Suggestions for Amendments to the eIDAS Reform

Safeguards to increase privacy and user-trust

Introduction

This collection of suggested amendments tries to remedy some of the problems identified[1] in the Commission's proposal for a Reform of the eIDAS Regulation.

1 https://epicenter.works/document/3865

Safeguard against Observability of User Behavior

Article 6a – paragraph 7

Text proposed by the Commission	*Amendment*
The user shall be in full control of the European Digital Identity Wallet. The issuer of the European Digital Identity Wallet ***shall not*** collect information about the use of the wallet ***which are not necessary for the provision of the wallet services, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it***. Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held. If the European Digital Identity Wallet is provided by private parties in accordance to paragraph 1 (b) and (c), the provisions of article 45f paragraph 4 shall apply mutatis mutandis.	The user shall be in full control of the European Digital Identity Wallet ***and their data***. The ***technical architecture shall make it impossible for the*** issuer of the European Digital Identity Wallet ***or third-party services connected to them or the Member State to*** collect ***or obtain*** information about the use of the wallet ***by the user. The exchange of information via the European Digital Identity Wallet shall not allow to providers of electronic attestation of attributes to track, link, correlate or otherwise obtain knowledge of transactions or user behavior.*** Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held. If the European Digital Identity Wallet is provided by private parties in accordance to paragraph 1 (b) and (c), the provisions of article 45f paragraph 4 shall apply mutatis mutandis.

Justification

The European Digital Identity Wallet aspires to become the general purpose infrastructure for our digital lives. User transactions will reveal information about the medical situation, travel history, consumption patterns and social interactions of citizens. Only an architecture that protects this data about a wide-range of online and offline user behavior from centralised surveillance is an electronic identity system deserving of citizens trust and a worthy European answer to competing systems from China or the USA.

Article 6a – paragraph 4 – point f

Text proposed by the Commission	*Amendment*
[inserted]	***Make it impossible for the issuer of the European Digital Identity Wallet or third-party services connected to them or the Member State to receive any information about the use of the European Digital Identity Wallet;***

Justification

The European Digital Identity Wallet aspires to become the general purpose infrastructure for daily digital interactions. User transactions will reveal large amounts of data, including data of highly personal nature, such as information of the individuals economic situation or information about the medical situation, travel history, consumption patterns and social interactions of citizens. Therefore, an architecture that protects this data about a wide-range of online and offline user behavior from centralised surveillance is an electronic identity system deserving of citizens trust and a worthy European answer to competing systems from China or the USA.

Article 6a – paragraph 4 – point b

Text proposed by the Commission	*Amendment*
ensure that ***trust service*** providers of qualified attestations of attributes cannot receive any information about the use of these attributes;	ensure that providers of qualified ***and non-qualified*** attestations of attributes cannot receive any information about the use of these attributes;

Justification

This amendments extends the safeguards to protect user behavior from being tacked. Examples of providers of non-qualified attribute attestation are private companies, membership clubs or universities. With this change in the text an existing technical safeguard of the European Digital Identity Wallet is simply extended to more stakeholders. Without this amendment it would, for example, be possible for a university to keep track of all the places a person showed their diploma (potential future employers, other universities, government entities, etc.) or the issuer of a Covid-19 Vaccination or Recovery Certificate to track every time a certificate is verified by a border crossing[2], restaurant or theater[3].

2 This protection against tracking is the current standard in Regulation (EU) 2021/953 Article 4 (2)

3 For an example of this protection against tracking the verification of Covid-19 certificates in domestic use cases, see § 4f of the Austrian Epidemiegesetz(https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=10010265)

Safeguard against unique, live-long tracking

Article 11a

Text proposed by the Commission	*Amendment*
Unique Identification 1. When notified electronic identification means and the European Digital Identity Wallets are used for authentication, Member States shall ensure unique identification. 2. Member States shall, for the purposes of this Regulation, include in the minimum set of person identification data referred to in Article 12.4.(d), a unique and persistent identifier in conformity with Union law, to identify the user upon their request in those cases where identification of the user is required by law. 3. Within 6 months of the entering into force of this Regulation, the Commission shall further specify the measures referred to in paragraph 1 and 2 by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(10).	***[Delete]***

Justification

A unique, persistent identifier for natural persons would in some Member Countries (e.g., Netherlands, Germany) be illegal or even unconstitutional[4]. Such an identifier poses a severe risk for tracking individuals and combining their information across government sectors contrary to established eGovernment practice[5].The risk of a unique, live-long identifier cannot be deemed the least intrusive method for the purpose of uniquely identifying an individual. Article 11a is also not needed as the existing interoperability framework of identification schemes according to the original Article 12 (4) (d) already entails a unique representation of an individual for cross-border cases.

4 In Germany, the use of unique persistent identifiers is prohibited under the census ruling of 1983. 65 BVerfGE 1 (1983)

5 https://www.bmdw.gv.at/Ministerium/DasBMDW/Stammzahlenregisterbehoerde/Bereichsspezifische_Personenkennzeichen.html

Article 6a – paragraph 4 – point e

Text proposed by the Commission	*Amendment*
ensure that the person identification data referred to in Articles 12(4), point (d) **uniquely *and persistently*** represent the natural or legal person is associated with it.	ensure that the person identification data referred to in Articles 12(4), point (d) represent the natural or legal person is associated with it.

Justification

The use of the European Digital Identity Wallet should further the protection granted to individuals' personal data protection and privacy. To this end, the amendment seeks to protects citizens against easily tracking them every time they use the Wallet online and offline or associating their interactions between different relying parties. This proposal follows established practices in Austria[6] and the Netherlands[7] also known in the standards community as "Pairwise Pseudonymous Identifiers[8]. The need for unlinkability and non-traceability was acknowledged by the eIDAS Expert Group.[9]

Article 12 – paragraph 4 – point d

Text proposed by the Commission	*Amendment*
a reference to a minimum set of person identification data necessary to uniquely ***and persistently represent*** a natural or legal person;	a reference to a minimum set of person identification data uniquely ***representing*** a natural or legal person***, which is available from electronic identification schemes;***

Justification

Reverting to the 2014 version of the eIDAS Regulation. The Commission proposal would require a unique and persistent identification independent from a particular electronic identification scheme. In effect, this seemingly technical change of the interoperability framework would have the same affect as Article 11a.

6 https://pure.tugraz.at/ws/portalfiles/portal/26511346/20191001_Japanese_Delegation.pdf
7 https://www.cs.ru.nl/E.Verheul/papers/eID2.0/eID%20PEP%201.29.pdf
8 https://pages.nist.gov/800-63-3/sp800-63c.html#ppi
9 See chapter 5 of the final Outline from February 17th 2022: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=37639&fromExpertGroups=true

Article 12 – paragraph 6 – point a

Text proposed by the Commission	*Amendment*
the exchange of information, experience and good practice as regards electronic identification schemes and in particular technical requirements related to interoperability***, unique identification*** and assurance levels;';	the exchange of information, experience and good practice as regards electronic identification schemes and in particular technical requirements related to interoperability and assurance levels;

Justification

Reverting to the 2014 version of the eIDAS Regulation. The Commission proposal would require a unique and persistent identification independent from a particular electronic identification scheme. In effect, this seemingly technical change of the interoperability framework would have the same affect as Article 11a.

Anti-Discrimination Provision

Article 6a – paragraph 6

Text proposed by the Commission	*Amendment*
The European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance 'high'. The use of the European Digital Identity Wallets shall be free of charge to natural persons.	The European Digital Identity Wallets shall be issued under a notified electronic identification scheme of level of assurance 'high'. The use of the European Digital Identity Wallets shall be free of charge to natural persons. ***Access to government or other essential services, the labour market and freedom obtain goods and services shall not be restricted or hindered for natural persons not using the European Digital Identity Wallet.***

Justification

A whole generation of citizens is not equipped with the digital literacy to use the European Digital Identity Wallet safely. A significant part of the population either has no Smartphone or one that is so old that it no longer receives security updates from the vendor and therefore cannot run the Wallet Application safely. Seniors are currently protesting on mass in Spain because digital systems used there are in effect excluding the older generation from the banking systems.[10] Forcing people to use digital technology they don't understand or for which they don't own the hardware to operate it safely is either surrendering them to identity theft or excluding them from society completely. Obtaining government services in the city of Vienna, Austria costs more for residents not using the electronic identity system.[11] In order not to further marginalise already disenfranchised parts of the electorate, this regulation needs to ensure the use of the European Digital Identity Wallet remains voluntary until we have closed the digital divide.

10 https://www.cbc.ca/news/world/spanish-retiree-campaign-in-person-banking-1.6344171
11 https://www.wien.gv.at/english/e-government/transportation/parking/residents/parking-permit.html

Article 45a

Text proposed by the Commission	*Amendment*
1. An electronic attestation of attributes shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.	1. An electronic attestation of attributes shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form ***or that it does not meet the requirements for qualified electronic attestations of attributes***.
2. A qualified electronic attestation of attributes shall have the same legal effect as lawfully issued attestations in paper form.	2. A qualified electronic attestation of attributes shall have the same legal effect as lawfully issued attestations in paper form.
3. A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified electronic attestation of attributes in any other Member State.	3. A qualified electronic attestation of attributes issued in one Member State shall be recognised as a qualified electronic attestation of attributes in any other Member State.
	4. Lawfully issued attestations in paper form shall be accepted by relying parties as an alternative to electronic attestation of attributes.

Justification

This amendment ensures that relying parties offer analog procedures for users not able or choosing not to use the European Digital Identity Wallet and that attributes are not inadmissible simply because they are non-qualified. Changes in paragraph 1 reflect suggestions from the French Presidency from March 10th 2022.

Ensuring Selective Disclosures of Attributes

Article 6a – paragraph 4 – point b

Text proposed by the Commission	*Amendment*
provide a mechanism to ensure that the relying party is able to authenticate the user ***and*** to receive electronic attestations of attributes;	provide a mechanism to ensure that the relying party is able to authenticate the user ***or*** to receive electronic attestations of attributes ***in the form of selective disclosures that are unlinkable to the user and minimise the processing of personal data***. ***Where attestations of attributes are adequate for the purposes of the relying party, no prior electronic authentication or identification shall take place;***

Justification

With regard to the goal of the regulation to put users in control about what they share with relying parties and in light of Recital 29, the attestation of attributes should not include a mandatory identification of the user. The authentication of the user is equated in Article 3(5) with the identification of the user. It should be clear to the user that, for example, verification of age does not allow relying parties to gather excessive information which could be used to track the user on subsequent interactions.

Regulation of Relying Parties & Use-cases

Article 6b

Text proposed by the Commission	*Amendment*
1. Where relying parties intend to rely upon European Digital Identity Wallets issued in accordance with this Regulation, they shall ***communicate it to*** the Member State where the relying party is established to ensure compliance with requirements set out in Union law or national law for the provision of specific services. ***When communicating their intention to rely on European Digital Identity wallets, they shall also inform about the intended use of the European Digital Identity Wallet.***	1. Where relying parties intend to rely upon European Digital Identity Wallets issued in accordance with this Regulation, they shall ***request approval from*** the Member State where the relying party is established to ensure compliance ***of their intended use and the information they intend to request*** with requirements set out in Union law or national law for the provision of specific services. ***Member States shall scrutinize requested use cases of the European Digital Identity proportionate to the potential privacy implications of the data exchanged and the purpose of the processing of personal information, thereby distinguishing between:*** ***(a) anonymous use for selective disclosures*** ***(b) pseudonym use for authentication*** ***(c) unique identification use*** ***(d) attribute attestation of special categories of personal data in accordance with Article 9 of Regulation (EU) 2016/679;***
2. Member States shall implement a common mechanism for the authentication of relying parties	2. Member States shall implement a common mechanism for the authentication ***and unique identification*** of relying parties***. Member states may revoke the authorization of relying parties in case of illegal or fraudulent use of the European Digital Identity Wallet in their country.***
3. Relying parties shall be responsible for carrying out the procedure for authenticating person identification data and electronic attestation of attributes originating from European Digital Identity Wallets.	3. Relying parties shall be responsible for ***communicating their unique identifier in every interaction with the European Digital Identity Wallet and*** carrying out the procedure for authenticating person identification data and electronic attestation of attributes originating
4. Within 6 months of the entering into force of this Regulation, the Commission shall establish technical and operational specifications for the requirements referred to in paragraphs 1 and 2 by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(10).	

from European Digital Identity Wallets.
4. Within 6 months of the entering into force of this Regulation, the Commission shall establish technical and operational specifications for the requirements referred to in paragraphs 1 and 2 by means of an implementing act on the implementation of the European Digital Identity Wallets as referred to in Article 6a(10).

Justification

This proposal is in line with the Compromise Text form the French Presidency from March 10th 2022.
The European Digital Identity Wallet should offer a trusted environment free of fraudulent or excessive request for personal information. To ensure the compliance of relying parties, their participations can't be left to the one-sided communication of intend to the eIDAS authority in their country of origin. We have seen in the devastating GDPR enforcement that this leads to year-long court battles and a loss of trust in the protection of personal information. For a trusted environment in which identity information with the highest degree of certainty can be shared responsibly by all citizens the Regulation needs to define a clear and effective authorization procedure for relying parties. Trust in this new system depends on the possibility to revoke the authorization of relying parties that have acted illegally or fraudulent. All member states need the possibility to protect their citizens from such actors.
Relying parties need to be uniquely identified when requesting personal information from the user via the European Digital Identity Wallet. The need for the identification of relying parties was acknowledged by the eIDAS Expert Group that's currently developing the Toolbox[12].

Article 6a – paragraph 4 – point a

Text proposed by the Commission	*Amendment*
	(5) for relying parties to be uniquely identified and limited to request information based on their approval of a Member State in accordance with Article 6b(1);

Justification

This proposal is in line with the Compromise Text form the French Presidency from March 10th 2022.
The Common Interface has to include this safeguard to prevent unapproved or unidentified relying parties to request information exceeding their use case. The eIDAS expert group acknowledged the need of "sharing policies" that restrict what information a relying party can ask from the user and prevent excessive information requests.[13] This is such an essential safeguard that it should not be left to a non-binding technical standard which can change at any time.

Recital 28

Text proposed by the Commission	*Amendment*

12 See chapter 4.4, 4.4.2 and 4.6.1 of the final Outline from February 17th 2022: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=37639&fromExpertGroups=true

13 See chapter 4.6.1 and footnote 22 of the final Outline from February 17th 2022: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=37639&fromExpertGroups=true

Wide availability and usability of the European Digital Identity Wallets require their acceptance by private service providers. Private relying parties ***providing services in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications should accept the*** use of European Digital Identity Wallets for the provision of services where strong user authentication for online identification is required by national or Union law ***or by contractual obligation***. Where very large online platforms as defined in Article 25.1. of Regulation [reference DSA Regulation] require users to authenticate to access online services, those platforms should be mandated to accept the use of European Digital Identity Wallets upon voluntary request of the user. Users should be under no obligation to use the wallet to access private services, but if they wish to do so, large online platforms should accept the European Digital Identity Wallet for this purpose while respecting the principle of data minimisation. Given the importance of very large online platforms, due to their reach, in particular as expressed in number of recipients of the service and economic transactions this is necessary to increase the protection of users from fraud and secure a high level of data protection. Self-regulatory codes of conduct at Union level ('codes of conduct') should be developed in order to contribute to wide availability and usability of electronic identification means including European Digital Identity Wallets within the scope of this Regulation. The codes of conduct should facilitate wide acceptance of electronic identification means including European Digital Identity Wallets by those service providers which do not qualify as very large platforms and which rely on third party electronic identification services for user authentication. They should be developed within 12 months of the adoption of this Regulation. The Commission should assess the effectiveness of these provisions for the

Wide availability and usability of the European Digital Identity Wallets require their acceptance by ***citizens as a trusted means of sharing their personal data with*** private service providers. Private relying parties ***should be required to provide a data protection impact assessment according to Article 35 of Regulation 2016/679 to the Member State they seek approval by the relevant national supervisory authority from of their*** use of European Digital Identity Wallets for the provision of services where strong user authentication for online identification is required by national or Union law. ***The information requested from the user via the European Digital Identity Wallet has to be necessary and proportionate for the intended use case of the relying party and follow the principle of data minimisation.*** Where very large online platforms as defined in Article 25.1. of Regulation [reference DSA Regulation] require users to authenticate to access online services, those platforms should be mandated to accept the use of European Digital Identity Wallets upon voluntary request of the user. Users should be under no obligation to use the wallet to access private services, but if they wish to do so, large online platforms should accept the European Digital Identity Wallet for this purpose while respecting the principle of data minimisation. Given the importance of very large online platforms, due to their reach, in particular as expressed in number of recipients of the service and economic transactions this is necessary to increase the protection of users from fraud and secure a high level of data protection. Self-regulatory codes of conduct at Union level ('codes of conduct') should be developed in order to contribute to wide availability and usability of electronic identification means including European Digital Identity Wallets within the scope of this Regulation. The codes of conduct should facilitate wide acceptance of electronic identification means including European Digital Identity Wallets by those service providers which do not qualify as very large platforms and which

availability and usability for the user of the European Digital Identity Wallets after 18 months of their deployment and revise the provisions to ensure their acceptance ***by means of delegated acts in the light of this assessment***.	rely on third party electronic identification services for user authentication. They should be developed within 12 months of the adoption of this Regulation. The Commission should assess the effectiveness of these provisions for the availability and usability for the user of the European Digital Identity Wallets after 18 months of their deployment and revise the provisions to ensure their acceptance.

Justification

To ensure a trusted environment for citizens using the European Digital Identity Wallet with private companies, those companies shall be obliged to provide a data protection impact assessment to evaluate the risk of this new technology. To avoid abuses of the European Digital Identity Wallet the requirement for strong user authentication should be limited to cases on a legal basis and not extend to the fulfillment of simple contractual obligation. Evaluation of the Code of Conduct should not automatically lead to a delegated act, potentially limiting SMEs.

Prevent over-identification and protect SMEs from requiring the Wallet

Article 12b – paragraph 2

Text proposed by the Commission	*Amendment*
Where private relying parties providing services are required by national or Union law, to use strong user authentication ***for online identification, or where strong user authentication is required by contractual obligation***, including in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, private relying parties shall also accept the use of European Digital Identity Wallets issued in accordance with Article 6a.	Where private relying parties providing services are required by national or Union law, to use strong user authentication for online identification, including in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications, private relying parties shall also accept the use of European Digital Identity Wallets issued in accordance with Article 6a.

Justification

The burden to use the European Digital Identity Wallet in all cases of contractual obligation would put many SMEs in Europe in an impossible situation as they often lack the technical circumstances to integrate the European system safely and privacy-respecting in their Customer Relationship Systems.
To avoid abuses of the European Digital Identity Wallet the requirement for strong user authentication should be limited to cases on a legal basis and not extend to the fulfillment of simple contractual obligation.

Biometrics and Cloud Storage

Recital 11

Text proposed by the Commission	*Amendment*
European Digital Identity Wallets should ensure the highest level of security for the personal data used for authentication irrespective of whether such data is stored locally or on cloud-based solutions, taking into account the different levels of risk. Using biometrics to authenticate ***is one of the identifications methods providing a high level of confidence, in particular when used in combination with other elements of authentication***. Since biometrics represents a unique characteristic of a person, the use of biometrics requires organisational and security measures, commensurate to the risk that such processing may entail to the rights and freedoms of natural persons and in accordance with Regulation 2016/679.	European Digital Identity Wallets should ensure the highest level of security for the personal data used for authentication irrespective of whether such data is stored locally or on cloud-based solutions, taking into account the different levels of risk. Using biometrics to authenticate ***shall not be a precondition for using the European Digital Identity Wallet, notwithstanding the requirement for strong user authentication***. ***Biometric data for the purpose of uniquely identifying a natural person in the context of this Regulation should not be stored in the cloud.*** Since biometrics represents a unique characteristic of a person, the use of biometrics requires organisational and security measures, commensurate to the risk that such processing may entail to the rights and freedoms of natural persons and in accordance with Regulation 2016/679. ***Storing information from the European Digital Identity Wallet in the cloud has to be an optional feature only active after the user has given explicit consent. Member States should offer at least one European Digital Identity Wallet that stores cryptographic material and handles transactions on the user device without requiring cloud services. Where the European Digital Identity Wallet is provided on the Smartphone of the user its cryptographic material should be stored in the secure elements of the device.***

Justification

Not all smartphones and smart devices are equipped with biometric authentication functionality. Furthermore, privacy risk entailed in such technology, requiring biometrics would exclude large parts of the population. Strong user authentication can also be achieved by a two-factor authentication. Most devices using biometrics for authentication do not store this information outside of the secure elements of the device. This Recital seems to suggest a scenario in which biometric information is stored in the cloud, which would amplify security risks associated with the envisioned applications. Contrary to other means of authentication, biometrics are life-long unique characteristics and their loss poses a severe risk for individuals (you can change your passwords, but you can't change your face or fingerprints).
To put users in control about their data in the European Digital Identity Wallets the envisioned system should not depend on a cloud-based infrastructure. Member states should at least offer one European Digital Identity Wallet on a smartphone or desktop device. When on a Smartphone the secure elements that Recital 21 open's up for this system has to be used to increase resilience against security threats.

Relationship to the GDPR

Article 5

Text proposed by the Commission	*Amendment*
Pseudonyms in electronic transaction	***Personal data protection and p***seudonyms in electronic transaction
Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.';	***1. Processing of personal data shall be carried out in accordance with Regulation (EU) 2016/679, in particular by implementing the principles of data minimisation, purpose limitation, and data protection by design and by default;*** ***2.*** Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.';

Justification

Restore references to the relationship between eIDAS and the European Data Protection Legislation back to the existing 2014 level of protections. The original eIDAS Regulation offered a higher standard of data protection than afforded by Directive 95/46/EC by mandating the facilitation of privacy by design in Article 12(3)(c). Now the tables have turned – data protection by design is law under the GDPR, but the new eIDAS no longer references it.

Article 6a – paragraph 7

Text proposed by the Commission	*Amendment*
The user shall be in full control of the European Digital Identity Wallet. The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it. Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held. If the European Digital Identity Wallet is provided by private parties in	The user shall be in full control of the European Digital Identity Wallet. The issuer of the European Digital Identity Wallet shall not collect information about the use of the wallet which are not necessary for the provision of the wallet services, nor shall it combine person identification data and any other personal data stored or relating to the use of the European Digital Identity Wallet with personal data from any other services offered by this issuer or from third-party services which are not necessary for the provision of the wallet services, unless the user has expressly requested it. Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held. If the European Digital Identity Wallet is provided by private parties in

accordance to paragraph 1 (b) and (c), the provisions of article 45f paragraph 4 shall apply mutatis mutandis.	accordance to paragraph 1 (b) and (c), the provisions of article 45f paragraph 4 shall apply mutatis mutandis. ***The issuer of the European Digital Identity Wallet is the controller according to Regulation (EU) 2016/679 regarding the processing of personal data in the European Digital Identity Wallet.***

Justification

The legislator could take the opportunity to clarify and assign roles and obligations of the parties concerned in the eIDAS regulationIn case of the European Digital Identity Wallet. The issuer is the controller as it determines the means of processing of personal data by determining the concrete system, i.e. the means of processing, irrespective whether that system is executed on a device under their control (see C-40/17 and C-25/17).

Article 12 – paragraph 3

Text proposed by the Commission	*Amendment*
-	***(c) it facilitates the implementation of the principle of data protection by design; and***
	(d) it ensures that personal data is processed in accordance with Regulation (EU) 2016/679

Justification

Restore references to the relationship between eIDAS and the European Data Protection Framework and reinstate the requirement for privacy by design back to the existing 2014 level of protections.

Article 20 – paragraph 2

Text proposed by the Commission	*Amendment*
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.	Where personal data protection rules appear to have been breached, the supervisory body shall inform the supervisory authorities under Regulation (EU) 2016/679 ***and the issuer of the European Digital Identity Wallet*** of the results of its audits.

Justification

According to Article 33 and 34 of the GDPR the controller has certain duties in case of a data breach. To fulfill these duties, they should be informed about a potential data breach in their system.

Article 24 – paragraph 2 – point j

Text proposed by the Commission	*Amendment*
-	***ensure lawful processing of personal data in***

accordance with Regulation (EU) 2016/679;

Justification

Restore references to the relationship between eIDAS and the European Data Protection Framework.

Right for Pseudonymity

Article 5

Text proposed by the Commission	*Amendment*
Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited.';	Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall not be prohibited***, and the use of pseudonyms shall always be an option in place of a unique identifier' or when authenticating with private relying parties***.

Justification

The use of pseudonyms is an important way for marginalized groups to exercise their right for freedom of expression safely and without the risk of harassment. To protect the privacy of individuals and not deter the privacy standard for users of the European Digital Identity Wallet, the use of pseudonyms has to be an option in all cases where full identification is not legally mandated.

Qualified Web Authentication Certificates

Article 45

Text proposed by the Commission	*Amendment*
Requirements for qualified certificates for website authentication 1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV. Qualified certificates for website authentication shall be deemed compliant with the requirements laid down in Annex IV where they meet the standards referred to in paragraph 3. 2. Qualified certificates for website authentication referred to in paragraph 1 shall be recognised by web-browsers. For those purposes web-browsers shall ensure that the identity data provided using any of the methods is displayed in a user friendly manner. Web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1, with the exception of enterprises, considered to be microenterprises and small enterprises in accordance with Commission Recommendation 2003/361/EC in the first 5 years of operating as providers of web-browsing services. 3. Within 12 months of the entering into force of this Regulation, the Commission shall, by means of implementing acts, provide the specifications and reference numbers of standards for qualified certificates for website authentication referred to in paragraph 1. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).'	***[Delete]***

Justification

Inclusion of country certificates in the list of trusted Root Certificate Authorities of Web Browsers creates an enormous risk for user safety and trust. It also undermines the security architecture of the web and opens the door for other state actors intent on including their certificates in the list of Root Certificate Authorities for the purpose of surveillance and interception of online traffic. This Article contradicts the underlying objective of the proposed eIDAS reform to ensure trustworthy digital environment, and therefore, should be deleted.

Protect the European Digital Identity Wallet from interception of transactions via proxies

Article 6a – paragraph 4 – point a

Text proposed by the Commission	*Amendment*
	(6) Proxies that act as intermediaries between relying parties and European Digital Identity Wallets shall not obtain knowledge about the contents of the transaction

Justification

The Common Interface should ensure that proxies acting as intermediaries between relying parties and users of the European Digital Identity Wallet can't intercept the contents of the transaction they convey.[14] *Such technical protections are commonplace and don't limit the functioning of the system. The existence of such proxies has been acknowledged in the eIDAS Expert Group*[15]*. While sufficient proliferation of the European Digital Identity Wallet among relying parties can be expected, providers of proxy services will remain few specialized service providers and could act as gatekeepers with in-depth knowledge about user behavior.*

Empowering Users to make Informed Decision when using the European Digital Identity Wallet

Article 6a – paragraph 3 – point c

Text proposed by the Commission	*Amendment*
[Added]	***(c) make an informed decision about the sharing of personal information with relying parties. This includes identification of the relying party, the possibility for complete or partial refusal of information requests from relying parties, a full transaction history .***

Justification

The success of the European Digital Identity Wallet depends on citizens making informed decisions on the information they share with relying parties. Similar guidance about mandatory information on the purpose of the processing by the relying party, as well as the possibility of the use to refuse information requests has been given by the eIDAS Expert Group that's currently developing the Toolbox. It is vital that users don't have to rely on technical recommendations that can change at any time, but that the regulation already guarantees them control over their data. [16]

14 See Issue#9 in the Recommendations from Eric Verheul: https://www.cs.ru.nl/E.Verheul/papers/eIDAS/Issues%20and%20recommendations%20on%20the%20eIDAS%20update%2020210130.pdf (page 11)

15 See chapter 4.8.3 of the final Outline from February 17th 2022: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=37639&fromExpertGroups=true

16 See chapter 4.6.1 of the final Outline from February 17th 2022: https://ec.europa.eu/transparency/expert-groups-register/screen/meetings/consult?lang=en&meetingId=37639&fromExpertGroups=true

Privacy-preserving features of the European Digital Identity Wallet

Recital 29

Text proposed by the Commission	*Amendment*
The European Digital Identity Wallet should technically enable the selective disclosure of attributes to relying parties. This feature should become a basic design feature thereby reinforcing convenience and personal data protection including minimisation of processing of personal data.	The European Digital Identity Wallet should technically enable the selective disclosure of attributes to relying parties. This feature should become a basic design feature thereby reinforcing convenience and personal data protection including minimisation of processing of personal data. ***Mechanisms for the validation of the European Digital Identity Wallet, selective disclosures and authentication of users to access online services shall be privacy-preserving thereby preventing the tracking of the user and respecting the principle of purpose limitation, which implies a right to pseudonymity to ensure the user cannot be linked across several relying parties.***

Justification

Essential functions of the Wallet have to be implemented in a privacy-preserving manner as to limit the potential for automated tracking of the user in cases where they are choosing to cancel an already initiated information sharing request from a relying party, only choosing to selectively disclose individual attributes about them (e.g. age verification in a liquor store) or using the Wallet to log into a service without being subsequently tracked by them. The last feature is offered by Apple's "Sign in with Apple" functionality, which the wallet seeks to replace.

Special Data Minimisation Obligations for Big Tech (VLOPs)

Article 12b – paragraph 3

Text proposed by the Commission	*Amendment*
Where very large online platforms as defined in Regulation [reference DSA Regulation] Article 25.1. require users to authenticate to access online services, they shall also accept the use of European Digital Identity Wallets issued in accordance with Article 6a strictly upon voluntary request of the user and in respect of the minimum attributes necessary for the specific online service for which authentication is requested, such as proof of age.	Where very large online platforms as defined in Regulation [reference DSA Regulation] Article 25.1. require users to authenticate to access online services, they shall also accept the use of European Digital Identity Wallets issued in accordance with Article 6a strictly upon voluntary request of the user and in respect of the minimum attributes necessary for the specific online service for which authentication is requested, such as proof of age. ***In this case, revocable pseudonyms can be generated and***

	used in connection to an identifiable European Digital Identity Wallets. The combination of person identification data and any other personal data and identifiers linked to the European Digital Identity Wallets with personal or non-personal data from any other services which are not necessary for the provision of the authentication or use of core services, is prohibited unless the user has expressly requested it.

Justification

This amendment aims to ensure that Big Tech can't use the Wallet to track people by providing technical safeguards in the way these companies can interact with the European Digital Identity Wallet when legally obliged to do so. Very large online platforms have a long track record of abusing and exploiting users' personal data for profit. This regulation has to provide robust safeguards against these tendencies. The success of the European Digital Identity Wallet depends on the citizen's trust in the overall system to protect government issued identity information whose proliferation would create severe risks on a large scale.

Prevent SMEs to be forced to support the European Digital Identity Wallet

Article 12b – paragraph 5

Text proposed by the Commission	*Amendment*
The Commission shall make an assessment within 18 months after deployment of the European Digital Identity Wallets whether on the basis of evidence showing availability and usability of the European Digital Identity Wallet, additional private online service providers shall be mandated to accept the use of the European Digital identity Wallet strictly upon voluntary request of the user. Criteria of assessment may include extent of user base, cross-border presence of service providers, technological development, evolution in usage patterns. The Commission shall be empowered to adopt delegated acts based on this assessment, regarding a revision of the requirements for recognition of the European Digital Identity wallet under points 1 to 4 of this article.	***[Delete]***

Justification

European Startups should be free to choose if they support the European Digital Identity Wallet in their services or not. Allowing the Commission to unilaterally oblige the use of this particular option for authentication would create a form of centralisation that could be dangerous for the innovative capacity of the European internet and detrimental for the freedom to conduct business for European SMEs.

Reporting Requirements

Article 48a – paragraph 2

Text proposed by the Commission	*Amendment*
The statistics collected in accordance with paragraph 1, shall include the following: (a) the number of natural and legal persons having a valid European Digital Identity Wallet; (b) the type and number of services accepting the use of the European Digital Wallet; (c) incidents and down time of the infrastructure at national level preventing the use of Digital Identity Wallet Apps**.**	The statistics collected in accordance with paragraph 1, shall include the following: (a) the number of natural and legal persons having a valid European Digital Identity Wallet; (b) the type and number of services accepting the use of the European Digital Wallet***, including the number of rejected applications including their reasoning***; (c) incidents and down time of the infrastructure at national level preventing the use of Digital Identity Wallet Apps; ***(d) the type and number of security incidents, suspected data breaches and affected users*** ***(e) the number of user complaints and suspected consumer protection or data protection incidents relating to relying parties.***

Justification

For a wholistic evaluation of the reform the reporting obligations for member states should include a variety of indicators, including foreseeable risks.

Sincerely,

epicenter.works – for digital rights