European Economic and Social Committee

OPINION

European Economic and Social Committee

eID

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity
[COM(2021) 281 final – 2021/0136 (COD)]

INT/951

Rapporteur: **Tymoteusz Adam ZYCH**

www.eesc.europa.eu

EN

www.eesc.europa.eu/facebook www.eesc.europa.eu/twitter www.eesc.europa.eu/linkedin www.eesc.europa.eu/instagram

Referral	European Parliament, 08/07/2021
	Council, 15/07/2021
Legal basis	Article 114 of the Treaty on the Functioning of the European Union
Section responsible	Single Market, Production and Consumption
Adopted in section	30/09/2021
Adopted at plenary	20/10/2021
Plenary session No	564
Outcome of vote (for/against/abstentions)	229/2/5

1. Conclusions and recommendations

1.1 The European Economic and Social Committee (EESC) welcomes the European Commission's proposal for an instrument amending the eIDAS Regulation as regards establishing a framework for a European Digital Identity (EDI), which would adjust this legal act to current market needs. Evaluation of the existing regulation has shown that there is a need to provide improved solutions for digital services that would extend access to both the private and public sectors, and be available for the vast majority of European citizens and residents.

1.2 However, the EESC notes that the proposed digitalisation of services may result in the exclusion of parts of European society, in particular older people, those with low digital literacy and persons with disabilities. Therefore, the EESC kindly invites the European Commission (EC) and the Member States to establish the necessary framework for digital education and information campaign, which at the same time should serve to increase awareness in the field of personal data protection.

1.3 The EESC welcomes the fact that use of EDI Wallet will be discretionary and free of charge. Nevertheless, the introduction of new digital solutions necessarily involves significant time and expense. Therefore, the EESC invites the EC to further assess the time needed for the actual implementation of the new Regulation in order to avoid negatively affecting the market, and to provide further analysis and greater clarity in the Regulation on the expected costs of its implementation.

1.4 The EESC notes that the proposed Section 9 of the Regulation provides for the mandatory cross-border recognition of qualified electronic attestation of attributes issued in a Member State. However, taking into account the fact that the provisions of Member States' domestic laws often differ significantly, the EESC recognises the need to clarify that the recognition of a qualified electronic attestation of attributes in one Member State is limited to confirmation of the facts, analogously to Article 2(4) of the Regulation on promoting the free movement of citizens by simplifying the requirements for presenting certain public documents in the European Union (EU) and amending Regulation (EU) No 1024/2012: "This Regulation does not apply to the recognition in a Member State of legal effects relating to the content of public documents issued by the authorities of another Member State".

1.5 From the EESC's point of view, effective data protection especially needs to be looked at in the context of the protection of fundamental rights, in particular the right to privacy and the right to the protection of personal data. Therefore, the EESC fully endorses the requirement that the European Digital Identity framework should give users the means to control who has access to their digital twin and exactly what data they can access. The EESC invites the EC and Member States to include, after consultations on technical aspects of the European Digital Identity framework, the issue of creating a register enabling users to track any access to their data.

1.6 The EESC would like to highlight security concerns relating to the digitalisation process, especially the development of the huge systems that store and process data vulnerable to fraud and loss. The EESC is also aware that there is currently no security system able to provide full data protection. Thus, in the EESC's opinion users of European Digital Identity Wallets should be guaranteed compensation for any undesirable situation relating to their data (e.g. data theft or disclosure). Such liability should be independent of whether the provider is at fault.

2. Introduction

2.1 The subject of this opinion is the EC's proposal for a regulation amending Regulation (EU) No 910/2014[1] (the "eIDAS Regulation") as regards establishing a framework for a EDI.

2.2 As set out in the Explanatory Memorandum, the eIDAS Regulation would provide the following protections and benefits: (1) access to highly secure and trustworthy electronic identity solutions, (2) assurance that public and private services can rely on trusted and secure digital identity solutions, (3) assurance that natural and legal persons are empowered to use digital identity solutions, (4) a guarantee that these solutions are linked to a variety of attributes and allow for the targeted sharing of identity data limited to the needs of the specific service requested, and (5) acceptance of qualified trust services in the EU and equal conditions for their provision. The proposed amendments are a response to the increase in demand for trusted digital cross-border solutions relying on the need to identify and authenticate users with a high level of assurance.

3. General comments

3.1 The EESC is aware of the new internal market demands concerning the development of electronic identification and trust services for electronic cross-border transactions. The existing solutions provided in the eIDAS Regulation, which started producing legal effects in several stages, starting in July 2016, do not meet these demands, which is confirmed by the fact that, as it stands, only 59% of EU residents have access to trusted and secure eID solutions. What is more, cross-border access to such services is limited due to the lack of interoperability between systems offered by individual Member States.

3.2 Therefore, the EESC welcomes the EC's new proposal for an instrument amending the eIDAS Regulation as regards establishing a framework for an EDI, which would adjust this legal act to current market needs. It is estimated that the solutions proposed in the Commission's

[1] OJ L 257, 28.8.2014, p. 73.

document could help to increase the number of digital ID users to as many as 80% or even 100% of all EU citizens and residents.

3.3 The EESC especially welcomes the solutions that aim to increase the security of users' personal data by guaranteeing the discretion to share the data and the possibility of controlling the nature and amount of data provided to relying parties. Since – according to the proposal – Member States will maintain control over digital service providers, they would guarantee that sensitive data sets (e.g. related to health, religion and beliefs, political opinions, racial or ethnic origin) are only provided upon request by service providers, following an informed decision taken by the identity owner in accordance with applicable national law.

3.4 The EESC points out that the timeline for the application of certain provisions of the new Regulation are rather optimistic, and invites the European Commission, when establishing the final application deadlines, also to take into consideration the time required for service providers to upgrade their IT systems to comply with the new obligations. The EESC therefore invites the EC to further analyse the time needed for the actual implementation of the new Regulation and thus to extend the timeline for its application so as not to affect the relevant market. As an example, the entry into force of the Regulation will require existing QTSPs offering remote signing based on QSCDs to become qualified providers for that specific service; it will take time for them to implement both the technical aspects and the authorisation procedure.

3.5 The EESC notes that the proposed digitalisation of services, regardless of its benefits, may also result in the exclusion of parts of European society, including in particular older people, those with low digital literacy and persons with disabilities. The EESC recognises the key role of European citizens' education in counteracting such exclusion; at the same time it should serve to increase awareness in the field of personal data protection.

4. **Availability and discretionary use of a European Digital Identity framework (EDIf)**

4.1 The EESC welcomes the idea of providing improved solutions for digital services that would extend access not only to public services, but also to the private sector. Moreover, the EESC agrees with the European Commission's attempts to make an EDIf available for the vast majority of European citizens. Due to the existing obstacles to access to eID services across borders (e.g. the lack of interoperability between eID schemes developed by Member States), many EU residents do not use them at all. The new solutions based on the EDI Wallets (EDIWs) may contribute making trusted online services available to at least 80% of Europeans.

4.2 Therefore, the EESC supports the proposal to require Member States to issue an EDIW– a tool that would enable the user to: (1) securely request and obtain, store, select, combine and share, in a manner that is transparent to and traceable by the user, the necessary legal person

identification data and electronic attestation of attributes to authenticate online and offline in order to use online public and private services, and (2) sign documents by means of a qualified electronic signature accepted throughout the EU.

4.3 Moreover, the EESC welcomes the proposal to ensure that the EDIW is equally accessible for persons with disabilities in line with the provisions of Annex I of Directive 2019/882, which is consistent with the EU principle of non-discrimination as set out in Article 21 of the Charter of Fundamental Rights of the EU. In order to avoid digital exclusion regarding that issue the EESC suggests that any solutions be developed in cooperation with the competent institutions and NGOs for persons with disabilities, on the basis of a "multi-stakeholder approach".

4.4 From the EESC's point of view, the fact that it will be left to the discretion of citizens and residents whether to use an EDIW is also a positive aspect. In the EESC's opinion, users should be under no obligation to use the wallet to access private or public services, but simply have the option to do so.

4.5 From the affordability perspective, the EESC welcomes the fact that use of the EDIW will be free of charge for users. However, the EESC invites the European Commission to further analyse and offer clarity in the Regulation on i) the issuing cost for natural persons, ii) the costs (issuing and usage) for legal entities, and iii) the costs of adding any digital identity attributes to such a wallet, as in the EESC's opinion each such addition would represent a trust service, thus entailing costs for the owner of the wallet.

5. **Usability aspects of a EDIf**

5.1 The EESC welcomes the European Commission's initiative to improve the usability of electronic identification means by creating a common EDIf based on cross-border reliance on an EDIW.

5.2 According to the proposal, usability may be improved by the means provided for in the new Article 12b of the eIDAS Regulation, containing a set of requirements concerning the recognition of EDIWs, addressed not only to Member States, but also to private relying parties providing services and "very large online platforms", defined in Article 25(1) of the proposed Digital Services Act[2]. On the basis of these new provisions some private sectors (i.e. transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education and telecommunications) should accept the use of EDIWs for the provision of services in cases where a strong user authentication for online identification is required by national or EU law or by contractual obligations. In light of the Commission's proposal, the same requirement would apply to the very large online platforms (e.g. social

2 COM/2020/825 final.

networks), which should accept the use of EDIWs in respect of the minimum attributes necessary for a specific online service for which authentication is requested, such as proof of age.

5.3 The EESC notes that, in order to guarantee the wide availability and usability of electronic identification means including EDIWs, private online service providers (which do not qualify as "very large platforms") should be involved in developing the self-regulatory "codes of conduct" facilitating wide acceptance of electronic identification means. The European Commission should be in charge of assessing the effectiveness and usability of such provisions for the users of EDIWs.

6. Issues concerning the legal effects of EDIWs

6.1 The EESC supports the proposal as regards the improvement in access to digital public services, including in cross-border situations.

6.2 The proposed new Section 9 of the eIDAS Regulation provides that a qualified electronic attestation of attributes issued in one Member State should be recognised as a qualified electronic attestation of attributes in any other Member State.

6.3 However, in respect of the domestic law of Member States, which may differ significantly in some cases, the EESC points out that the attributes attested against authentic sources in one Member State should be limited solely to confirmation of factual circumstances and should produce no legal effects in other Member States, unless the attested attributes comply with its national law. In essence, the proposed legal solutions should not affect the recognition in one Member State of legal effects relating to the content of the attributes attested against authentic sources in another Member State, by analogy with the provisions of Regulation (EU) 2016/1191[3] Some personal data (regarding a person's religion or beliefs) may serve as an example. In some EU countries, this kind of information causes legal effects (e.g., in Germany vital records include information on religion, which determines the obligation to pay a church tax in order to marry in a religious ceremony), while in other countries it does not (e.g. in Poland).

6.4 Therefore, the EESC invites the European Commission to consider clarifying the text of Section 9, so as to be clear that the recognition of a qualified electronic attestation of attributes in any other Member State is limited to confirmation of the factual circumstances related to the attribute in question, and does not produce legal effects in other Member States unless the attested attributes comply with their national law.

---

3 OJ L 200, 26. 07. 2016, p. 1.

7. **Security aspects**

A. Data protection in the context of fundamental rights

7.1 The EESC notes that, due to the lack of a common EDIf, in most cases citizens and other residents face obstacles in digital cross-border exchange of information related to their identity and, moreover, in exchanging such information securely and with a high level of data protection.

7.2 Therefore the EESC welcomes the attempts to create an interoperable and secure system based on EDIWs, which may enhance the exchange of information between Member States in relation, among other things, to employment situations or social rights. In this context, the EESC expects that the new EDIf will, for example, create possibilities for rapidly increasing cross-border employment opportunities, and for extending the automatic granting of social rights without additional application procedures or other administrative effort.

7.3 However, from the EESC's point of view, effective data protection is the main concern to be addressed in the context of the protection of fundamental rights, especially the right to privacy and the right to the protection of personal data.

7.4 Therefore, the EESC fully supports the requirement that the EDIf should offer everyone the means to control who has access to their digital twin and to which data exactly (including access by the public sector). As pointed out in the proposal, this will also require a high level of security with respect to all aspects of digital identity provisioning, including the issuing of EDIWs, and the infrastructure for the collection, storage and disclosure of digital identity data.

7.5 In that context, the EESC welcomes the proposal that users will be entitled to selectively disclose their attributes, limited to those that are necessary in a particular situation. According to the proposal, while using an EDIW, the user will have control over the amount of data provided to third parties and should be informed about the attributes required for the provision of a specific service.

7.6 The EESC supports the proposal for the physical and logical separation of personal data relating to the provision of EDIWs from any other data stored by the issuers of EDIWs, and approves of the requirement that providers of qualified electronic attestation of attributes services should sit under a separate legal entity.

7.7 In addition to effective data protection, which needs to be guaranteed, users' control over their data is essential. In that regard, the EESC would also approve the creation of an EDIf building on legal identities issued by Member States and on the provision of qualified and non-qualified digital identity attributes.

7.8 The EESC points out that in order to guarantee a high level of legal protection of users' data, users should be given more control over EDIWs, including the traceability of access to each user's data. For this purpose the technical aspects, to be determined during discussions following approval of the proposal, should include creating a register enabling the user to verify on request any instance of access to their data.

B. Other security and liability aspects

7.9 According to the proposal, the new EDIf will provide mechanisms for the prevention of fraud and for ensuring the authentication of personal identification data. Since the proposal includes a provision introducing means allowing for verification of attributes against authentic sources, this might improve, for example, child safety online by preventing them from accessing content inappropriate for their age. The EESC notes that at national level such effective protection is currently either not available or highly ineffective.

7.10 The EESC welcomes the idea that web browsers should ensure support and interoperability with qualified certificates for website authentication pursuant to the eIDAS Regulation. They should recognise and display qualified certificates for website authentication to provide a high level of assurance, allowing website owners to assert their identity as owners of a website and users to identify the website owners with a high degree of certainty. At the same time, the EESC sees a need to provide simple, fast and effective appeal mechanisms to ensure that a website is unblocked when it has been incorrectly marked as dangerous. Liability rules should also be established in relation to all the cases where a website has been incorrectly qualified as dangerous.

7.11 The EESC would like to point out that each digitalisation of data raises security concerns, especially the huge systems that store and process data, which constitute a source of information vulnerable to fraud and data loss. The EESC is also aware that there is currently no fully effective security system (i.e. free from gaps and errors) that would entirely eliminate such a threat.

7.12 Therefore, the EESC points out that, in order to minimise all such undesirable situations relating to users' data, the technical architecture of the EDIf developed by Member States in coordination with the Commission should focus on measures increasing data security and providing data control mechanisms. Such mechanisms are important in the context of e.g. using data collected from users for purposes other than originally intended. At the same time,

the EESC believes that the technical architecture should be developed with respect for fundamental rights and the principle of Members States' sovereignty.

7.13 The EESC notes that Article 13(1) of the eIDAS Regulation establishes liability for trust service providers for damage caused intentionally or negligently to any natural or legal person due to failure to comply with the obligations under that Regulation (and with the cybersecurity risk management obligations under Article 18 of the proposed "NIS 2 Directive", according to the Commission's proposal). This provision should be applied in accordance with national rules on liability (Article 13(3)).

7.14 In the context of liability concerns, the EESC would like to point out that the issues related to the definition of damage, its size and due compensation are regulated by the Members States' domestic law. According to these rules, the liability of trust service providers may be limited under the relevant provisions of domestic law and the "service provision policies", which are defined by the providers.

7.15 The EESC believes that users of EDIWs should be guaranteed compensation for any undesirable situation relating to their data, such as data theft, loss, disclosure, use for purposes other than originally intended, etc. Such liability should include all the situations mentioned above, irrespective of the provider's intention or negligence (irrespective of the provider's fault).

7.16 Any theft, unauthorised disclosure or loss of data (especially personal data) may cause long-term harm to its owner. Once digital information is released, it may be acquired in the long term by many entities, against the will of its owner. The EESC encourages the Commission and Member States to search for and develop effective mechanisms that would constitute a remedy for data owners in such cases.

7.17 The proposed solutions of the new system will force service providers to significantly upgrade their electronic security systems to a much higher level, paying particular attention to cybersecurity. The EESC expects that this will involve significant costs and modernisation of the existing IT infrastructure and might constitute an excessive burden for some service providers that might even lead to the disappearance, from some markets, of service providers that cannot afford such investments in a short period of time. Therefore, in the EESC's opinion, the Commission and Member States should search for solutions that would protect providers from discrimination in that field and allow for a "soft" landing in this regard, including by offering the possibility of ensuring compliance with the new requirements in several stages, within a reasonable period of time.

Brussels, 20 October 2021.

Christa SCHWENG
The president of the European Economic and Social Committee

_____