Recital 6

(6) Natural or legal persons who own person identification data should be considered to be Digital Identity subjects. Regulations (EU) 2016/679, and (EU) 2018/1725 and Directive 2002/58/EC apply to the processing of personal data in the implementation of this Regulation. Therefore, this Regulation should lay down specific safeguards to prevent providers of electronic identification means and electronic attestation of attributes from combining personal data from other services with the personal data relating to the services falling within the scope of this Regulation. This Regulation further specifies the application of principles of purpose limitation, data minimisation, and data protection by design and by default to specific use-cases, without prejudice to Regulation (EU) No 2016/679.


Recital 8

(8) In order to ensure compliance with Union law or national law, service providers should register with the Member States before they are able to rely on the European Digital Identity Wallets. Natural or legal persons should be able to submit a complaint with regard to the use of the European Digital Identity Wallets by a relying party. That will allow Member States to protect users from fraud and prevent the unlawful use of identity data and electronic attestations
of attributes, as well as to ensure that the processing of sensitive data, like health data, can be verified by relying parties in accordance with Union law or national law. **Member States should prevent the unlawful use of identity data, and ensure that the relying parties only require data that is strictly necessary for the provision of the service.**

Recital 9

(9) All European Digital Identity Wallets should allow users to electronically identify and authenticate online and offline across borders for accessing a wide range of public and private services. Without prejudice to Member States’ prerogatives as regards the identification of their nationals and residents, Wallets can also serve the institutional needs of public administrations, international organisations and the Union’s institutions, bodies, offices and agencies. Offline use would be important in many sectors, including in the health sector where services are often provided through face-to-face interaction and ePrescriptions should be able to rely on QR-codes or similar technologies to verify authenticity. **The users should have access to a simple interface that would allow them to have an overview of their current and previous authorisations with regard to the sharing of personal data or electronic attestation of attributes. They should have the possibility to withdraw their consent.** Relying on the level of assurance “high”, the European Digital Identity Wallets should benefit from the potential offered by tamper-proof technology such as secure elements, to comply with the security and integrity requirements under this Regulation. The European Digital Identity Wallets should also allow users to create and use qualified electronic signatures and seals which are accepted across the Union. To achieve simplification and cost reduction benefits to persons and businesses across the Union, including by enabling powers of representation and e-mandates, Member States should issue European Digital Identity Wallets relying on common standards to ensure seamless interoperability and a high level of security. Only Member States’ competent authorities can provide a high degree of confidence in establishing the identity of a person and therefore provide assurance that the person claiming or asserting a particular identity is in fact the person he or she claims to be. It is therefore necessary for certain use cases that the European Digital Identity Wallets rely on the legal identity of citizens, other residents or legal entities. Trust in the European Digital Identity Wallets would be enhanced by the fact that issuing parties are required to implement appropriate technical and organisational measures to ensure a level of security commensurate to the risks raised for the rights and freedoms of the natural persons, in line with Regulation (EU) 2016/679.

Recital 9a - NEW

*In order to ensure the successful uptake of the European Digital Identity Wallet, it is crucial to ensure trust in the technical framework behind, and digital ecosystem surrounding, the*
A high degree of transparency can contribute to establishing trust by allowing users to make informed decisions about the security and privacy characteristics of the European Digital Identity Wallet, as well as allowing for public scrutiny of the activities and actors involved in the framework. For this reason, Member States should ensure that relevant information, such as privacy protective settings, technical architecture, security frameworks, and the location where the processing of personal data is carried out, is included in the set of minimum information about the European Digital Identity Wallet and is made publicly available.

### Recital 9b - NEW

(9b) One of the objectives of the European Digital Identity Wallet should be to improve the possibilities of citizens to make their own choices about what data they share, to minimise the amount of shared data for the service they want to use and to better manage and control the shared data.

### Recital 10

(10) In order to achieve a high level of security and trustworthiness, this Regulation establishes the requirements for European Digital Identity Wallets. The conformity of European Digital Identity Wallets with those requirements should be certified by accredited public or private sector bodies designated by Member States. Relying on a certification scheme based on state-of-the-art technology and commonly agreed standards with Member States should ensure a high level of trust, interoperability and data protection. Certification should in particular rely on the relevant European cybersecurity certifications schemes established pursuant to Regulation (EU) 2019/881. Such certification should be without prejudice to certification as regards personal data processing pursuant to Regulation (EC) 2016/679.

### Recital 11

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, on cloud-based solutions or on a combination of both, taking into account the different levels of risk. Using biometrics to authenticate should not be a precondition for using the European Digital Identity Wallet.
Identity Wallet, notwithstanding the requirement for strong user authentication. Since biometrics represents a unique characteristic of a person, the use of biometric data is limited to specific scenarios pursuant to Regulation (EU) 2016/679, and requires technical and organisational security measures, commensurate to the risk that such processing may entail to the rights and freedoms of natural persons and in accordance with that Regulation. The ability to store information from the European Digital Identity Wallet in the cloud should only be active after the user has given explicit consent. Member States should allow the European Digital Identity Wallet to store cryptographic material and handle transactions on the user device without requiring cloud services, unless the user explicitly consents to such storage. Where the European Digital Identity Wallet is provided on the device of the user, its cryptographic material should be stored in the secure elements of the device.

COMP 8 - AM 38 GREENS
FALL: AM 37 LEFT

RECITAL 12

(12) To ensure that the European Digital Identity framework is open to innovation, technological development and future-proof, Member States should be encouraged to set-up jointly sandboxes to test innovative solutions in a controlled and secure environment in particular to improve the functionality, protection of personal data, security and interoperability of the solutions and to inform future updates of technical references and legal requirements. This environment should foster the inclusion of European Small and Medium Enterprises, start-ups and individual innovators and researchers, while improving compliance and preventing the placing on the market of solutions which infringe Union law on data protection and IT security.

*COMP 9 - AM 41 GREENS, 42 LEFT, 43 ECR, 44 RE, 45 EPP
FALL: 0

RECITAL 17

Service providers use the identity data provided by the set of person identification data available from electronic identification schemes pursuant to Regulation (EU) No 910/2014 in order to match users from another Member State with the legal identity of that user. However, despite the use of the eIDAS data set, in many cases ensuring an accurate match requires additional information about the user and specific unique identification procedures at national level. To further support the usability of electronic identification means, this Regulation should require Member States to take specific measures to ensure a correct identity match in the process of electronic identification. The use of person identification data or a combination of person identification data, including the use of unique and persistent identifiers issued by Member States or generated by the European Digital Identity Wallet is essential to ensuring that the identity of the user, in particular in the public sector and, where required by Union or national law, can be verified. Member State law should be able to require the use of sector-or relying party specific unique and persistent identifiers. The European Digital Identity
The European Digital Identity Wallet should be capable of storing those identifiers and disclosing them where requested by the user.

**RECITAL 25**

(25) *In the internal market, citizens need to have the opportunity to exchange information about their identity across borders. However, in most cases, citizens and other residents cannot digitally exchange, across borders, officially certified information related to their identity, such as addresses, age and professional qualifications, driving licenses and other permits and payment data, securely and with a high level of data protection. This could result in the transfer of that data in a less secure and less organised manner.*

**RECITAL 29**

(29) The European Digital Identity Wallet should technically enable the selective disclosure of attributes to relying parties in a secure and user-friendly manner as one of its key features and advantages. It should also ensure that no attributes are disclosed to parties that are not registered to receive such attributes. This feature should become a basic design feature thereby reinforcing convenience and personal data protection including minimisation of processing of personal data in particular privacy by design and by default. Mechanisms for the validation of the European Digital Identity Wallet, the selective disclosure and authentication of users to access online services should 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. The technical architecture and implementation of the European Digital Identity Wallet should be in full compliance with Regulation (EU) 2016/679. In addition, the decentralised nature of the wallet should enable self-signing and revocability of attributes and identifiers.
**COMP 12 - AM 52 EPP**

**FALL: 0**

**RECITAL 29a NEW**

(28 a) *Unless specific rules of Union or national law require users to identify themselves, the use of services under a pseudonym should be allowed and should not be restricted by Member States, for example by imposing a general obligation on service providers to limit the pseudonymous use of their services.*

***

**PROPOSED AMs FOR SEPARATE VOTE:**

AM46 LEFT, 64 LEFT, 65 GREENS, 66 EPP, 67 LEFT

***

**COMP 13 - AM 82 EPP, 83 LEFT, 84 GREENS**

**FALL: AM 75 LEFT**

**Article 3 point 42 (Article 1.3.i - definitions)**

(42) ‘European Digital Identity Wallet’ is an electronic identification means that allows the user, on a device under the user’s control to store and manage identity data, explicit confirmations of consent to share personal data, credentials and attributes linked to the user’s identity, to provide them selectively to duly registered relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and to create qualified electronic signatures and seals.

**COMP 14 - AM 85 GREENS & AM 86 LEFT**

**FALL: AM 4 ECR, AM 88 LEFT, 89 GREENS, 90 ID, 91 GREENS, 92 LEFT, 99 ECR**

**Article 3 point 43 (Article 1.3.i - definitions)**

(43) ‘attribute’ means an electronic representation of a feature, characteristic or quality of a natural or legal person or of an entity.
Protection of personal data, and pseudonyms in electronic transactions.

1. Processing of personal data shall be carried out in accordance with Regulations (EU) 2016/679 and (EU) 2018/1725 and, where relevant, Directive 2002/58/EC, by implementing the principles of data minimisation, purpose limitation, and data protection by design and by default, in particular with respect to the technical measures for the implementation of this Regulation and the interoperability framework in accordance with Article 12 thereof.

2. Without prejudice to the legal effect given to pseudonyms under national law, the use of pseudonyms in electronic transactions shall be permitted. The use of pseudonyms freely chosen by the user shall always be an option to substitute a unique identifier where identification of the user is not required by Union or national law.

3. Relying parties shall make reasonable efforts to enable the use of their services without electronic identification or authentication.

(2) for relying parties to request and validate person identification data and electronic attestations of attributes in accordance with Regulation (EU) 2016/679;.

(2a) for relying parties to be duly registered on a publicly available list and for their information requests to be visible on that publicly available list;
Article 6a. 4a. 3
Article 1.7 EUDIW

(3) for the presentation in accordance with Regulation (EU) 2016/679 to relying parties of person identification data such as credentials, electronic attestation of attributes or other data, in local mode not requiring internet access for the wallet and for the user to make an informed decision about the sharing of personal information with relying parties, while ensuring that selective disclosure is possible, such presentation including complete or partial refusal of information requests from relying parties, a full transaction history, the possibility to withdraw previously given consent to information requests and information about the exercise of rights as data subject;

* COMP 19 - AM 7 ECR & 128 LEFT
FALL: 0

Article 6a. 4a new
Article 1.7 EUDIW

4a. Where there is a chain of relying parties, intermediaries shall not obtain knowledge about the contents of the transaction;

* COMP 20 AM 9 ECR, 129 LEFT, 130 RENEW, 131 EPP, 132 GREENS
FALL: 0

Article 6a.4b
Article 1.7 EUDIW

(b) ensure that providers of qualified and non-qualified electronic attestations of attributes are technologically prevented from receiving any information about the use of these attributes;
Article 6a.4e
Article 1.7 EUDIW

(e) ensure that the person identification data referred to in Articles 12(4), point (d) uniquely and persistently represents the natural or legal person and that the reference to that data is different for the different relying parties, if legally required;

---

Article 6a.4e a new Article 1.7 EUDIW

(e a) enable the user to access, in a readable format, a list of actions, transactions or uses of electronic attestations of attributes or person identification data, that have been authorised by the user;

(e b) enable the user to transfer the European Digital Identity Wallet's data, and to block the access to it in case of a security breach, allowing for the data suspension, revocation or withdrawal.

---

Article 6a.7
Article 1.7 EUDIW

7. The technical framework for the European Digital Identity Wallet shall be subject to the following principles:

(a) The user shall be in full control of the European Digital Identity Wallet and the user’s data, including self-certification;

(b) The European Digital Identity Wallet shall use decentralised elements for the identity architecture.
(c) The set of electronic identification means, attributes and certificates contained in a European Digital Identity Wallet shall be stored securely and exclusively on devices controlled by the user, unless the user freely consents to storage on third-party devices or to a cloud based option.

(d) The European Digital Identity Wallet shall provide cryptographically verifiable credentials.

(e) The European Digital Identity Wallet shall allow secure connections between the user and the relying parties.

(f) The technical architecture of the European Digital Identity Wallet shall prevent the issuer of the European Digital Identity Wallet, Member State or any other parties from collecting or obtaining electronic identification means, attributes, electronic documents contained in a European Digital Identity Wallet and information about the use of the wallet by the user, except where requested by the user using devices in the user’s control. The exchange of information via the European Digital Identity Wallet shall not allow providers of electronic attestations of attributes to track, link, correlate or otherwise obtain knowledge of transactions or user behaviour.

(g) Unique and persistent identifiers shall not be accessible to relying parties in cases other than when identification of the user is required by Union or national law.

(h) Member States shall ensure that relevant information on the European Digital Identity Wallet is publicly available.

(i) Personal data relating to the provision of European Digital Identity Wallets shall be kept physically and logically separate from any other data held.

(j) If the European Digital Identity Wallet is provided by private parties in accordance to paragraph 1 (b) and (c), the provisions of Article 45f(4) shall apply mutatis mutandis;

(k) Where attestation of attributes does not require the identification of the user, zero knowledge attestation shall be performed.


(m) The European Digital Identity Wallet shall provide a complaint mechanism to enable users to inform the supervisory body under this Regulation and the supervisory authorities established under Regulation (EU) 2016/679 directly where a relying party requests a disproportionate amount of data which is not in line with the registered intended use of that data.
Article 6a. 7 NEW

Article 1.7 EUDIW

7a. Access to public and private services, to online platforms within the meaning of Regulation (EU) XXX/XXX [Digital Services Act] or to the labour market by natural persons shall not be made conditional on the use of the European Digital Identity Wallet.

The use of the European Digital Identity Wallets shall be optional, provided free of charge and in no circumstance create grounds for any type of discrimination.

Natural persons shall not suffer disadvantages for not using the European Digital Identity Wallet.

Article 3
(55) ‘identity matching’ means a process where person identification data or person identification means are matched with or linked to an existing account belonging to the same person.

Article 11a Identity matching

1. When notified electronic identification means and the European Digital Identity Wallets are used for electronic identification, Member States shall ensure identity matching.

2. In order to identify the user upon their request in those cases where identification of the user is required by law, a unique and persistent identifiers issued by Member States or generated by the European Digital Identity Wallets shall be provided together with the minimum set of person identification data referred to in Article 12(4), point (d). Member States may require unique and persistent identifiers can to be sector or relying party specific as long as they uniquely identify the user across the Union.

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).
COMP 26 AM 13 ECR, 187 LEFT
FALL: AM 186 GREENS

Article 1 – paragraph 1 – point 13 – point b
Article 12 paragraph 4 point d

(d) a reference to a set of person identification data necessary to uniquely represent a natural or legal person, which is available from electronic identification schemes;

*COMP 27 AM 16 ECR, AM 205 LEFT, 206 SD, 207 RENEW

Article 17 paragraph 4 f
Article 1.20a2

(f) to cooperate with supervisory authorities established under Regulation (EU) 2016/679, in particular, by informing them without undue delay, about the results of audits of qualified trust service providers, where there is evidence that personal data protection rules have been breached and about security breaches which are likely to constitute personal data breaches, or about suspicions of such breaches that it has become aware of in the performance of its tasks, without prejudice to Regulation (EU) 2016/679.

*COMP 28 AM 14 ECR, 211 LEFT, 212 RENEW, 213 EPP, 214 GREENS, 215 SD, 220 LEFT
FALL: AM15 ECR

Article 20. 2
Article 1.1.22b

Without prejudice to any further obligations on data controllers or processors arising from Regulation (EU) 2016/679, where there is any reason to believe that data protection rules could have been breached, the supervisory body shall inform the supervisory authorities under Regulation (EU) 2016/679, the issuer and the controller of the European Digital Identity Wallet without undue delay and shall provide the results of its audits as soon as they are available;

AM in the operative part for separate vote: AM 119 (new paragraph)

AMENDMENTS ON RECITALS NOT TO BE PUT TO VOTE (tabled on provisions falling outside the LIBE-ITRE agreement on the collaboration modalities):

AM17-18 ID, 39-40 ID, 49 GREENS, 50 LEFT, 51 RE, 58 LEFT, 59-60 GREENS, 61 LEFT, 62 GREENS, 63 LEFT, 68 GREENS, 69 ID, 70 GREENS
***

**AMENDMENTS ON THE OPERATIVE PART NOT TO BE PUT TO VOTE** *(tabled on provisions falling outside the LIBE-ITRE agreement on the collaboration modalities):*