eIDAS: European Digital Identity Wallet

Analysis and Amendments to the Implementing Acts 2

1 April 2025 (v6)

This analysis and the proposed amendments are based on the second batch of implementing acts for the eIDAS regulation (EU) 2024/1183 after their public consultation[1] in their most recent version. They were sent out by the European Commission to negotiators on 27 March 2025 and will be discussed and voted at the comitology meeting on 9 April 2025[2]. This document only focuses on the implementing acts regarding the registration of wallet-relying parties (Article 5b) and the cross-border identity matching (Article 11a).

To better understand this document, we refer to our consultation response for the previous version of the implementing acts in the second batch[3], the open letter about them signed by 15 digital rights and consumer protection organisations[4] and our extensive work on this file over the past three years[5].

We are extremely alarmed that the Commission has reversed course and made wallet relying party registration certificates optional again. This problem already existed in the first version of this implementing act, but was resolved in the subsequent second version. Now the problem is re-introduced. This risks leaving users critically exposed to illegal information requests that go beyond the relying party registration. No EUDI Wallet is able to protect users from such illegal requests because without registration certificates they lack the information to detect over-asking. Thereby, **one harmonised protection level across the Union is impossible to achieve** and the **only avenue available for a cautious user is to not share their information with relying parties from other EU member states**, thereby undermining the single market and the aim of eIDAS.

Similarly, instead of protecting the right to use pseudonyms the Commission has threatened this important safeguard against over-identification, as they further weakened the possibility for the Wallet to distinguish between Know your customer ("KYC") and non-KYC[6] use cases. This means, the Wallet will have to provide the same level of irrefutable identification available to eGovernment and banks also to Facebook, TikTok and other Big Tech Platforms. With this decision the Commission has created a situation in which the **EUDI Wallet is not safe to use online.**

Lastly, the unique persistent identification of users that Article 11a of the regulation only allows for public sector bodies in cross-border scenarios, is not only extended to the private sector but in the most recent version of the text those private companies no longer need to fall under a legal KYC obligation. This further erodes the distinction between the different use cases of the EUDI Wallet and will create the risk of unique persistent identifiers to proliferate to sectors that rely on tracking and profiling. This directly contradicts the trilogue agreement with the European Parliament and has already prompted parliamentary questions that the Commission did not answer sufficiently[7].

1 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14399-European-Digital-Identity-Wallets-registration-of-relying-parties_en
2 https://ec.europa.eu/transparency/comitology-register/screen/committees/C47300/consult?lang=en
3 https://epicenter.works/en/content/eidas-amendments-to-the-implementing-acts-batch-2-rev4 and https://epicenter.works/content/eidas-amendments-to-the-implementing-acts-batch-2-rev5
4 https://epicenter.works/en/content/open-letter-eidas-implementing-acts
5 https://epicenter.works/en/documents?tx_news_pi1%5BoverwriteDemand%5D%5Btags%5D=19
6 Know your customer (KYC) cases are such where a Union or national law obliges the relying party to identify their users.
7 https://www.europarl.europa.eu/doceo/document/P-10-2025-000847_EN.html

Still we want to acknowledge that we also see improvements with the transparency of the relying party registry that will help foster a better understanding of the eIDAS ecosystem. Additionally, there are also procedural improvements and clarifications in all implementing acts.

5B: RELYING PARTY REGISTRATION

Protection against illegal information requests

We are puzzled by the Commission's sudden reversal of its position after the issue of registration certificates was discussed at length in previous versions of these implementing acts. Those certificates are the precondition for any EUDI Wallet being able to detect over-asking and protecting users from illegal information requests. In the public consultation the Commission proposed that member states can also choose not to issue registration certificates, thereby making those countries a safe haven for companies aiming to undermine the trust in the eIDAS ecosystem. After a huge outcry from digital rights and consumer protection groups[8], as well as critical statements from many member states in the Comitology meeting, the draft was revised so that the previous version of the implementing acts mandated every member state to issue registration certificates. Without any explanation we are now back at square one with optional certificates.

More importantly, the protection against over-reaching information requests was an important requirement of the European Data Protection Supervisor ("EDPS") when he discussed the EUDI Wallet on 7 February 2023 at the Cybersecurity Standardisation Conference[9]: "The only way we can protect personal identification data from excessive requests for data that is not necessary from the service providers is to define relevant reference standards, with precision, **which categories of data can be requested from the user of the Wallet, for specified use cases or purposes.**" (highlights in the original). In a recent statement the EDPS went even further and called specifically to make registration certificates mandatory in this implementing act[10]: "the EDPS strongly recommends replacing "may" with "must" in Article 8(1)"

Since the legislator agreed with the EDPS on the formulation of Article 5b it is now the obligation of the Commission to propose an implementing act that empowers the EUDI Wallet to do its job in protecting

8 https://epicenter.works/en/content/open-letter-eidas-implementing-acts
9 https://www.edps.europa.eu/data-protection/our-work/publications/speeches-articles/2023-02-07-where-are-we-heading-digital-identities_en
10 See point 18: https://www.edps.europa.eu/system/files/2025-01/2024-1052_formal_comments_en.pdf

users and really putting them in control over their data and use of the Wallet, irrespective of where the relying party is registered. Only mandatory registration certificates can achieve harmonized trust levels and predictability for users.

Based on our previous submissions we want to reiterate: The foundational protection of the eIDAS ecosystem is the mandatory registration of relying parties in their country of establishment, while also ensuring cross-border interoperability of wallets and relying party interactions. Article 5b(3) of eIDAS clarifies that a relying party acts illegally if it requests information going beyond its registration. The adopted implementing acts based on Article 5a regarding protocols and interfaces specifies in Article 3(7) that users have at least to be warned if they are confronted with such illegal information requests. Member States can go beyond and also prevent illegal information requests from reaching the user.

Crucially, this agreement is rendered meaningless by the Commission's proposal to make it optional for Member States to issue relying party registration certificates. These registration certificates contain the information what attributes a relying party intends to request. They also include information if the relying party falls under a legal requirement to identify the user (KYC). Relying parties without such certificates cannot be prevented from participating in the eIDAS ecosystem, since Member States are obliged to issue relying party access certificates. A wallet user interacting with a relying party without a relying party registration certificate lacks the information concerning what attributes they are allowed to request and if the user has the right to use a pseudonym. In practice, the absence of a relying party registration certificate will work like a "wildcard" certificate allowing the relying party to obtain all possible attributes – even the ones going beyond their registration – and the users cannot even be warned about this.

The Commission's proposal makes it impossible for a harmonized protection framework to be established with eIDAS. Member States are unable to protect their citizens from illegal information requests from other EU countries, which undermines trust, cross-border interactions and the whole eIDAS ecosystem. Companies that wish to undermine the eIDAS protections can forum shop to establish themselves in countries which do not issue relying party registration certificates. For example, Big Tech companies (VLOPs) could incorporate subsidiaries that obtain an access certificate, but no registration certificate, preventing all other Member States from protecting their wallet users against illegal requests.

The implementing acts go as far as contradicting the very goal of the eIDAS regulation, which according to Article 1 is "to ensure the proper functioning of the internal market". Mistrust against relying parties of other EU countries would be a **devastating blow for the eIDAS ecosystem**, rendering it dead on arrival. We therefore strongly advise against the adoption of the Commission's proposal and argue in favor of making the relying party registration certificates mandatory in all EU member states again.

5b: Article 8 paragraph 1 – Wallet-relying party registration certificates	
1. Member States ~~**may**~~ authorise at least one certificate authority to issue wallet-relying party registration certificates.	1. Member States **shall** authorise at least one certificate authority to issue wallet-relying party registration certificates.
Relying party registration certificates must be mandatory to ensure a harmonized protection level. The information from the relying party registration has to be available to the wallet solution in order to empower the wallet user to take an informed decision about any information requests they receive. Trust in cross-border interactions and the eIDAS ecosystem heavily depends on a level playing field of protections across the European Union.	

5b: Article 8 paragraph 2ff– Wallet-relying party registration certificates	
2. **~~Where a~~** Member State **~~authorised the issuance of a wallet-relying party registration certificate, that Member State~~** shall 3. require providers of wallet-relying party registration certificates to issue wallet-relying party registration certificates exclusively to registered wallet-relying parties; (a) ensure that each intended use is expressed in the wallet-relying party registration certificates; (b) ensure that wallet-relying party registration certificates include a general access policy, being syntactically and semantically harmonised across the Union, informing users that the wallet-relying party is only allowed to request the data specified in the registration certificates for the intended use registered in the registration certificates; (c) ensure that wallet solutions comply with the general access policy by informing users when a wallet-relying party requests data that is not specified in the registration certificates; (d) ensure that wallet-relying party registration certificates are syntactically and semantically harmonised across the Union and that they meet the requirements set out in Annex V; (e) establish dedicated certificate policies and certificate practice statements for the wallet-relying party registration certificates in accordance with the requirements set out in point (d); (f) ensure that wallet-relying parties declare if they intend to rely upon electronic identification of natural persons as part of their registration.	2. Member State**s** shall**:** (**a**) require providers of wallet-relying party registration certificates to issue wallet-relying party registration certificates exclusively to registered wallet-relying parties; (**b**) ensure that each intended use is expressed in the wallet-relying party registration certificates; (**c**) ensure that wallet-relying party registration certificates include a general access policy, being syntactically and semantically harmonised across the Union, informing users that the wallet-relying party is only allowed to request the data specified in the registration certificates for the intended use registered in the registration certificates; (**d**) ensure that wallet solutions comply with the general access policy by informing users when a wallet-relying party requests data that is not specified in the registration certificates; (**e**) ensurethat wallet-relying party registration certificates are syntactically and semantically harmonised across the Union and that they meet the requirements set out in Annex V; (**f**) establish dedicated certificate policies and certificate practice statements for the wallet-relying party registration certificates in accordance with the requirements set out in point (d); (**g**) ensure that wallet-relying parties declare if they intend to rely upon electronic identification of natural persons **where required by Union or national law** as part of their registration.
The obligations listed in this section are applicable to all member states, since every member state is under the obligation to issue a wallet solution. Without this clarification point d (previously c) would mandate the member state that issued the relying party registration certificate to ensure compliance of (all other) wallet solutions. This reading would potentially lead to the registration certificate being a simple allow/prohibit statement, instead of the list of registered attributes that is checked against the actual request. *The right to use pseudonyms can only be achieved if the wallet solution knows if a particular use case falls under a legal obligation to identify the user or not. This needs to be clarified in point g (previously f).* *We assume that point a (previously paragraph 3) was mistakenly formatted as a paragraph and really*	

meant as the first sub-point under paragraph 2.

5b: Recital 3	
To ensure broad access to the registers and to achieve interoperability, Member States should set up both human and machine-readable interfaces that meet the technical specifications set out in this Regulation. Providers of wallet-relying party access certificates and wallet-relying party registration certificates, ~~**where available,**~~ should, for the purpose of issuing those certificates, also be able to rely upon these interfaces.	To ensure broad access to the registers and to achieve interoperability, Member States should set up both human and machine-readable interfaces that meet the technical specifications set out in this Regulation. Providers of wallet-relying party access certificates and wallet-relying party registration certificates should, for the purpose of issuing those certificates, also be able to rely upon these interfaces.
(see above)	

5b: Recital 9	
As set out in Regulation (EU) No 910/2014, wallet-relying parties are not to request users to provide any data other than those indicated for the intended use of wallets during the registration process. Wallet users should be able to verify the registration data of wallet-relying parties. To enable wallet users to verify that the attributes being requested by the wallet-relying party are within the scope of their registered attributes, Member States ~~**may**~~ require the issuance of wallet-relying party registration certificates to registered wallet-relying parties. To ensure the interoperability of the wallet-relying party registration certificates, Member States should ensure that those certificates meet the requirements and standards set out in the Annex. In particular, wallet-relying parties should declare, whether they intend to rely upon electronic identification of natural persons to meet one of the requirements set out in paragraph 1 of Article 6 of Regulation (EU) 2016/679 of the European Parliament and of the Council1 for the purpose of transparency. Further, relying parties are not to refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.	As set out in Regulation (EU) No 910/2014, wallet-relying parties are not to request users to provide any data other than those indicated for the intended use of wallets during the registration process. Wallet users should be able to verify the registration data of wallet-relying parties. To enable wallet users to verify that the attributes being requested by the wallet-relying party are within the scope of their registered attributes, Member States **shall** require the issuance of wallet-relying party registration certificates to registered wallet-relying parties. To ensure the interoperability of the wallet-relying party registration certificates, Member States should ensure that those certificates meet the requirements and standards set out in the Annex. In particular, wallet-relying parties should declare, whether they intend to rely upon electronic identification of natural persons to meet one of the requirements set out in paragraph 1 of Article 6 of Regulation (EU) 2016/679 of the European Parliament and of the Council1 for the purpose of transparency. Further, relying parties are not to refuse the use of pseudonyms, where the identification of the user is not required by Union or national law.
(see above)	

Clearly distinguish KYC from non-KYC use cases in their registration

The right to use a pseudonym in cases where the relying party does not fall under a legal obligation to identify the user (Know-your-customer or "KYC") is enshrined in Articles 5 and 5b(9) as well as in Recitals 57 and 60 of the eIDAS regulation. Since the last version of the implementing acts the drafts deteriorated to a point where this safeguard for users of the EUDI Wallet can no longer be delivered and enforcement by national eIDAS authorities will be almost impossible.

The current draft insufficiently distinguishes between use cases of the EUDI wallet in which the relying party is under a legal obligation to identify the wallet user and other cases. Article 8 paragraph 7 fails to capture this distinction and is not in line with the aforementioned requirements of the eIDAS regulation. Because identification can happen with or without a legal obligation, but the right to use pseudonyms is dependent on that distinction, it is important to let relying parties specify if such a legal obligation applies to them or not.

Furthermore, specifying if such an obligation applies to a particular use case should be done by describing the concrete legal provisions from which such an obligation arises from. Meaningful oversight and efficient administrative procedures will depend on the knowledge based on which concrete legal provision such an obligation for the relying party arises. Otherwise, in a dispute about the correctness of any given relying party registration the national register would have to screen all legal provisions to identify those that might be applicable to a particular registration. Such information should also be made available through the relying party registry.

Simply put, the requirements we find in Annex V paragraph 3 (k) should also be incorporated in Article 8 paragraph 7 and Annex I paragraph 7. This increases the efficiency of administrative procedures of national registers, increases transparency and enables greater trust in the correctness and completeness of the information provided in the relying party register.

See changes proposed above on Article 8.

5b: Annex V paragraph 3 point j item 4 – wallet-relying party registration certificates	
to include a declaration on the ~~**intention**~~ to identify natural persons referred to in Article 8(2)g;	to include a declaration on the **legal requirement** to identify natural persons referred to in Article 8(2)g;
The registration certificate has to include the information if the particular use case falls under a legal obligation to identify the user or not. ***The referenced Article 8(2)g currently doesn't exist and requires our above amendment to Article 8.***	

5b: Annex I paragraph 9a – Information regarding wallet-relying parties	
[INSERTED]	**9a. For each intended use, where applicable, a description of the legal requirements by Union or national law that oblige the wallet relying party to identify the wallet user.**
Part of the information relying parties' provide in the course of their registration should be a description of	

the legal provisions based on which they assume to fall under an obligation to identify the wallet user. *This is in the interest of an efficient and expedient procedure for providing relying party certificates by national registers. Should the information provided in the register be disputed, the register would have to do its own assessment and without knowing the legal provisions that's potentially applicable, it would create an undue bureaucratic burden on the national administration. Otherwise, the register would have to go through a cumbersome legal analysis to establish which obligations are applicable or not.* ***Alternatively, a leaner version of this process is for relying parties to specify in their registration at least if they rely on identification because of a legal obligation or based on their terms of service.***

Ensure the correctness of data in the eIDAS system

The last version of the implementing acts removed the crucial obligation in the relying party registration process to ensure the validity, authenticity and integrity of the information provided to the registry. Trust in the eIDAS ecosystem depends on the correctness of the foundational information who asks what for which purpose that forms the basis of all transactions. Removing due diligence completely also doesn't follow the "proportionate-to-risk" requirement from Article 5b paragraph 2 of eIDAS since this will increase the likelihood of of failures or fraud in the information provided by relying parties.

5b: Article 6 – paragraph 3	
3. Where possible, registrars shall verify in an automated manner: (a) the accuracy of the information required under Article 5; [...]	3. Where possible, registrars shall verify in an automated manner: (a) the accuracy**, validity, authenticity and integrity** of the information required under Article 5; [...]
The relying party registry should be under a due diligence obligation to verify the information provided by the relying party is valid, authentic and passes integrity checks.	

Register of Relying Parties

We want to congratulate the Commission for the changes in the public register of relying parties. These improvements in the ability to iterate the registry and expect uniform results for each match will enable transparency and independent, data-driven oversight so as to ensure trust in the eIDAS ecosystem can be uphold. These changes reflect the obligation of Article 5b paragraph 5 of eIDAS to make relying party registration information publicly available.

Suspension based on proportional harms

We welcome the many clarifications in Article 9 paragraph 4. The suspension procedure is much stronger if there is a clear obligation of relying party registrars to adhere to requests from other competent authorities. Furthermore, we welcome that inaccurate registration information according to

Article 9 or the failure to minimise the requested attributes according to Recital 12 provide grounds for suspension/cancellation of the corresponding access and registration certificates.

Lastly, we welcome that our suggestion has been taken on board that registrars have to take the fundamental rights, security and confidentiality of users in the ecosystem into consideration.

Furthermore, we welcome the clarifications in Annex IV and V that requests for suspension of access or registration certificates from data protection authorities have to be adhered to. This clarification concurs with our reading of Article 46a paragraph 5 (f) of the eIDAS regulation.

Record keeping

We still welcome the clarification in Article 10 to align it with the 10 year retention period specified in Recital 9 and also the newly introduced Recital 14 detailing the purpose of record keeping.

Handling of Contact Information

We still support the exclusion of the physical address of relying parties specified in Annex 1 paragraph 4 from the accessibility via the relying party registry and the access and registration certificates. This achieves the right balance and ensures the completeness requirement for the relying party registry can be adhered to.

11A: IDENTITY MATCHING

Extension of identity matching to the private sector

We still find ourselves in the situation to revisit one of the most controversial issues of the eIDAS negotiations. This is very surprising since these controversial changes were made in non-public drafts after the public consultation[11] and on the explicit request of powerful industry actors[12]. Since the previous version we asked for the articles of the implementing act to be cleaned of the language that contradicted the eIDAS regulation. Yet, the issue was not resolved, because the problematic interpretation still resides in the Articles and Recitals and was actually extended to now also include non-KYC private sector relying parties. Crucially, the title of the implementing act on Article 11a now contradicts the language of Article 11a by no longer referencing public sector bodies.

The legal basis of the implementing act is based on Article 11a which limits the identity matching to public sector cross-border cases. This was the explicit will of the European Parliament in the trilogue agreement from 28. June 2023 clearly:

> *"10 Unique and persistent identifier (UPI) (rows 176 to 180a)*
> • *Title is cross-border record matching (or something similar)*
> • *Keep paragraph 1 on obligation* ***for MS to perform identity matching***
> • ***Deletion to all references to UPI*** *across the text*
> • *Inclusion of the wallet to incorporate the current system through an implementing act"*

Subsequently, member states tried to insert a text that would make their identity matching available to the private sector in KYC-cases[13]. Yet, this was unsuccessful and the final text of Article 11a(1) put very strict limits to only allow identity matching and only for the public sector in cross-border cases:

> *"**When acting as relying parties for cross-border services, Member States** shall ensure unequivocal identity matching for natural persons using notified electronic identification means or European Digital Identity Wallets."*

Yet, the Commission extends the scope of the implementing act towards the private sector cases. In the interest of upholding trust in the eIDAS ecosystem and in the democratic process, these new provisions have to be deleted immediately.

11a: Title	
laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards cross-border identity matching of natural persons	laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards cross-border identity matching of natural persons **by public sector bodies**

11 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14400-European-Digital-Identity-Framework-cross-border-identity-matching_en
12 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14400-European-Digital-Identity-Framework-cross-border-identity-matching/F3513199_en
13 See 2021/0136(COD), row 179

The private sector was explicitly excluded from the identity matching according to Article 11a. This change in the title of the implementing act is removing a crucial safeguard of the eIDAS regulation and goes against the trilogue agreement reached with the European Parliament. This is undemocratic!

11a: Article 2 paragraph 9 – General Requirements	
Where Member States enable wallet-relying parties which are not public sector bodies to perform identity matching the mechanisms and procedures laid down in this Regulation shall apply, where applicable.	**[DELETE]**
Article 11a of eIDAS provides no legal basis to extend the scope of identity matching to the private sector. Article 5f of eIDAS[14] only creates an obligation for certain sectors to offer the wallet on a voluntary basis, but it does not extend the scope of any particular method of identification or is specific for cross-border cases. This implementing act is based on Article 11a and has to take the legal text and the political agreement undermining it into consideration.	

Alternative proposal to at least mitigate the problem:

11a: Article 2 paragraph 9 – General Requirements	
Where Member States enable wallet-relying parties which are not public sector bodies to perform identity matching the mechanisms and procedures laid down in this Regulation shall apply, where applicable.	Where Member States enable wallet-relying parties which are not public sector bodies to perform identity matching the mechanisms and procedures laid down in this Regulation shall apply, where applicable. **The relying parties have to be required by union or national law to identify users.**
Even when a member state chooses to extend identity matching to the private sector, the limitation to legal KYC obligations should apply.	

11a: Recital 4	
To ensure that the identity matching process functions in a reliable manner across all Member States, Member States acting as relying parties, should perform the initial identity matching when a natural person first requests to get granted access to a service operated by the relying party, based on either the minimum dataset as laid out in Commission Implementing Regulation (EU) 2015/15011 or the person identification dataset laid out in Implementing Regulation (EU) 2024/29772. ~~**While t**~~his Regulation focuses on	To ensure that the identity matching process functions in a reliable manner across all Member States, Member States acting as relying parties, should perform the initial identity matching when a natural person first requests to get granted access to a service operated by the relying party, based on either the minimum dataset as laid out in Commission Implementing Regulation (EU) 2015/15011 or the person identification dataset laid out in Implementing Regulation (EU) 2024/29772. **T**his Regulation **solely** focuses on

14 The Commission attempted to justify their overreaching by relying on Article 5f: https://www.europarl.europa.eu/doceo/document/P-10-2025-000847-ASW_EN.html

Member States acting as relying parties~~, Regulation (EU) No 910/2014 leaves it for Member States to decide if the identity matching system is also made available to private relying parties~~. Where Member States foresee identity matching for relying parties which are not public sector bodies, they should apply as far as possible the mechanisms and procedures laid down in this Regulation.	Member States acting as relying parties. Where Member States foresee identity matching for relying parties which are not public sector bodies, they should **limit it to relying parties where identification of users is required by Union or national law and** apply as far as possible the mechanisms and procedures laid down in this Regulation.
This extension of the identity matching system to the private sector illegally extends the mandate for this implementing act provided for by Article 11a and contradicts the political agreement in trilogue.	

Do not add last-minute unregulated person identifiers

In the previous version of the implementing act new provisions were included that allow for completely new person identifiers that are unspecified and unregulated. We recommended removing these identifiers since unequivocal identity matching was ensured already by the legislators. Yet, in the most recent version even more "additional information or complementary procedures" were introduced. Such last-minute additions of personal information in cross-border cases introduce a severe risk for the data protection of users.

If data beyond the mandatory data sets were required for cross-border identity matching when using the wallet, this would have been taken into account by the legislator in the amended legislation. However, this is not the case. To add an additional data set for the use in cross-border identity matching is thus beyond the boundaries of what this implementing act is allowed to regulate. Such additional identifiers might also not be available or harmonized across member states.

Furthermore, the addition of any optional data identifier would regularly lead to unsuccessful matching processes, because successful matching would only be possible if both parties used the same optional data identifier. However, this cannot be guaranteed without further definition, so the addition of any optional data identifiers should be avoided.

11a: Article 2 paragraph 3 & 4 – General requirements	
3. When reliance is on a wallet, the information to be used for unequivocal identity matching shall be the mandatory person identification data set out in Section 1 of the Annex to Commission Implementing Regulation (EU) 2024/2977, ~~**together with any optional data that is needed to ensure that the presented dataset is unique including, where appropriate, additional information or complementary procedures**~~. 4. When reliance is on a notified electronic identification scheme, the information to be used	3. When reliance is on a wallet, the information to be used for unequivocal identity matching shall be the mandatory person identification data set out in Section 1 of the Annex to Commission Implementing Regulation (EU) 2024/2977. 4. When reliance is on a notified electronic identification scheme, the information to be used for unequivocal identity matching shall be the mandatory attributes of the minimum data set for a natural person set out in Section 1 of the Annex to Commission Implementing Regulation (EU) 2015/1501.

for unequivocal identity matching shall be the mandatory attributes of the minimum data set for a natural person set out in Section 1 of the Annex to Commission Implementing Regulation (EU) 2015/1501 **~~including, where appropriate, any additional information or complementary procedures~~**.	
see above	

11a: Recital 6	
For the purpose of cross-border identity matching when using the wallets, the information used for unequivocal identity matching should be the mandatory data identifiers of the person identification dataset set out in Section 1 of the Annex to Commission Implementing Regulation (EU) 2024/2977**~~, together with any optional data needed to ensure that the set of person identification data is unique~~**.	For the purpose of cross-border identity matching when using the wallets, the information used for unequivocal identity matching should be the mandatory data identifiers of the person identification dataset set out in Section 1 of the Annex to Commission Implementing Regulation (EU) 2024/2977.
See above	