BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

THE EUROPEAN COMMISSION PROPOSAL AMENDING THE eIDAS REGULATION (EU) No 910/2014: A PERSONAL DATA PROTECTION PERSPECTIVE

By Alessandro Ortalda, Niko Tsakalakis, Lina Jasmontaite

Contents

1 Introduction

On 23 July 2014, Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market (hereinafter 'eIDAS Regulation') was adopted. The goal of the Regulation has been 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"[1]. In the review pursuant to Article 49 of eIDAS Regulation, the European Commission (EC) concluded that overall, the eIDAS has furthered the development of the Single Market[2]. At the same time, the EC noted that "eID under eIDAS has not achieved its potential in terms of effectiveness regarding digital identity"[3] and that there has been a slow take-up and divergent practices and approaches to eID schemes by the Member States[4]. In light of this, the EC proposed amendments to eIDAS Regulation on 3 June 2021.

The explanatory memorandum that accompanies the proposed amendments to eIDAS Regulation (hereinafter 'eIDAS Proposal') acknowledges that in its current form, the eIDAS Regulation is a poor fit to address the demands and challenges of the electronic identity landscape and market demand for electronic identity solutions. In view of this, the eIDAS Proposal seeks to foster electronic identity adoption across the European Union (EU) by introducing the mandatory notification of electronic identity schemes of Member States (previously voluntary)[5] and the European Digital Identity Wallet (hereinafter 'EDIW')[6].

The proposed amendments further the scope of electronic identity in Europe and connect with other legislative instruments, most notably to Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (hereinafter 'General Data Protection Regulation', 'GDPR') and Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. In order to

[1] European Parliament, Council of the European Union, *Regulation 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 (eIDAS)* (2014), Recital 2.
[2] European Commission, *Report to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)* (2021), p 7.
[3] European Commission, *Commission Staff Working Document. Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity* (2021).
[4] Massimo Pedroli, George O'Neill, Arianna Fravolini, Leonardo Marcon, *Overview of Member States' eID Strategies. Version 3.0* (2020), p. 79.
[5] "Member States shall notify […] at least one electronic identification scheme", European Commission, *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* (2021), Article 7.
[6] European Commission, *Proposal amending Regulation (EU) No 910/2014*, Article 6a.

ensure legal certainty and consistency, it is important to examine the interplay between the different legal regimes and identify possible issues that could be addressed during the ongoing legislative process.

The present report explores the eIDAS Proposal with the aim to identify issues that may arise from a data protection point of view. For each identified issue, the report provides an overview presenting the background, the potential impacts, and possible solutions. It also suggests points for consideration for the regulators, policymakers, and other stakeholders.

The report acknowledges that the review process is ongoing and that the eIDAS Proposal might change or additional clarification might be published at a later stage (for instance, through the publication of Implementing Acts).

The report does not aim to be exhaustive. A quick glance to the opinions issued by the European Data Protection Supervisor[7], the European Economic and Social Committee[8], and the European Committee of the Regions[9], and to the outcomes of the public consultation on the eIDAS Proposal[10] reveals that there are other aspects that need to be considered. The present report looks at the interplay between the framework related to electronic identification and the GDPR and focuses on potential issues for the rights and freedoms of individuals (thus excluding, for instance, cost/opportunity considerations for private stakeholders) that the authors believe to represent concrete but addressable issues.

The present report hopes to provide useful observations for the regulators, policymakers and the stakeholders involved in the review process and, in doing so, to support their work toward an eIDAS Proposal that will ensure the achievement of the electronic identity goals of the EU while being respectful of the rights and freedoms of individuals and fully compatible with already existing legislative instruments.

[7] See European Data Protection Supervisor, *Formal comments of the EDPS on the 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* (2021).
[8] See European Economic and Social Committee, *Opinion: A trusted and secure European e-ID. INT/951* (2021).
[9] See European Committee of the Regions, *Opinion: European Digital Identity. ECON-VII/019* (2021).
[10] See European Commission, *EU digital ID scheme for online transactions across Europe. Feedback and statistics: Proposal for a regulation*, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-EU-digital-ID-scheme-for-online-transactions-across-Europe/feedback_en?p_id=25256419.

2 Preliminary assessment

2.1 Unclear relation between eIDAS and GDPR

Background and overview of the gap or issue
The processing of personal data in the EU must adhere to its data protection framework. eIDAS Regulation Article 5(1) refers to this, pointing to Directive 95/46/EC, the main data protection instrument when the eIDAS Regulation was adopted.[11] Under eIDAS Regulation Article 12(3)(d), the Interoperability Framework[12] shall ensure compliance with the data protection framework. In fact, the eIDAS Regulation went beyond Directive 95/46/EC in requiring the facilitation of privacy by design under eIDAS Regulation Article 12(3)(c), in a sense anticipating the GDPR that replaced Directive 95/46/EC and introduced an obligation for data protection by design[13]. The recitals of the eIDAS Proposal recognise that processing for the purposes of electronic identification and trust services fall within the scope of the GDPR, for instance at Recitals 6, 10 and 21. eIDAS Proposal Article 6a(7) even implicitly defines person identification data as personal data, further strengthening the interplay between the electronic identification and data protection regimes. Despite this, references to the data protection legislation have been excluded from eIDAS Proposal Articles 5 and 12. And, although the eIDAS Proposal introduces some data minimisation and selective disclosure controls, the explicit mention to privacy by design has been deleted. These changes complicate how to fully assess the interplay the eIDAS Proposal and the GDPR.
Proposed solution or mitigation
The eIDAS Proposal should explain clearly and explicitly its relationship with the GDPR and if it is to be considered a *lex specialis* regarding the processing of person identification data, it should be made explicit which regulation takes precedence in case of conflict[14]. Although references to the GDPR in the recitals of the eIDAS Proposal are frequent, they are not in themselves legally binding. The omission of privacy by design should also be clarified. Although implementation of privacy by design controls, like selective disclosure, are welcome, an obligation to adhere to privacy by design goes further as it captures technical and organisational controls in relation to the risks and industry best practices and can have wider implications for architectural decisions[15].

Relevant provisions	
eIDAS	**GDPR**
• eIDAS Proposal Recitals 6, 10, 21 • eIDAS Proposal Articles 5, 12	N/A

[11] Its inclusion was the result of the advice of the European Data Protection Supervisor. See European Data Protection Supervisor, *Executive summary of the Opinion of the European Data Protection Supervisor on the Commission proposal for a regulation of the European Parliament and of the Council on trust and confidence in electronic transactions in the internal market (Electronic Trust Services Regulation)* (2013).

[12] The Interoperability Framework is a set of technical and organisational requirements to translate person identification data between electronic identification schemes. See Niko Tsakalakis, *Analysing the impact of the GDPR on eIDAS. Supporting effective data protection by design for cross-border electronic identification through unlinkability measures,* University of Southampton (2020), page 7.

[13] By extrapolation from Articles 12(3)(c), 5(1) 5(2), and Recital 11 'privacy by design' in eIDAS relates at the very least to data minimisation and pseudonymisation, so the terms 'data protection by design' and 'privacy by design' are seen as synonymous for the purposes of this report.

[14] E.g., by replicating the wording of Directive 2002/58/EC, clarifying its position as *lex specialis* to the GDPR. See, European Parliament, Council of the European Union, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)* (2002), Article 1(2).

[15] Such as, for instance, choosing local or cloud-based storage as per eIDAS Proposal Recital 11.

2.2 Overlap of the liability regimes of eIDAS and GDPR

Background and overview of the gap or issue	
The eIDAS Regulation includes a specific liability regime for electronic identification services in Article 11. The Member State, together with the issuer of the electronic identity (if different from the Member State), is liable for damages related to the attribution of person identification data to individuals. The same approach is taken in relation to availability of data: the Member State, together with the operator (if different from the Member State), is liable for damages related to the online availability of data. The eIDAS Proposal upholds Article 11 and adds under Article 11a additional liability of the Member State for issues related to the unique identification in cases of authentication via EDIW. Because of the lack of clarity around the relationship between the eIDAS Proposal and the GDPR (see section 2.1), it is unclear how liability will be assigned where the damage is caused by a violation of a data protection obligation. Under GDPR Article 82(4), such an infringement will result in joint responsibility of all the data controllers and data processors involved in the processing activity. In contrast, eIDAS Proposal Article 11 assigns responsibility to specific parties but does not clarify how responsibility will be assigned when multiple parties are involved.	
Proposed solution or mitigation	
The eIDAS Proposal should clarify how its liability provisions relate to data protection obligations and attribution of responsibility, especially in the case of complex national electronic identification schemes with multiple parties involved. If the intention is for eIDAS Articles 11 and 11a to work alongside GDPR Article 82(4) to assign joint responsibility, this should be made clear. This will also assist in clarifying the overall relationship with the GDPR when conflicts of norms arise (see section 2.1).	
Relevant provisions	
eIDAS	**GDPR**
• eIDAS Proposal Articles 11, 11a	• GDPR Article 82

2.3 Issues around data minimisation and selective disclosure

Background and overview of the gap or issue
The eIDAS Regulation has been criticized for its implementation of the principle of data minimisation and, specifically, for its lack of selective disclosure measures for identifiers[16]. Electronic identification under the eIDAS Regulation requires the transmission of the complete mandatory minimum data set of person identification data even when the relying party can provide services using less information. In response to the outcomes of the Impact Assessment performed by the European Commission, which acknowledges the issue[17], the eIDAS Proposal introduces the concept of selective disclosure for EDIWs. eIDAS Proposal Recital 29 specifies that EDIWs "should technically enable the selective disclosure of attributes to relying parties." This is effected by Article 6a(3)(a) in combination with the recognition of the legal effect of electronic attestation of attributes under Article 45a(2). The term 'electronic attestation of attributes' is used in the eIDAS Proposal to refer to 'attribute-based credentials'[18]. However, eIDAS Proposal Article 6a(4)(d) might render the practical implementation of selective disclosure useless. Under Article 6a(4)(d), relying parties shall authenticate the user before receiving electronic attributes. It is not clear what the effects of such an authentication should be. Note that in eIDAS Regulation Article 3(5), which has not been replaced in the eIDAS Proposal, the concept of authentication is conflated with that of electronic identification. A prior complete identification would negate any privacy benefits of the selective disclosure of attributes.
Proposed solution or mitigation
The eIDAS Proposal should clarify the meaning of Article 6a(4)(d) and that attribute attestation is possible without prior electronic identification of the person. It should also clarify how selective disclosure and electronic identification can work with pseudonyms under Article 5 (see section 2.5).

Relevant provisions	
eIDAS	**GDPR**
• eIDAS Proposal Recital 29 • eIDAS Proposal Articles 6a	• GDPR Article 5(1)(c)

[16] Niko Tsakalakis, Sophie Stalla-Bourdillon, and Kieron O'hara, *Data protection by design for cross-border electronic identification: Does the eIDAS Interoperability Framework need to be modernised?* in Eleni Kosta, Simone Fischer-Hübner, Jo Pierson, Daniel Slamanig, Stephan Krenn (eds.), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, Vienna, Austria, Springer International Publishing (2019), pp. 255–74.

[17] "It is compulsory to exchange the full minimum eIDAS data set and there is no possibility for the user to limit the transmitted personal data to the minimum required for a specific transaction", European Commission, *Commission Staff Working Document*, p.14.

[18] "Attribute Based Credentials (ABC) are a form of authentication mechanism that allows to flexibly and selectively authenticate different attributes about an entity without revealing additional information about the entity (zero-knowledge property)", PrivacyPatterns.org, https://privacypatterns.org/patterns/Attribute-based-credentials

2.4 Measures to ensure unlinkability of users

Background and overview of the gap or issue
Unlinkability refers to a privacy by design goal under which the linking of different datasets, flows or processes can violate data minimisation and purpose limitation[19] and lead to profiling the user. The eIDAS Regulation does not contain specific provisions for unlinkability. On the contrary, the requirement to provide every relying party with a unique identifier 'as persistent as possible in time' and the mandatory minimum data set make linkability easier[20]. The eIDAS Proposal takes steps to address this issue and introduces controls for unlinkability in the form of policy measures. Under Article 6a(7), the issuers of EDIWs are prohibited from monitoring where and for what purpose personal data have been used and from combining person identification data and other personal data. To reinforce such prohibition, providers of such services are required to keep the person identification data related to the provision of the EDIW physically and logically separate from any other data. Additionally, the wording of Article 6a(4)(b), which prohibits attribute service providers from knowing the recipients of the attributes, might hint at a technical control ('*cannot receive*') towards unlinkability. If service providers cannot observe where the attributes are used (unobservability of recipients)[21], they will be unable to link together that two attributes relate to each other. This is not further specified in the eIDAS Proposal. Unobservability is prescribed in the eIDAS Proposal only in relation to issuers (of EDIWs and attestations). This is not enough to prevent linkability risks across the rest of the system. Specifically, the EDIW as the intermediary between the user and the relying party is in a position to know all user actions. Policy measures for unlinkability (like the dataset separation under Article 6a(7) and 45(f)(3)) will not be effective in the event of a compromise by an attacker. If the EDIWs are compromised, a hostile actor might be able to link all uses of a user[22]. And, unless the use of persistent identifiers in relation to selective disclosure is not clarified, relying parties that have received the same unique identifier might be able to link their datasets together.
Proposed solution or mitigation
The eIDAS Proposal should clarify the policy and technical measures to engineer unlinkability. Technical unlinkability should be expanded beyond issuers to include wallet apps and relying parties, as the policy controls that the eIDAS Proposal contains will be insufficient if any of the parties is compromised by a hostile actor.
Relevant provisions

eIDAS	GDPR
• eIDAS Proposal Article 6a	• GDPR Article 5(1)(c)

[19] Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, *The Standard Data Protection Model. v 2,0b* (2020), p. 27
[20] See Tsakalakis et al, *Data Protection by Design for Cross-Border Electronic Identification*.
[21] See Andreas Pfitzmann, Marit Hansen, *Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management* (2011).
[22] Similar fears have been expressed in other variations of this 'hub-and-spoke' architecture. See Luís A. N. Brandão, Nicolas Christin, and George Danezis, *Toward Mending Two Nation-Scale Brokered Identification Systems,* Proceedings on Privacy Enhancing Technologies (2015), pp. 135–55.

2.5 Unique identifier and privacy by design

Background and overview of the gap or issue
The eIDAS Regulation specifies a mandatory minimum data set that contains a unique identifier "as persistent as possible in time"[23]. The amended wording used in eIDAS Proposal Article 12(4)(d) clarifies that the minimum data set must represent a person "uniquely and persistently". From a privacy by design point of view, this could be problematic. The mandatory inclusion of a persistent identifier increases the risks of linkability (see section 2.4). Relying parties across the EU will potentially be able to associate different datasets using the persistent identifier as an anchor. Moreover, the mandatory inclusion of a persistent unique identifier invalidates any practical use of pseudonyms under eIDAS Regulation Article 5[24]. Mandatory disclosure of the minimum data set, including a persistent unique identifier, precludes in practice the use of pseudonyms, as any pseudonym could be associated with identifying information and become a *de facto* unique identifier. In addition to that, the use of unique identifiers is specifically prohibited in certain Member States (e.g., in Germany[25] and Austria[26]). The eIDAS Regulation circumvents this issue by allowing a semi-permanent identifier ("as possible in time"), unique per receiving party, which does not seem to be the case in the eIDAS Proposal. It is questionable, therefore, how the use of the minimum data set will conform to such prohibitions.
Proposed solution or mitigation
The eIDAS Proposal must clarify the format of unique identifiers. It must also clarify under which conditions these identifiers will change (e.g., in case of expiration or theft of the electronic identification means) and how their use will be justified in jurisdictions where prohibitions exist. Most importantly, the eIDAS Proposal should justify how persistent unique identifiers address data protection by design under the GDPR, especially given the existence of electronic identification systems that offer pseudonymisation and selective disclosure. The justification must assess their appropriateness against the 'state-of-the-art', the cost of implementation and the risks to the rights of individuals as per GDPR Article 25.

Relevant provisions	
eIDAS	**GDPR**
• eIDAS Proposal Article 12	• GDPR Article 25(1)

[23] European Commission, *Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market* (2015), Annex 1(d).
[24] Niko Tsakalakis, Sophie Stalla-Bourdillon, Kieron O'Hara, *What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation*, in Detlef Hühnlein, Heiko Roßnagel, Christian H. Schunck, Maurizio Talamo (eds.), Open Identity Summit 2016: October 13–14, 2016, Rome, Italy, vol. P-264, Gesellschaft für Informatik. (2016), pp. 167-174.
[25] Under decision of the German Constitutional Court: Volkszählung Urteil des Ersten Senats vom 15 Dezember 1983 auf die mündliche Verhandlung vom 18 und 19 Oktober 1983. 65 BVerfGE 1 (1983).
[26] Where the use is not prohibited but it is strictly regulated: Bundesgesetz uber das polizeiliche Meldewesen. BGBl. I Nr. 9/1992 (1992) s 16a.

2.6 Data availability and fallback procedures in case of Digital Wallet withdrawn

Background and overview of the gap or issue	
eIDAS Proposal Article 10a introduces requirements that regulate the withdrawal of EDIWs in case of security breach. EDIWs are to be withdrawn after a suspension of three months if the security breach is not remedied, or without delay where it is justified by the severity of the breach. eIDAS Proposal Article 10a is not intended to substitute eIDAS Regulation Article 10, which deals with security breaches of electronic identification schemes and which has not been subject to any amendment in the eIDAS Proposal. Neither eIDAS Regulation Article 10 nor eIDAS Proposal Article 10a explicitly spell out if withdrawal should be interpreted as a definitive and irreversible recall. Also, the requirement for an immediate withdrawal of EDIWs introduced in the eIDAS Proposal reveals to be problematic insofar the severity of the breach necessary to activate such an obligation is not specified. In case of withdrawal without delay, it is possible to envisage situations where users will be deprived of their access right to the EDIW with no time to transfer data to another solution (through their right to data portability). This may be further aggravated when the EDIW is issued directly by the Member State as per eIDAS Proposal Article 6a(2)(b), since in such cases the number of available EDIWs might be limited as it is unlikely that Member States will create multiple EDIWs. Without access to the EDIW, users might not have any means to access their data. This would be in violation of the principle of data availability as sanctioned in GDPR Article 32.	
Proposed solution or mitigation	
The eIDAS Proposal should require EDIWs to have fallback procedures in place such as agreements between EDIW providers to migrate data without delay in case of withdrawal. Users shall be informed of these agreements when choosing an EDIW and appropriate legal bases to ensure a compliant and timely transfer be identified beforehand. The eIDAS Proposal should also consider situations where it will not be possible to migrate data to another EDIW, such as in cases where only one EDIW is available in the Member State where the security breach occurs. Extra-territorial fallback procedures in the form of Member States agreements should be considered.	
Relevant provisions	
eIDAS	**GDPR**
• eIDAS Proposal Article 10a	• GDPR Article 32

2.7 Synergies between security breach notification obligations

Background and overview of the gap or issue
The proposed amendments introduce notification of a security breach of the EDIW. According to the eIDAS Proposal "where European Digital Wallets issued pursuant to Article 6a and the validation mechanisms referred to in Article 6a(5) points (a), (b) and (c) are breached or partly compromised in a manner that affects their reliability or the reliability of the other European Digital Identity Wallets, the issuing Member State shall, without delay, suspend the issuance and revoke the validity of the European Digital Identity Wallet and inform the other Member States and the Commission accordingly." Once the security breach is addressed, the issuing Member State shall re-establish the issuance and the use of the European Digital Identity Wallet and inform other Member States and the Commission without undue delay. The same provision also provides a possibility of withdrawing the EDIW without delay, "where justified by the severity of the breach" and sets the time limit of three months for "the breach or compromise" to be addressed. This provision creates a parallel framework for notifications of security breaches in addition to the one provided in Article 10 of the eIDAS Regulation. The set-up of the notification mechanism is essentially similar and added value of the duplication should be considered. eIDAS Proposal Article 10a includes concepts such as, "partly compromised" and "the severity of the breach", which entail subjective judgment and on a practical level may lead to a fragmentated implementation of the provision. Despite the fact that "partly compromised" is used in Article 10 of eIDAS Regulation, the use of this term is inconsistent with other provisions of eIDAS Regulation and other legal frameworks, namely the GDPR and the NIS Directive. The proposed amendments do not provide the criteria to determine the severity of the breach. The time limit of three months to address the breach of security provides structure and a clear timeline for the revocation and withdrawal process. At the same time, it awards the providers of EDIWs with flexibility as to when to address the detected flaws in security, which may undermine the interests and rights of users. The provision has to be worded in a way that providers of EDIWs would be incentivised to address and to contain security breaches immediately.
Proposed solution or mitigation
The proposal should clarify that notifications of security breaches of EDIWs by Member States should operate in tandem with the requirement for qualified and non-qualified trust service providers to notify the relevant competent authorities without undue delay provided in Article 19(2) of the eIDAS Regulation. Criteria should be established to determine the severity of the breach that would be coherent with the co-existing legislative measures, namely the GDPR and the NIS Directive. The Commission implementing acts intend to specify the proposed Article 10a. However, the proposed provision should clarify whether such assessment should be done under NIS Directive, which focuses on societal and economic activities, or under the GDPR, which focuses on rights of individuals. Furthermore, the proposed amendments should clarify that in cases where a security breach of the EDIW qualifies as a personal data breach under Article 4(12) of the GDPR, the providers of trusted services must evaluate and document risks arising from the breach and notify the competent data protection authority and individuals.

Relevant provisions	
eIDAS proposal	**GDPR**
• eIDAS Proposal Article 10a	• GDPR Article 33(1) • GDPR Article 34(1)

2.8 Synergies between data security obligations

Background and overview of the gap or issue	
The eIDAS Proposal suggests amending eIDAS Regulation Article 20 with the following text: "Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. the audit shall confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation and in Article 18 of Directive (EU) XXXX/XXXX [NIS2]. " The provision assumes that audits will confirm that the qualified trust service providers and the qualified trust services provided by them adhere to the requirements listed in eIDAS Regulation and NIS2. Provided the explicit reference to data protection framework in the proposed amendment to paragraph 2 of the same provision, the conformity assessment should also consider whether the requirements stemming from the Article 32(1) of GDPR are fulfilled.	
Proposed solution or mitigation	
In order to address the abovementioned points, the proposed provision could be amended as follows "the audit shall analyse whether the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation, in Article 18 of Directive (EU) XXXX/XXXX [NIS2] and in Article 32.1 of Regulation (EU) 2016/679".	
Relevant provisions	
eIDAS	**GDPR**
• eIDAS proposal Articles 20(1), 20(2)	• GDPR Article 32(1)

2.9 Fostering cooperation of competent authorities

Background and overview of the gap or issue	
The proposal suggests replacing Article 20(2) last sentence by the following: "Where personal data protection rules appear to have been breached, the supervisory body shall inform the supervisory authorities under Regulation (EU) 2016/679 of the results of its audits." Encouraging cooperation and fostering information sharing between and among different national authorities concerned is crucial to improve cyber resilience. At the same time, the duties of competent authorities should be clearly defined. This provision implies that the supervisory body reviewing the conformity assessment report (that is due every 24 months) is in a position to judge whether the qualified trust service providers and the qualified trust services provided by them are in compliance with the GDPR. Such authorities may lack capacity to make such a judgment.	
Proposed solution or mitigation	
It should be clarified that in cases "where there is any reason to believe that data protection rules could have been breached", the competent data protection authority (i.e., the supervisory authorities under Regulation (EU) 2016/679) should be informed. In cases, where personal data breaches are detected during the review of conformity assessment reports, the competent authorities should inform the controllers (i.e., qualified trusted service providers) and then they should notify the competent data protection authority of a personal data breach according to Article 33(1).	
Relevant provisions	
eIDAS	**GDPR**
• eIDAS proposal Article 20.2	• GDPR Article 33.1

2.10 Issues concerning the protection of vulnerable individuals

Background and overview of the gap or issue	
In general, the eIDAS Proposal tends toward a user-centric approach and, as stated at Recital 2, to put individuals (and legal entities) in charge of their online identity and data. In light of this approach, it also addresses the accessibility needs of persons with disabilities in Article 15. However, this approach seems to ignore elements related to the digital literacy of European citizens that might introduce discrimination in the implementation of electronic identity in the Union. The last Digital Economy and Social Index, published by the European Commission in November 2021, reveals that many European citizens only have basic digital literacy[27]. Promoting digital literacy or eliminating social barriers for vulnerable people is not in the mandate of the eIDAS Regulation or eIDAS Proposal. However, the risks around it may effectively hinder the creation of a European electronic identity space.	
Proposed solution or mitigation	
The eIDAS Proposal should address this risk by requiring Member States to introduce specific measures to protect individuals from discrimination arising from a lack of digital literacy or a lack of access to the digital infrastructure. For instance, Member States might create entities and organisations (or give mandate to existing ones) to act as intermediaries and support these vulnerable groups of people in using EDIW to access services (e.g., local NGOs visiting houses of vulnerable people on-demand to support or to bring necessary equipment or connectivity). Also, Member States should always ensure a way to access services that does not require EDIW or any other technological means that might create an entry barrier.	
Relevant provisions	
eIDAS	**GDPR**
N/A	N/A

[27] See European Commission, *The Digital Economy and Society Index 2021*.

3 Conclusions

As this brief report demonstrates, some of the changes introduced by the eIDAS Proposal seems to be conscious of the data protection rights of individuals and aims to safeguard them. In particular, the eIDAS Proposal improves on the eIDAS Regulation by taking steps towards a user-centric approach aimed at ensuring users are in control of their data. At the same time, some of the changes reveal the possibility that compliance issues might materialise if the draft of the eIDAS Proposal is not amended. For instance, the eIDAS Proposal lacks clarity on how to make its data protection-friendly and user-centric approach coherent with some other provisions that appear to be problematic from a data protection standpoint (like, for instance, those related to the minimum dataset).

In general, the identified potential issues do not present a critical profile. None of the potential issues seem to pose a high risk of incompatibility between the European legal regime on electronic identification and the European legal regime on data protection provided by the GDPR. Nevertheless, these should be addressed to ensure consistency across all the frameworks. The authors believe that all the potential issues analysed in the report can be addressed through specific and tailored amendments, or by adding further clarifications either in the text of the eIDAS Proposal or subsequent instruments such as Implementing Regulations.

The eIDAS Proposal is not only a welcomed addition that may further strengthen the legal regime on electronic identification in Europe; it is also an opportunity to bring more clarity across different legal frameworks involving digital means and, in doing so, help the European Union to promote the use of such means.

4 References

Brandão, Luís A. N., Nicolas Christin, and George Danezis, *Toward Mending Two Nation-Scale Brokered Identification Systems,* Proceedings on Privacy Enhancing Technologies (2015), pp. 135–55.

Bundesgesetz uber das polizeiliche Meldewesen. BGBl. I Nr. 9/1992 (1992).

Conference of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, *The Standard Data Protection Model. v 2,0b* (2020).

European Commission, *Commission Staff Working Document. Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) n° 910/2014 as regards establishing a framework for a European Digital Identity* (2021).

European Commission, *EU digital ID scheme for online transactions across Europe. Feedback and statistics: Proposal for a regulation*, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12528-EU-digital-ID-scheme-for-online-transactions-across-Europe/feedback_en?p_id=25256419.

European Commission, *Implementing Regulation (EU) 2015/1501 of 8 September 2015 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market* (2015).

European Commission, *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* (2021).

European Commission, *Report to the European Parliament and the Council on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)* (2021).

European Committee of the Regions, *Opinion: European Digital Identity. ECON-VII/019*, 2021.

European Data Protection Supervisor, *Executive summary of the Opinion of the European Data Protection Supervisor on the Commission proposal for a regulation of the European Parliament and of the Council on trust and confidence in electronic transactions in the internal market (Electronic Trust Services Regulation)* (2013).

European Data Protection Supervisor, *Formal comments of the EDPS on the 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* (2021).

European Economic and Social Committee, *Opinion: A trusted and secure European e-ID. INT/951*, (2021).

European Parliament and Council of the European Union, *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)* (2002).

European Parliament, Council of the European Union, *Regulation 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 (eIDAS)* (2014).

Pedroli, Massimo, George O'Neill, Arianna Fravolini, Leonardo Marcon, *Overview of Member States' eID Strategies. Version 3.0* (2020).

Pfitzmann, Andreas, Marit Hansen, *Terminology for Talking about Privacy by Data Minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management* (2011).

PrivacyPatterns.org, https://privacypatterns.org/patterns/Attribute-based-credentials.

Tsakalakis, Niko, *Analysing the impact of the GDPR on eIDAS. Supporting effective data protection by design for cross-border electronic identification through unlinkability measures,* University of Southampton (2020).

Tsakalakis, Niko, Sophie Stalla-Bourdillon, and Kieron O'hara, *Data protection by design for cross-border electronic identification: Does the eIDAS Interoperability Framework need to be modernised?* in Eleni Kosta, Simone Fischer-Hübner, Jo Pierson, Daniel Slamanig, Stephan Krenn (eds.), *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, Vienna, Austria, Springer International Publishing (2019), pp. 255–74.

Tsakalakis, Niko, Sophie Stalla-Bourdillon, Kieron O'Hara, *What's in a name: the conflicting views of pseudonymisation under eIDAS and the General Data Protection Regulation*, in Detlef Hühnlein, Heiko Roßnagel, Christian H. Schunck, Maurizio Talamo (eds.), Open Identity Summit 2016: October 13–14, 2016, Rome, Italy, vol. P-264, Gesellschaft für Informatik. (2016), pp. 167-174.

Volkszählung Urteil des Ersten Senats vom 15 Dezember 1983 auf die mündliche Verhandlung vom 18 und 19 Oktober 1983. 65 BVerfGE 1 (1983).