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

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.

Changes to legislation: *There are outstanding changes not yet made to Regulation (EU) No 910/2014 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

(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

***Changes to legislation:** There are outstanding changes not yet made to Regulation (EU) No 910/2014 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

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),

Changes to legislation: *There are outstanding changes not yet made to Regulation (EU) No 910/2014 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

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.

***Changes to legislation:** There are outstanding changes not yet made to Regulation (EU) No 910/2014 of the European Parliament and of the Council. Any changes that have already been made to the legislation appear in the content and are referenced with annotations. (See end of Document for details) View outstanding changes*

(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,