Dear Executive Vice-President Henna Virkkunen,
Director-General Roberto Viola,
Director Christiane Kirketerp de Viron,

Brussels, 8. June 2026

Rejoinder: Reply Open letter concerning the latest batch of eIDAS Implementing Acts

We thank the Commission for its reply on the 22nd of May[1] to our open letter from the 10th of March 2026[2] concerning the latest batch of Implementing Acts under Regulation (EU) No 910/2014 (eIDAS), and for its continued work on the implementation of Regulation (EU) 2024/1183. We hope this response can be taken into account in the ongoing comitology process and the upcoming vote on 18. June 2026.

We remain concerned that several provisions in the current batch of draft Implementing Acts do not adequately address previously identified legal and technical shortcomings and risk undermining key safeguards established by the eIDAS Regulation itself. Our detailed legal and technical analysis is available here.[3] Given that the European Digital Identity Wallet is intended to become a foundational component of Europe's digital public infrastructure, it is essential that its implementing framework fully reflects the objectives, safeguards and fundamental rights protections established by the Regulation.

1. Mandatory Registration Certificates to Protect against excessive Data Requests

Article 5b of Regulation (EU) No 910/2014[4] establishes a mechanism to achieve data minimisation by mandating that all relying parties be registered in a public registry with their use cases and the attributes they intend to request from EUDI Wallet users. This public registry enables oversight and informs public debate with live data about the trajectory of the eIDAS ecosystem[5]. The safeguarding effect of this mechanism is rendered useless if the actual requests can diverge from the registration. The registration certificate is the mechanism to provide the EUDI Wallet with the information necessary to block requests illegally going beyond the registration. The Commission proposal leaves registration certificates optional and thereby negates this core pillar in the eIDAS regulation. This undermines the primary goal of eIDAS by creating gaps in the harmonised trust level within the Union.

The resulting framework creates a potential "weakest-link" problem. A relying party could choose to establish itself in a Member State that does not operate with equivalent certification or registration mechanisms, thereby benefiting from lower levels of scrutiny while still participating in a Union-wide trust framework. The prohibition of "**over-asking**" by relying parties can only be enforced effectively if wallet-relying party registration certificates are mandatory in all Member States. The EDSB has observed that in cases where the registration certificates are not issued it would be "*considerably more difficult and cumbersome for wallet users to verify whether the attributes being requested by*

[1] https://epicenter.works/content/response-and-rejoinder-eidas-open-letter
[2] https://epicenter.works/content/open-letter-concerning-the-fourth-batch-of-eidas-implementing-acts
[3] https://epicenter.works/content/eidas-amendments-to-the-implementing-acts-batch-4-rev8 and https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/16113-European-Digital-Identity-Wallet-registration-of-wallet-relying-parties-update-/F33378018_en
[4] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC http://data.europa.eu/eli/reg/2024/1183/oj
[5] We intend to make use of this public registry with the free software project https://whoidentifies.me/

the wallet-relying party are within the scope of their registered attributes".[6] This issue has been separately raised in an open letter signed by 15 consumer protection and digital rights NGOs.[7] While the Commission did address it after the consultation, the adopted drafts reintroduced it.[8]

Furthermore, the framework entrusts the prevention of excessive data requests to the discretion and supervisory activities of registrars. However Article 9(2)(c) of the Implementing Regulation[9] does not establish mandatory enforcement mechanisms. When a relying party requests excessive attributes, registrars must first conduct a proportionality assessment (***Article 9(4)***) and then may ultimately decide not to suspend or cancel the registration. The **provision grants significant discretion** *("Registrars may suspend or cancel")* instead of imposing a uniform obligation to intervene *("shall")*.

Article 9 (2) and (4) provide limited guidance regarding the discretionary powers in which registrars must intervene and does not establish a comprehensive framework for assessing technical security risks. Recital 11 of the Implementing Regulation likewise concretised the roles of registrars as oversight of compliance with data minimisation obligations, rather than serving as a replacement for security certification. Furthermore it fails establish an equivalent system of technical assurance, security verification, and ex ante scrutiny.

2. Don't neglect the Right to use Pseudonyms

We acknowledge the directly applicable right to use pseudonyms, but note the absence of sufficiently detailed provisions ensuring its effective implementation in practice. The current framework does not adequately specify how wallet-relying parties must accommodate pseudonymous use or how compliance with Article 5b(9) should be assessed. This risks that pseudonyms **remain formally permissible while becoming practically unobtainable** due to requirements that indirectly compel users to disclose their identity. Where no legal identification requirements exists, system design choices may create strong incentives for over-identification by prompting users to divulge more information. Requiring relying parties to **specify** whether **identification requirements** derive from Union law, national law or contractual conditions would be a necessity to enable the EUDI Wallet to offer the use of pseudonyms instead of the legal name of the user.

We want to highlight that the lack of technical specification for pseudonyms in the adopted and currently negotiated implementing acts might lead to a situation where **no EUDI Wallet can be formally certified** since the requirements of Article 5a(4)(b) are not met. Given the enormous risk that citizens are facing from an EUDI Wallet that that doesn't support pseudonyms, **Member States should consider limiting their relying party registry** to only accept use cases that fall under on a legal obligation to identify the user.

---

[6] European Data Protection Supervisor (EDPS), Formal Comments 2024/1052 on the draft Commission Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 https://www.edps.europa.eu/system/files/2025-01/2024-1052_formal_comments_en.pdf

[7] https://epicenter.works/en/content/open-letter-eidas-implementing-acts

[8] https://epicenter.works/en/content/eidas-amendments-to-the-implementing-acts-batch-2-rev6 and Implementing Regulation (EU) 2025/848

[9] Commission Implementing Regulation (EU) 2025/848 of 6 May 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the registration of wallet-relying parties http://data.europa.eu/eli/reg_impl/2025/848/oj

3. Remove disproportionate mandatory biometric data

We remain extremely alarmed about the proposal to make biometric portrait images a mandatory element of the person identification dataset. Having biometric information transacted as a verifiable credential to relying parties puts every user of the EUDI Wallet at a disproportionate risk.

The European Parliament's first-reading position on eIDAS 2.0, adopted by plenary on 16 March 2023 and recorded in Report A9-0038/2023, stated unambiguously that *"the use of biometric data should be limited to specific scenarios (...) and requires organisational and security measures, commensurate to the risk"*[10] adding the explicit principle that *"**the use of biometrics should not be obligatory**"* and *"Using biometrics to identify and authenticate should not be a precondition for using EDIWs (EUDI Wallets)"*. Furthermore, Parliament also wanted explicit prior approval for any relying party intending to request special categories of data like biometrics "*Relying parties that intend to process special categories of personal data, such as health or biometric data as referred to in Article 9 of the Regulation (EU) 2016/679 shall require prior approval from the competent authorities in the Member State in which they intend to provide their services.*". During the trilogue negotiations, all these safeguards for biometric data were removed because assurances were given to the Parliamentarians that biometric information shall not be an inherent element of the EUDI Wallet. Surprisingly, the Commission has since moved in the opposite direction by first including the portrait image as an optional data field in Commission Implementing Regulation 2024/2977 and with the current draft Ares(2026)1286304 making the portrait image mandatory for all EUDI Wallet users. This procedure raises **serious democratic concerns**, since the adopted eIDAS regulation provides no clear basis for such massive biometric data processing. Current drafts directly contradict statements during the negotiations and the European Parliament has no formal role in the adoption of the Implementing Acts.

Mandating biometric information within the system, means that the entire processing carried out through the EUDI Wallet would fall under Article 9 GDPR, subjecting every wallet interaction to the heightened regime for special categories of personal data. This stands in direct contradiction to the Parliament's own democratically adopted position.[11] Thus entities with no legitimate need to process facial images would nonetheless become exposed to biometric data flows, requiring them to conduct data protection impact assessments, establish appropriate processing arrangements and identify a valid Article 9 legal basis. Applying a compliance framework intended for genuinely sensitive biometric processing to routine digital identity transactions creates a burden that is disproportionate to many use cases.

The **risk of function creep** persists once parties are generally allowed to carry biometric attributes regardless of whether such functionality is required or proportionate. This raises concerns under the principles of data minimisation and privacy by design. Not only is biometric information impossible to change for a person, the EUDI Wallet will transact this information to relying parties with transferable cryptographic proofs of authenticity, adding to the risk through data breaches and misuse. While it has been stated that portraits cannot be requested for simple age-verification purposes, it remains **unclear which objective criteria** will govern assessments of necessity and proportionality. Compliance with the GDPR remains necessary but does not demonstrate that the proposed

[10] *Report on the proposal for a regulation amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity (eIDAS)*, A9-0038/2023, Recital 11 https://www.europarl.europa.eu/doceo/document/A-9-2023-0038_EN.html

[11] https://epicenter.works/fileadmin/medienspiegel/user_upload/eIDAS_iA_-_amendments-rv8.pdf

architecture itself satisfies the principles of data minimisation by design. While the selective disclosure feature requires user consent, this does not account for the reality that consent within digital identity ecosystems is not always freely given. Significant asymmetries of power often exist between users and service providers. A more proportionate approach would be to retain portrait images as optional or context-dependent attributes that are available for genuinely high-assurance use cases and to **move "portrait" from Annex I – point 1 Table 1 to Table 2**.

4. Technical safeguards to ensure compliance of very large online platforms

We are concerned about the lack of proposed technical specifications, which would allow legal obligations to be fulfilled in a manner that undermines their practical effectiveness. Direct application of Articles 5b(9) and 5f(3) of the eIDAS Regulation does not resolve the concern that the implementing acts create technical pathways that enable platforms to avoid meaningful compliance while formally respecting the provisions.

WebAuthn and PassKey specifications may permit very large online platforms to satisfy a narrow and formalistic interpretation of their obligations. If authentication can be delegated to existing proprietary credential ecosystems, platforms may be able to claim compliance without providing users with the privacy guarantees, pseudonymous authentication capabilities and technical safeguards that the EUDI Wallet framework is intended to provide. Fundamental rights protections in digital identity systems cannot be assessed solely at the level of legal obligations as they depend equally on the **technical architecture through which those obligations are implemented**. To put it simply, the law can't fix what technology has broken.

5. Preserve strong Tracking Protections

Article 5a (16) of the eIDAS Regulation requires that the technical framework "*shall not allow*" transactions or user behaviour to be tracked, linked or correlated. This constitutes an unambiguous prohibition, which needs to be preserved with the same level of protection in the requirements of the Implementing Acts.

By contrast, the requirement in Art. 3 (10) of the draft Implementing Regulation merely obliges that wallet providers **"*enable privacy-preserving techniques*"** that ensure unlinkability. The obligation to enable a technique is fundamentally different from an obligation to achieve an outcome. A wallet architecture could formally satisfy Art. 3(10) by incorporating privacy-preserving techniques that are insufficient or incorrectly implemented. Privacy-preserving techniques need not merely exist within the system in principle, but must effectively prevent correlation of transactions in practice. Art. 3(10) should be amended to reflect an outcome standard. The obligation to "*enable*" privacy-preserving techniques must be replaced with an obligation to ***"ensure"*** that the wallet architecture makes correlation of **transactions technically impossible.**

Art. 4(4) of the Amendments to the Implementing Regulation[12] requires revocation techniques to be privacy-preserving and that **"*hinder*"** linkability or traceability. The language of Art. 4(4) requires an **equivalent level of protection** to the prohibition standard of Art. 5a(16) to "*prevent*" linkability. Under the principle of hierarchy of norms, an implementing act adopted under Art. 291 TFEU cannot

[12] Draft Commission Implementing Regulation (EU) amending Implementing Regulation (EU) 2025/1569 as regards applicable standards and specifications https://eur-lex.europa.eu/eli/reg_impl/2025/1569/oj/eng

lower the standard established by the regulation it implements. **The implementing Acts should reflect the language and ambition of Article 5a(16) more directly.**

The European Digital Identity Wallet can only achieve broad public trust and acceptance if privacy, security, user control, and fundamental rights protections are consistently embedded in both its legal and technical structure. We therefore respectfully ask the Commission and Member States to address these concerns in the upcoming discussions and to ensure full alignment with the eIDAS Regulation.

We remain at your disposal for further exchange.

Sincerely,

epicenter.works – for digital rights