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

CHAPTER I

GENERAL PROVISIONS

Article 1

Subject matter

With a view to ensuring the proper functioning of the internal market while aiming at an adequate level of security of electronic identification means and trust services this Regulation:

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

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

Article 2

Scope

1 This Regulation applies to electronic identification schemes that have been notified by a Member State, 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.

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 legal person;

(2) ‘electronic identification means’ means a material and/or immaterial unit containing person identification data and which is used for authentication for an online service;

(3) ‘person identification data’ means a set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established;

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

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

(6) ‘relying party’ means a natural or legal person that relies upon an electronic identification 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[(1)];

(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 creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

(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;

(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 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;

(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 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 an electronic signature or a seal is valid.

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.

2 Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms 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.

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);

(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 Commission shall publish in the *Official Journal of the European Union* a list of the electronic identification schemes which were notified pursuant to paragraph 1 of this Article and the basic information thereon.

3 If 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 months 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

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 12

Cooperation and 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 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 representing a natural or legal person, 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 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 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, 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 and 8 of this Article shall be adopted in accordance with the examination procedure referred to in Article 48(2).

CHAPTER III

TRUST SERVICES

SECTION 1

General provisions

Article 13

Liability and burden of proof

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 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 are recognised under an agreement concluded between the Union and the third country in question or an international organisation in accordance with Article 218 TFEU.

2 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;

b 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.

Article 15

Accessibility for persons with disabilities

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.

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).

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 the 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. The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.

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 inform the 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.

4 The Commission may, by means of implementing acts, establish reference number of the following standards:

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

b auditing rules under which conformity assessment bodies will carry out their conformity assessment of the qualified trust service providers as 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 services, they shall submit to the supervisory body a notification of their intention together with a conformity assessment report issued by a conformity assessment body.

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.

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

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.

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 The Commission may, by means of implementing acts, define the formats and procedures for the purpose 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 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 is issued.

The information referred to in the first subparagraph shall be verified by the qualified trust service provider either directly or by relying on a third party in accordance with national law:

a by the physical presence of the natural person or of an authorised representative of the legal person; or

b 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 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 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.

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

a 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 manner, 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;

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;

g take appropriate measures against forgery and theft of data;

h record and keep accessible 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(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.

5 The Commission may, by means of implementing acts, establish 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 Article shall be presumed where trustworthy systems and products meet those standards. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

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

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.

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

Article 29

Requirements for qualified electronic signature creation devices

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

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 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).

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 The Commission may, 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.

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 The Commission may, by means of implementing acts, establish 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 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 The Commission may, by means of implementing acts, 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 signature meets those standards. 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 paragraph 1 shall be presumed where the arrangements for the qualified preservation service for qualified electronic signatures meet those standards. 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

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.

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 The Commission may, by means of implementing acts, establish 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. 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 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.

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.

2 The Commission may, by means of implementing acts, establish reference numbers of standards for the binding of date and time to data and for 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.

2 The Commission may, by means of implementing acts, establish 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).

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.

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).

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 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 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 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 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.

CHAPTER VI

FINAL PROVISIONS

Article 49

Review

The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council 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 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.

The report referred to in the first paragraph shall be accompanied, where appropriate, by legislative proposals.

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.

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 they expire.

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, 23 July 2014.

For the Parliament

The President

M. SCHULZ

For the Council

The President

S. GOZI

(**1**) Directive 2014/24/EU of the European Parliament and of the Council of 26 February 2014 on public procurement and repealing Directive 2004/18/EC (OJ L 94, 28.3.2014, p. 65).

Status:
Point in time view as at 23/07/2014.

Changes to legislation:
There are currently no known outstanding effects for the Regulation (EU) No 910/2014 of the European Parliament and of the Council.