular:~~

~~(a)~~

~~to cooperate with other supervisory bodies and provide them with assistance in accordance with Article 18;~~

~~(b)~~

~~to analyse the conformity assessment reports referred to in Articles 20(1) and 21(1);~~

~~(c)~~

~~to inform other supervisory bodies and the public about breaches of security or loss of integrity in accordance with Article 19(2);~~

~~(d)~~

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

~~(e)~~

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

~~(f)~~

~~to cooperate with the data protection authorities, in particular, by informing them without undue delay, about the results of audits of qualified trust service providers, where personal data protection rules appear to have been breached;~~

~~(g)~~

~~to grant qualified status to trust service providers and to the services they provide and to withdraw this status in accordance with Articles 20 and 21;~~

~~(h)~~

~~to inform the body responsible for the national trusted list referred to in Article 22(3) about its decisions to grant or to withdraw qualified status, unless that body is also the supervisory body;~~

~~(i)~~

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

~~(j)~~

~~to require that trust service providers remedy any failure to fulfil the requirements laid down in this Regulation.~~

~~5. Member States may require the supervisory body to establish, maintain and update a trust infrastructure in accordance with the conditions under national law.~~

~~6. By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities together with a summary of breach notifications received from trust service providers in accordance with Article 19(2).~~

~~7. The Commission shall make the annual report referred to in paragraph 6 available to Member States.~~

~~8. The Commission may, by means of implementing acts, 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).~~

~~Article 18~~

~~Mutual assistance~~

~~1. Supervisory bodies shall cooperate with a view to exchanging good practice.~~

A supervisory body shall, upon receipt of a justified request from another supervisory body, provide that body with assistance so that the activities of supervisory bodies can be carried out in a consistent manner. Mutual assistance may cover, in particular, information requests and supervisory measures, such as requests to carry out inspections related to the conformity assessment reports as referred to in Articles 20 and 21.

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

(a)

the supervisory body is not competent to provide the requested assistance;

(b)

the requested assistance is not proportionate to supervisory activities of the supervisory body carried out in accordance with Article 17;

(c)

providing the requested assistance would be incompatible with this Regulation.

3. Where appropriate, Member States may authorise their respective supervisory bodies to carry out joint investigations in which staff from other Member States' supervisory bodies is involved. The arrangements and procedures for such joint actions shall be agreed upon and established by the Member States concerned in accordance with their national law.

Article 19

Security requirements applicable to trust service providers

1. Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide. Having regard to the latest technological developments, those measures shall ensure that the level of security is commensurate to the degree of risk. In particular, measures shall be taken to prevent and minimise the impact of security incidents and inform stakeholders of the adverse effects of any such incidents.

2. Qualified and non-qualified trust service providers shall, without undue delay but in any event within 24 hours after having become aware of it, notify the supervisory body and, where applicable, other relevant bodies, such as the competent national body for information security or the data protection authority, of any breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein.

~~Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.~~

~~Where appropriate, in particular if a breach of security or loss of integrity concerns two or more Member States, the notified supervisory body shall inform the supervisory bodies in other Member States concerned and ENISA.~~

~~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.~~

~~3. The supervisory body shall provide ENISA once a year with a summary of notifications of breach of security and loss of integrity received from trust service providers.~~

~~4. The Commission may, by means of implementing acts,:~~

~~(a)~~

~~further specify the measures referred to in paragraph 1; and~~

~~(b)~~

~~define the formats and procedures, including deadlines, applicable for the purpose of paragraph 2.~~

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

Article 19a

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 2022/2555, those measures shall include at least the following:***

- ***(i) measures related to registration and on-boarding procedures to a trust service;***
- ***(ii) measures related to procedural or administrative checks needed to provide trust services;***
- ***(iii) measures related to the management and implementation of trust services.***

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

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

SECTION 3 - Qualified trust services

Article 20 - Supervision of qualified trust service providers

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

1a. Qualified trust service providers shall inform the supervisory body at the latest[2] ***one month in advance about planned audits and allow for the participation of the supervisory body as an observer upon request.***

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

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

~~3. Where the supervisory body requires the qualified trust service provider to remedy any failure to fulfil requirements under this Regulation and where that provider does not act accordingly, and if applicable within a time limit set by the supervisory body, the supervisory body, taking into account, in particular, the extent, duration and consequences of that failure, may withdraw the qualified status of that provider or of the affected service it provides and inform the body referred to in Article 22(3) for the purposes of updating the trusted lists referred to in Article 22(1). The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned.~~3. Where the qualified trust service provider fails to fulfil any of the requirements set out by this Regulation, the supervisory body shall require it to provide a remedy within a set time limit, if applicable.

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

[2] The „at the latest" is a typo, the right wording is „at least".

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

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

3c. The supervisory body shall inform the qualified trust service provider of the withdrawal of its qualified status or of the qualified status of the service concerned. The supervisory body shall inform the body 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 Directive (EU) 2022/2555.

4. ***By ... [***12 months ***after the date of entry*** into force of this ***amending*** Regulation***]***, the Commission shall, by means of implementing acts, establish ***a list of*** reference ***standards and when necessary, establish specifications and procedures*** for the following~~The Commission may, by means of implementing acts, establish reference number of the following standards:~~

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

(b) the auditing requirements for the ~~rules under which~~ conformity assessment bodies ~~will~~ to carry out their conformity assessment***, including composite assessment,*** of the qualified trust service providers as referred to in paragraph 1.

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

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

Article 21 - Initiation of a qualified trust service

1. Where trust service providers~~, without qualified status,~~ intend to start providing 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 21 of Directive (EU) 2022/2555***.

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

In order to verify the compliance of the trust service provider with the requirements laid down in Article ***21 of Directive (EU) 2022/2555***, the supervisory body shall request the competent authorities referred to in ***Directive (EU) 2022/2555*** to carry out supervisory actions in that regard and to provide information about the outcome ***without undue delay, and no later than two months from the receipt of this request by the competent authorities referred to in Directive (EU) 2022/2555. If the verification is not concluded*** within ***two months of the notification, the competent authorities referred to in Directive (EU) 2022/2555 shall inform the supervisory body specifying the reasons for the delay and the period within which the verification is to be concluded***.

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

~~If~~ 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.

3. Qualified trust service providers may begin to provide the qualified trust service after the qualified status has been indicated in the trusted lists referred to in Article 22(1).

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

Article 22 - Trusted lists

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

2. Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.

3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.

4. The Commission shall make available to the public, through a secure channel, the information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing.

5. By 18 September 2015 the Commission shall, by means of implementing acts, specify the information referred to in paragraph 1 and define the technical specifications and formats for trusted

lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 23 - EU trust mark for qualified trust services

1. After the qualified status referred to in the second subparagraph of Article 21(2) has been indicated in the trusted list referred to in Article 22(1), qualified trust service providers may use the EU trust mark to indicate in a simple, recognisable and clear manner the qualified trust services they provide.

2. When using the EU trust mark for the qualified trust services referred to in paragraph 1, qualified trust service providers shall ensure that a link to the relevant trusted list is made available on their website.

3. By 1 July 2015 the Commission shall, by means of implementing acts, provide for specifications with regard to the form, and in particular the presentation, composition, size and design of the EU trust mark for qualified trust services. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 24- Requirements for qualified trust service providers

1. When issuing a qualified certificate or a qualified electronic attestation of attributes~~for a trust service~~, a qualified trust service provider shall verify~~, by appropriate means and in accordance with national law,~~ the identity and, if applicable, any specific attributes of the natural or legal person to whom the qualified certificate or the qualified electronic attestation of ***attributes will be*** issued~~is issued~~.

The ***verification of the identity*** ~~information~~ referred to in the first subparagraph shall be verified***, by appropriate means,*** by the qualified trust service provider either directly or by relying on a third ***, based on one*** of the following ***methods or on a combination thereof when needed, and in accordance with the implementing acts referred to in paragraph 1a*** ~~party in accordance with national law:~~

(a) by means of ***the European Digital Identity Wallet or*** a notified electronic identification means which meets the requirements set out in Article 8 with regard to the assurance ***level*** 'high'; ~~by the physical presence of the natural person or of an authorised representative of the legal person; or~~

(b) by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a), (c) or (d)**.** ~~remotely, using electronic identification means, for which prior to the issuance of the qualified certificate, a physical presence of the natural person or of an authorised representative of the legal person was ensured and which meets the requirements set out in Article 8 with regard to the assurance levels 'substantial' or 'high'; or~~

(c) by using other identification methods which ensure the identification of the person with a high level of confidence, the conformity of which shall be confirmed by a conformity assessment body;~~by means of a certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) or (b); or~~

(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.*~~by using other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body.~~

(da) ***The verification of the attributes referred to in the first subparagraph shall be verified, by appropriate means, by the qualified trust service provider, either directly or by relying on a third party, based on one of the following methods or on a combination thereof when needed, and in accordance with the implementing acts referred to in paragraph 1a:***

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

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

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

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

(v) through the physical presence of the natural person or of an authorised representative of the legal person by appropriate [evidences,] procedures and in accordance with national laws.'

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

2. A qualified trust service provider providing qualified trust services shall:

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

~~inform the supervisory body of any change in the provision of its qualified trust services and an intention to cease those activities;~~

(b) employ staff and, if applicable, subcontractors who possess the necessary expertise, reliability, experience, and qualifications and who have received appropriate training regarding security and personal data protection rules and shall apply administrative and management procedures which correspond to European or international standards;

(c) with regard to the risk of liability for damages in accordance with Article 13, maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with national law;

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

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

(f) use trustworthy systems to store data provided to it, in a verifiable form so that:

(i) they are publicly available for retrieval only where the consent of the person to whom the data relates has been obtained,

(ii) only authorised persons can make entries and changes to the stored data,

(iii) the data can be checked for authenticity;

(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 ***21*** of Directive ***(EU) 2022/2555***, those measures shall include at least the following:

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

(ii) measures related to procedural or administrative checks;

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

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

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

(h) record and keep accessible as long as necessary~~for an appropriate period of time~~, including 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, ~~in particular,~~ for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. Such recording may be done electronically;

(i) have an up-to-date termination plan to ensure continuity of service in accordance with provisions verified by the supervisory body under point (i) of Article ~~17~~46b(4);

~~(j) ensure lawful processing of personal data in accordance with Directive 95/46/EC;~~

(k) in case of qualified trust service providers issuing qualified certificates, establish and keep updated a certificate database.

3. If a qualified trust service provider issuing qualified certificates decides to revoke a certificate, it shall register such revocation in its certificate database and publish the revocation status of the certificate in a timely manner, and in any event within 24 hours after the receipt of the request. The revocation shall become effective immediately upon its publication.

4. With regard to paragraph 3, qualified trust service providers issuing qualified certificates shall provide to any relying party information on the validity or revocation status of qualified certificates issued by them. This information shall be made available at least on a per certificate basis at any time and beyond the validity period of the certificate in an automated manner that is reliable, free of charge and efficient.

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

5. ***By... [***12 months ***after the date*** of the entering into force of this ***amending*** Regulation***]***, the ~~The~~ Commission ~~may~~shall, by means of implementing acts, establish ***a list of reference*** standards ***and where necessary, establish specifications and procedures*** for the requirements referred to in paragraph ***2(b) to (h) of this Article***~~reference numbers of standards for trustworthy systems and products, which comply with the requirements under points (e) and (f) of paragraph 2 of this Article~~. Compliance with the requirements laid down in this ***paragraph of this*** Article shall be presumed, where ***those standards, specifications, and procedures are met***~~trustworthy systems and products meet those standards~~. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

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

Article 24a - Recognition of qualified trust services

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

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

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

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

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

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

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

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

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

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

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

SECTION 4 - Electronic signatures

Article 25 - Legal effects of electronic signatures

1. An electronic signature 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 signatures.

2. A qualified electronic signature shall have the equivalent legal effect of a handwritten signature.

~~3. A qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States.~~

Article 26 - Requirements for advanced electronic signatures

1. An advanced electronic signature shall meet the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

2. Within 24 months after the entry into force of this Regulation, the Commission shall carry out an assessment on whether it is necessary to adopt an implementing act, establishing a list of reference standards and when necessary, establishing specifications and procedures for advanced electronic signatures. Based on the outcome of this assessment, the Commission may adopt such an implementing act. Compliance with the requirements for advanced electronic signatures shall be presumed when an advanced electronic signature meets those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 27 - Electronic signatures in public services

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

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

3. Member States shall not request for cross-border use in an online service offered by a public sector body an electronic signature at a higher security level than the qualified electronic signature.

~~4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic signatures. Compliance with the requirements for advanced electronic signatures referred to in paragraphs 1 and 2 of this Article and in Article 26 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).~~

5. By 18 September 2015, and taking into account existing practices, standards and Union legal acts, the Commission shall, by means of implementing acts, define reference formats of advanced electronic signatures or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 28 - Qualified certificates for electronic signatures

1. Qualified certificates for electronic signatures shall meet the requirements laid down in Annex I.

2. Qualified certificates for electronic signatures shall not be subject to any mandatory requirement exceeding the requirements laid down in Annex I.

3. Qualified certificates for electronic signatures may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic signatures.

4. If a qualified certificate for electronic signatures has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of a qualified certificate for electronic signature:

(a) if a qualified certificate for electronic signature has been temporarily suspended that certificate shall lose its validity for the period of suspension;

(b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.

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

Article 29 - Requirements for qualified electronic signature creation devices

1. Qualified electronic signature creation devices shall meet the requirements laid down in Annex II.

1a. Generating ***or*** managing ***electronic signature creation data or*** duplicating ***such*** signature creation data ***for back-up purposes may only be done*** on behalf of ***and at the request of the signatory*** by a qualified trust service provider providing a qualified trust service for the management of a remote qualified ***electronic*** signature creation device.

2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified electronic signature creation devices. Compliance with the requirements laid down in Annex II shall be presumed where a qualified electronic signature creation device meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 29a - Requirements for a qualified service for the management of remote *qualified* electronic signature creation devices

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

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

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

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

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

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

2. ***By... [***12 months ***after the entry*** into force of this ***amending*** Regulation***]***, the Commission shall, by means of implementing acts, establish ***reference standards and, when necessary, technical and operational specifications*** for the purposes of paragraph 1. ***These implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).***

Article 30 - Certification of qualified electronic signature creation devices

1. Conformity of qualified electronic signature creation devices with the requirements laid down in Annex II shall be certified by appropriate public or private bodies designated by Member States.

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

3. The certification referred to in paragraph 1 shall be based on one of the following:

(a) a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in the list established in accordance with the second subparagraph; or

(b) a process other than the process referred to in point (a), provided that it uses comparable security levels and provided that the public or private body referred to in paragraph 1 notifies that process to the Commission. That process may be used only in the absence of standards referred to in point (a) or when a security evaluation process referred to in point (a) is ongoing.

The Commission shall, by means of implementing acts, establish a list of standards for the security assessment of information technology products referred to in point (a). Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

3a. The ***validity of a*** certification referred to in paragraph 1 shall ***not exceed*** 5 years, conditional upon a regular 2 year vulnerabilities assessment. Where vulnerabilities are identified and not remedied, the certification shall be ***cancelled***.

4. The Commission shall be empowered to adopt delegated acts in accordance with Article 47 concerning the establishment of specific criteria to be met by the designated bodies referred to in paragraph 1 of this Article.

Article 31 - Publication of a list of certified qualified electronic signature creation devices

1. Member States shall notify to the Commission without undue delay and no later than one month after the certification is concluded, information on qualified electronic signature creation devices that have been certified by the bodies referred to in Article 30(1). They shall also notify to the Commission, without undue delay and no later than one month after the certification is cancelled, information on electronic signature creation devices that are no longer certified.

2. On the basis of the information received, the Commission shall establish, publish and maintain a list of certified qualified electronic signature creation devices.

3. ***By... [***12 months ***after the date of entry*** into force of this ***amending*** Regulation***]***, the~~The~~ Commission ~~may~~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).

Article 32 - Requirements for the validation of qualified electronic signatures

1. The process for the validation of a qualified electronic signature shall confirm the validity of a qualified electronic signature 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 electronic signature was created by a qualified electronic signature creation device;

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

(h) 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 qualified electronic signatures meet the standards***, specifications and procedures*** referred to in paragraph 3.

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

3. ***By.... [***12 months ***after the date*** of the entering into force of this ***amending*** Regulation***]***, the~~The~~ Commission ~~may~~shall, by means of implementing acts, establish ***a list of reference*** standards ***and when necessary, establish specifications and procedures*** ~~reference numbers of standards~~ for the validation of qualified electronic signatures. ~~Compliance with the requirements laid down in paragraph 1 shall be presumed where the validation of qualified electronic signatures meets those standards.~~ Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

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

1. The process for the validation of an advanced electronic signature based on 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.

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

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

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

Article 33 - Qualified validation service for qualified electronic signatures

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

(a) provides validation in compliance with Article 32(1); and

(b) allows relying parties to receive the result of the validation process in an automated manner, which is reliable, efficient and bears the advanced electronic signature or advanced electronic seal of the provider of the qualified validation service.

2. ***By.... [12 months after the date of the entering into force of this amending Regulation], the*** ~~The~~ Commission ***shall*** ~~may~~, by means of implementing acts, ***establish a list of reference standards and when necessary, establish specifications and procedures*** ~~establish 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 signatures meets those standards***, specifications and procedures***. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

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. ~~The Commission may, by means of implementing acts, establish reference numbers of standards for the qualified preservation service for qualified electronic signatures.~~ 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 ~~those~~ the standards~~.~~, ***specifications and procedures*** referred to in paragraph 3.~~Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).~~

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

SECTION 5 - Electronic seals

Article 35 - Legal effects of electronic seals

1. An electronic seal 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 seals.

2. A qualified electronic seal shall enjoy the presumption of integrity of the data and of correctness of the origin of that data to which the qualified electronic seal is linked.

~~3. A qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States.~~

Article 36 - Requirements for advanced electronic seals

1. An advanced electronic seal shall meet the following requirements:

(a) it is uniquely linked to the creator of the seal;

(b) it is capable of identifying the creator of the seal;

(c) it is created using electronic seal creation data that the creator of the seal can, with a high level of confidence under its control, use for electronic seal creation; and

(d) it is linked to the data to which it relates in such a way that any subsequent change in the data is detectable.

2. By... [24 months after the date of the entering into force of this amending Regulation], the Commission shall carry out an assessment on whether it is necessary to adopt an implementing act, establishing a list of reference standards and when necessary, establishing specifications and procedures for advanced electronic seals. Based on the outcome of this assessment, the Commission may adopt such an implementing act. Compliance with the requirements for advanced electronic seals shall be presumed when an advanced electronic seal meets those standards, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 37 - Electronic seals in public services

1. If a Member State requires an advanced electronic seal in order to use an online service offered by, or on behalf of, a public sector body, that Member State shall recognise advanced electronic seals, advanced electronic seals based on a qualified certificate for electronic seals and qualified electronic seals at least in the formats or using methods defined in the implementing acts referred to in paragraph 5.

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

3. Member States shall not request for the cross-border use in an online service offered by a public sector body an electronic seal at a higher security level than the qualified electronic seal.

~~4. The Commission may, by means of implementing acts, establish reference numbers of standards for advanced electronic seals. Compliance with the requirements for advanced electronic seals referred to in paragraphs 1 and 2 of this Article and Article 36 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).~~

5. By 18 September 2015, and taking into account existing practices, standards and legal acts of the Union, the Commission shall, by means of implementing acts, define reference formats of advanced electronic seals or reference methods where alternative formats are used. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

Article 38 - Qualified certificates for electronic seals

1. Qualified certificates for electronic seals shall meet the requirements laid down in Annex III.

2. Qualified certificates for electronic seals shall not be subject to any mandatory requirements exceeding the requirements laid down in Annex III.

3. Qualified certificates for electronic seals may include non-mandatory additional specific attributes. Those attributes shall not affect the interoperability and recognition of qualified electronic seals.

4. If a qualified certificate for an electronic seal has been revoked after initial activation, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted.

5. Subject to the following conditions, Member States may lay down national rules on temporary suspension of qualified certificates for electronic seals:

(a) if a qualified certificate for electronic seal has been temporarily suspended, that certificate shall lose its validity for the period of suspension;

(b) the period of suspension shall be clearly indicated in the certificate database and the suspension status shall be visible, during the period of suspension, from the service providing information on the status of the certificate.

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

Article 39 - Qualified electronic seal creation devices

1. Article 29 shall apply mutatis mutandis to requirements for qualified electronic seal creation devices.

2. Article 30 shall apply mutatis mutandis to the certification of qualified electronic seal creation devices.

3. Article 31 shall apply mutatis mutandis to the publication of a list of certified qualified electronic seal creation devices.

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.

Article 40 - Validation and preservation of qualified electronic seals

Articles 32, 33 and 34 shall apply mutatis mutandis to the validation and preservation of qualified electronic seals.

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

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

SECTION 6 - Electronic time stamps

Article 41 - Legal effect of electronic time stamps

1. An electronic time stamp 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 of the qualified electronic time stamp.

2. A qualified electronic time stamp shall enjoy the presumption of the accuracy of the date and the time it indicates and the integrity of the data to which the date and time are bound.

~~3. A qualified electronic time stamp issued in one Member State shall be recognised as a qualified electronic time stamp in all Member States.~~

Article 42 - Requirements for qualified electronic time stamps

1. A qualified electronic time stamp shall meet the following requirements:

(a) it binds the date and time to data in such a manner as to reasonably preclude the possibility of the data being changed undetectably;

(b) it is based on an accurate time source linked to Coordinated Universal Time; and

(c) it is signed using an advanced electronic signature or sealed with an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

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

2. ***By ... [***12 months ***after the date*** of the entering into force of this ***amending*** Regulation***]***, the ~~The~~ Commission ~~may~~shall, by means of implementing acts, establish ***a list of reference*** standards ***and when necessary, establish specifications and procedures*** ~~reference numbers of standards~~ for the binding of date and time to data and for ***establishing the accuracy of*** ~~accurate~~ time sources. ~~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 meets those standards.~~ Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 7 - Electronic registered delivery services

Article 43 - Legal effect of an electronic registered delivery service

1. Data sent and received using an electronic registered delivery service 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 of the qualified electronic registered delivery service.

2. Data sent and received using a qualified electronic registered delivery service shall enjoy the presumption of the integrity of the data, the sending of that data by the identified sender, its receipt by the identified addressee and the accuracy of the date and time of sending and receipt indicated by the qualified electronic registered delivery service.

Article 44 - Requirements for qualified electronic registered delivery services

1. Qualified electronic registered delivery services shall meet the following requirements:

(a) they are provided by one or more qualified trust service provider(s);

(b) they ensure with a high level of confidence the identification of the sender;

(c) they ensure the identification of the addressee before the delivery of the data;

(d) the sending and receiving of data is secured by an advanced electronic signature or an advanced electronic seal of a qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;

(e) any change of the data needed for the purpose of sending or receiving the data is clearly indicated to the sender and addressee of the data;

(f) the date and time of sending, receiving and any change of data are indicated by a qualified electronic time stamp.

In the event of the data being transferred between two or more qualified trust service providers, the requirements in points (a) to (f) shall apply to all the qualified trust service providers.

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

2. ~~2.~~ ***By ... [***12 months ***after the date*** of the entering into force of this ***amending*** Regulation***]***, the~~The~~ Commission ~~may~~shall, by means of implementing acts, establish ***a list of reference*** standards ***and when necessary, establish specifications and procedures*** ~~reference numbers of standards~~ for processes for sending and receiving data. ~~Compliance with the requirements laid down in paragraph~~

~~1 shall be presumed where the process for sending and receiving data meets those standards.~~ Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

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

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

SECTION 8 - Website authentication

Article 45 - Requirements for qualified certificates for website authentication

1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV. ***Evaluation of compliance with those requirements*** shall be ***carried out in accordance with the standards and the specifications*** referred to in paragraph 3.

2. Qualified certificates for website authentication ***issued in accordance with*** paragraph 1 shall be recognised by web-browsers. Web-browsers shall ensure that the identity data ***attested in the certificate and additional attested attributes are*** 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 ***during*** the first 5 years of operating as providers of web-browsing services.

~~2. The Commission may, by means of implementing acts, establish reference numbers of standards for qualified certificates for website authentication. Compliance with the requirements laid down in Annex IV shall be presumed where a qualified certificate for website authentication meets those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).~~2b. ***Qualified certificates for website authentication shall not be subject to any mandatory requirements other than the requirements laid down in paragraph 1.***

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

Article 45a-1 - Cybersecurity precautionary measures

1. Web-browsers shall not take any measures contrary to their obligations set out in Article 45, notably the requirement to recognise Qualified Certificates for Website Authentication, and to display the identity data provided in a user friendly manner.

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

3. Where measures are taken, web-browsers shall notify their concerns in writing without undue delay, jointly with a description of the measures taken to mitigate those concerns, to the Commission, the competent supervisory authority, the entity to whom the certificate was issued and

to the qualified trust service provider that issued that certificate or set of certificates. Upon receipt of such a notification, the competent supervisory authority shall issue an acknowledgement of receipt to the web-browser in question.

4. The competent supervisory authority shall consider the issues raised in the notification in accordance with Article 17(3)(c). When the outcome of that investigation does not result in the withdrawal of the qualified status of the certificate(s), the supervisory authority shall inform the web-browser accordingly and request it to put an end to the precautionary measures referred to in paragraph 2.

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.

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

Article 45b - Electronic attestation of attributes in public services

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

Article 45c - Requirements for qualified electronic attestation of attributes

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

1a. Evaluation of compliance with the requirements laid down in Annex V shall be carried out in accordance with the standards, specifications and procedures 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. ***By ... [***6 months ***after the date*** of the entering into force of this ***amending*** Regulation***]***, the Commission shall***, by means of implementing acts,*** establish ***a list of reference*** standards ***and when***

necessary, establish specifications and procedures for qualified electronic attestations of attributes***. Those implementing acts shall be consistent with the*** implementing act ***referred to in Article 6a(11)*** on the implementation of the European Digital Identity ***Wallet and shall be adopted in accordance with the examination procedure*** referred to in Article ***48(2)***

Article 45d - Verification of attributes against authentic sources

1. Member States shall ensure ***within 24 months after entry into force of the implementing acts referred to in Article 6a(11) and Article 6c(4)*** that, at least for the attributes listed in Annex VI, wherever these attributes rely on authentic sources within the public sector, measures are taken to allow qualified ***trust service*** providers of electronic attestations of attributes to verify ***these attributes*** by electronic means at the request of the user ***and*** in accordance with national or Union law.

2. ***By … [***6 months ***after the date*** of the entering into force of this ***amending*** Regulation***], the Commission shall***, taking into account relevant international standards, ***by means of implementing acts, establish a list of reference*** standards and ***when necessary, establish specifications and procedures for*** the catalogue of attributes and schemes for the attestation of attributes and verification procedures for qualified electronic attestations of attributes***. Those implementing acts shall be consistent with the*** implementing act ***referred to in Article 6a(11)*** on the implementation of the European Digital Identity ***Wallet and shall be adopted in accordance with the examination procedure*** referred to in Article ***48(2)***.

Article 45da - Requirements for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source.

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

(a) the requirements set out in Annex VIa;

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

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

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

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

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

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

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

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

6. By … [6 months after the date of the entering into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and when necessary, establish specifications and procedures for electronic attestation of attributes issued by or on behalf of a public sector body responsible for an authentic source. Those implementing acts shall be consistent with the implementing act referred to in Article 6a(11) on the implementation of the European Digital Identity Wallet and shall be adopted in accordance with the examination procedure referred to in Article 48(2).

7. By … [6 months after the date of entry into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and when necessary, establish specifications, formats and procedures for the purposes of paragraph 3. Those implementing acts shall be consistent with the implementing act referred to in Article 6a(11) on the implementation of the European Digital Identity Wallet and shall be adopted in accordance with the examination procedure referred to in Article 48(2).”

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

Article 45e - Issuing of electronic attestation of attributes to the European Digital Identity Wallets

1. Providers of electronic attestations of attributes shall provide EUDI Wallet users with the possibility to request, obtain, store and manage the electronic attestation of attributes irrespective of the Member States where the wallet is provided.

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

Article 45f - Additional rules for the provision of electronic attestation of attributes services

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

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

4. Providers of qualified electronic attestation of attributes' services shall ***implement the provision of such qualified trust*** services ***in a manner that is functionally separated from any other service provided by them***.

SECTION 10 - ELECTRONIC ARCHIVING SERVICES

Article 45g - *Legal effect of* electronic archiving services

1. Electronic data and electronic documents preserved 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 preserved using a qualified electronic archiving service.

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

Article 45ga - Requirements for qualified electronic archiving services

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

(a) They are provided by qualified trust service providers

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

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

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

2. By … [12 months after the date of the entering into force of this amending Regulation], the Commission shall, by means of implementing acts, establish a list of reference standards and when necessary, establish specifications and procedures 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, specifications and procedures. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

SECTION 11 - ELECTRONIC LEDGERS

Article 45h - Legal effects of electronic ledgers

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

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

Article 45i - Requirements for qualified electronic ledgers

1. Qualified electronic ledgers shall meet the following requirements:

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

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

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

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

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

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

CHAPTER IV - ELECTRONIC DOCUMENTS

Article 46 - Legal effects of electronic documents

An electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

CHAPTER IVa - GOVERNANCE FRAMEWORK

Article 46a - Supervision of the EDIW framework

1. Member States shall designate one or more supervisory bodies established in their territory. Supervisory bodies shall be given the necessary powers and adequate resources for the exercise of their tasks in an effective, efficient and independent manner.

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

3. The role of the supervisory bodies shall be:

- *(a) to supervise providers of European Digital Identity Wallets established in the designating Member State and to ensure, through ex ante and ex post supervisory activities, that those issuers and the European Digital Identity Wallets they provide meet the requirements laid down in this Regulation.*
- *(b) to take action, if necessary, in relation to providers of European Digital Identity Wallets established in the territory of the designating Member State, through ex post supervisory activities, when informed that those issuers and the European Digital Identity Wallets they provide allegedly do not meet the requirements laid down in this Regulation.*

4. The tasks of the supervisory bodies shall include in particular:

- *(a) to cooperate with other supervisory bodies and to provide them with assistance in accordance with Articles 46c and 46e;*
- *(b) to request information necessary to monitor the compliance with the relevant provisions of this Regulation;*
- *(c) to inform the relevant national competent authorities of the Member States concerned, designated pursuant to Directive (EU) 2022/2555, of any significant breaches of security or loss of integrity they become aware of in the performance of their tasks and, in the case of a significant breach of security or loss of integrity which concerns other Member States, to inform the single point of contact of the Member State concerned designated pursuant to Directive (EU) 2022/2555 and single points of contact designated pursuant to Article 46c of this Regulation in the other Member States concerned. The notified supervisory body shall inform the public or require the European Digital Identity Wallet provider to do so where it determines that disclosure of the breach of security or loss of integrity is in the public interest;*
- *(d) to carry out on-site inspections and off-site supervision;*
- *(e) to require that providers of European Digital Identity Wallets remedy any failure to fulfil the requirements laid down in this Regulation;*

(f) To suspend or cancel the registration and inclusion of relying parties in the mechanism referred to in Article 6b(2) in the case of illegal or fraudulent use of the European Digital Identity Wallet;

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

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

6. By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities.

7. The Commission shall make the annual reports referred to in paragraph 6 available to the European Parliament and the Council.

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

Article 46b - Supervision of trust services

1. Member States shall designate a supervisory body established in their territory or, upon mutual agreement with another Member State, a supervisory body established in that other Member State. That body shall be responsible for supervisory tasks in the designating Member State. Supervisory bodies shall be given the necessary powers and adequate resources for the exercise of their tasks.

2. Member States shall notify to the Commission the names and the addresses of their respective designated supervisory bodies.

3. The role of the supervisory body shall be:

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

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

4. The tasks of the supervisory body shall include in particular:

(a) to inform the relevant national competent authorities of the Member States concerned, designated pursuant to Directive (EU) 2022/2555, of any significant breaches of security or loss of integrity they become aware of in the performance of their tasks and, in the case of a significant breach of security or loss of integrity which concerns other Member States, to inform the single point of contact of the Member State concerned designated pursuant to Directive (EU) 2022/2555 and single points of contact designated pursuant to [Article 46c] of this Regulation in the other Member States concerned. The notified supervisory body shall inform the public or require the trust service provider to do so where it determines that disclosure of the breach of security or loss of integrity is in the public interest;

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

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

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

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

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

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

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

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

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

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

5. Member States may require the supervisory body to establish, maintain and update a trust infrastructure in accordance with the conditions under national law.

6. By 31 March each year, each supervisory body shall submit to the Commission a report on its previous calendar year's main activities.

7. The Commission shall make the annual reports referred to in paragraph 6 available to the European Parliament and the Council.

8. By … [12 months after the date of entry into force of this amending Regulation], the Commission shall adopt guidelines on the exercise by the Supervisory bodies of the tasks referred to in paragraph 4, and, by means of implementing acts adopted in accordance with the examination procedure referred to in Article 48(2), define the formats and procedures for the report referred to in paragraph 6.

Article 46c - Single points of contact

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

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

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

4. The Commission shall publish a list of the notified single points of contact.

Article 46d - Mutual assistance

1. In order to facilitate the supervision and enforcement of obligations under this Regulation, supervisory bodies responsible for trust services and for European Digital Identity Wallets may seek, including through the EDICG, mutual assistance from supervisory bodies of another Member State where the trust service provider or the provider of the European Digital Identity Wallet is established, its network and information systems are located, or its services are provided.

2. The mutual assistance shall at least entail that:

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

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

(c) where appropriate, supervisory bodies may carry out joint investigations with other Member States' supervisory bodies. The arrangements and procedures for such joint actions shall be agreed upon and established by the Member States concerned in accordance with their national law.

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

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

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

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

4. By … [12 months after the date of entry into force of this amending Regulation] [and every two years thereafter], the EDICG shall issue guidance on the organisational aspects and procedures for the mutual assistance referred to in paragraphs 1 and 2.

Article 46e - The European Digital Identity Cooperation Group

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

2. The EDICG shall be composed of representatives appointed by the Member States and of the Commission. The EDICG shall be chaired by the Commission who shall provide the EDICG Secretariat.

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

4. The European Union Agency for Cybersecurity shall be invited to participate as observer in the workings of the EDICG when it exchanges views, best practices and information on relevant cybersecurity aspects such as notification of security breaches, the use of cybersecurity certificates or standards are addressed.

5. The EDICG shall have the following tasks:

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

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

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

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

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

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

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

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

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

(vii) organise peer reviews of electronic identification schemes to be notified falling under this Regulation;

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

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

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

7. Within 12 months of the entry into force of the Regulation, the Commission shall, by means of implementing acts, establish the necessary procedural arrangements to facilitate the cooperation between the Member States referred to in point (vii) of paragraph 5 . That implementing act shall be adopted in accordance with the examination procedure referred to in Article 48(2).

CHAPTER V - DELEGATIONS OF POWER AND IMPLEMENTING PROVISIONS

Article 47 - Exercise of the delegation

1. The power to adopt delegated acts is conferred on the Commission subject to the conditions laid down in this Article.

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

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

4. As soon as it adopts a delegated act, the Commission shall notify it simultaneously to the European Parliament and to the Council.

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

Article 48 - Committee procedure

1. The Commission shall be assisted by a committee. That committee shall be a committee within the meaning of Regulation (EU) No 182/2011.

2. Where reference is made to this paragraph, Article 5 of Regulation (EU) No 182/2011 shall apply.

Article 48a - Reporting requirements

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

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

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

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

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

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

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

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

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

CHAPTER VI - FINAL PROVISIONS

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 months after its entering into force.~~no later than 1 July 2020~~. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions, ***including, in particular, the provisions included in Article 6c(3)***~~including Article 6, point (f) of Article 7 and Articles 34, 43, 44 and 45~~, taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments. Where necessary, that report shall be accompanied by a proposal for amendment of this Regulation.

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

~~The report referred to in the first paragraph shall be accompanied, where appropriate, by legislative proposals.~~

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.

Article 50 - Repeal

1. Directive 1999/93/EC is repealed with effect from 1 July 2016.

2. References to the repealed Directive shall be construed as references to this Regulation.

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 be considered as qualified electronic signature

creation devices under this Regulation until ***36 months*** following the entry into force of this Regulation.

2. Qualified certificates issued to natural persons under Directive 1999/93/EC shall be considered as qualified certificates for electronic signatures under this Regulation until ***24 months after*** the entry into force of this Regulation.~~they expire.~~

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 after the entry into force of this Regulation.

2b. Qualified trust service providers that have been granted their qualified status under this Regulation before [date of entry into force of the amending Regulation], using methods for identity verification for the issuance of qualified certificates in compliance with Article 24(1), shall submit a conformity assessment report to the supervisory body proving compliance with Article 24(1) as soon as possible, but no later than 24 months after entry into force of the amending Regulation. Until the submission of such a conformity assessment report and the completion of its assessment by the supervisory body, the qualified trust service provider may continue to rely on the use of the methods for identity verification set out in Article 24(1) of Regulation (EU) No 910/2014.

3. A certification-service-provider issuing qualified certificates under Directive 1999/93/EC shall submit a conformity assessment report to the supervisory body as soon as possible but not later than 1 July 2017. Until the submission of such a conformity assessment report and the completion of its assessment by the supervisory body, that certification-service-provider shall be considered as qualified trust service provider under this Regulation.

4. If a certification-service-provider issuing qualified certificates under Directive 1999/93/EC does not submit a conformity assessment report to the supervisory body within the time limit referred to in paragraph 3, that certification-service-provider shall not be considered as qualified trust service provider under this Regulation from 2 July 2017.

Article 52 - Entry into force

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

2. This Regulation shall apply from 1 July 2016, except for the following:

(a) Articles 8(3), 9(5), 12(2) to (9), 17(8), 19(4), 20(4), 21(4), 22(5), 23(3), 24(5), 27(4) and (5), 28(6), 29(2), 30(3) and (4), 31(3), 32(3), 33(2), 34(2), 37(4) and (5), 38(6), 42(2), 44(2), 45(2), and Articles 47 and 48 shall apply from 17 September 2014;

(b) Article 7, Article 8(1) and (2), Articles 9, 10, 11 and Article 12(1) shall apply from the date of application of the implementing acts referred to in Articles 8(3) and 12(8);

(c) Article 6 shall apply from three years as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8).

3. Where the notified electronic identification scheme is included in the list published by the Commission pursuant to Article 9 before the date referred to in point (c) of paragraph 2 of this Article, the recognition of the electronic identification means under that scheme pursuant to Article 6 shall take place no later than 12 months after the publication of that scheme but not before the date referred to in point (c) of paragraph 2 of this Article.

4. Notwithstanding point (c) of paragraph 2 of this Article, a Member State may decide that electronic identification means under electronic identification scheme notified pursuant to Article 9(1) by another Member State are recognised in the first Member State as from the date of application of the implementing acts referred to in Articles 8(3) and 12(8). Member States concerned shall inform the Commission. The Commission shall make this information public.

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

Done at Brussels,

ANNEX I - REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SIGNATURES

Qualified certificates for electronic signatures shall contain:

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

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

- for a legal person: the name and, where applicable, registration number as stated in the official records,
- for a natural person: the person's name;

(c) at least the name of the signatory, or a pseudonym; if a pseudonym is used, it shall be clearly indicated;

(d) electronic signature validation data that corresponds to the electronic signature creation data;

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

(f) the certificate identity code, which must be unique for the qualified trust service provider;

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

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

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

(j) where the electronic signature creation data related to the electronic signature validation data is located in a qualified electronic signature creation device, an appropriate indication of this, at least in a form suitable for automated processing.

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.

~~3. Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider.~~

~~4. Without prejudice to point (d) of point 1, qualified trust service providers managing electronic signature creation data on behalf of the signatory may duplicate the electronic signature creation data only for back-up purposes provided the following requirements are met:~~

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

~~(b) the number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.~~

ANNEX III - REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR ELECTRONIC SEALS

Qualified certificates for electronic seals shall contain:

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

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

- for a legal person: the name and, where applicable, registration number as stated in the official records,
- for a natural person: the person's name;

(c) at least the name of the creator of the seal and, where applicable, registration number as stated in the official records;

(d) electronic seal validation data, which corresponds to the electronic seal creation data;

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

(f) the certificate identity code, which must be unique for the qualified trust service provider;

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

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

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

(j) where the electronic seal creation data related to the electronic seal validation data is located in a qualified electronic seal creation device, an appropriate indication of this, at least in a form suitable for automated processing.

ANNEX IV - REQUIREMENTS FOR QUALIFIED CERTIFICATES FOR WEBSITE AUTHENTICATION

Qualified certificates for website authentication shall contain:

(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for website authentication;

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

- for a legal person: the name and, where applicable, registration number as stated in the official records,
- for a natural person: the person's name;

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

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

(d) elements of the address, including at least city and State, of the natural or legal person to whom the certificate is issued and, where applicable, as stated in the official records;

(e) the domain name(s) operated by the natural or legal person to whom the certificate is issued;

(f) details of the beginning and end of the certificate's period of validity;

(g) the certificate identity code, which must be unique for the qualified trust service provider;

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

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

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

Annex V - REQUIREMENTS FOR QUALIFIED ELECTRONIC ATTESTATION OF ATTRIBUTES

Qualified electronic attestation of attributes shall contain:

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

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

- for a legal person: the name and, where applicable, registration number as stated in the official records,
- for a natural person: the person's name;

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

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

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

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

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

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

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

Annex VI - MINIMUM LIST OF ATTRIBUTES

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

1. Address;

2. 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;

8a. ***Powers and mandates to represent natural or legal persons***

9. Public permits and licenses;

10. ***For legal persons,*** financial and company data.

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

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

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

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

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

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

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

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

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

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

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