The Consumer Voice in Europe

MAKING EUROPEAN DIGITAL IDENTITY AS SAFE AS IT IS NEEDED

BEUC position paper

Contact: Kasper Drazewski – digital@beuc.eu

BUREAU EUROPÉEN DES UNIONS DE CONSOMMATEURS AISBL | DER EUROPÄISCHE VERBRAUCHERVERBAND
Rue d'Arlon 80, B-1040 Brussels • Tel. +32 (0)2 743 15 90 • www.twitter.com/beuc • www.beuc.eu
EC register for interest representatives: identification number 9505781573-45

Co-funded by the European Union
Ref: BEUC-X-2022-016 - 10/02/2022

Why it matters to consumers

The life of EU consumers is more than ever built around digital services, both public and private. Consumers are increasingly required to identify themselves online via different means to access such services. It is important that they can use a Digital Identity solution that is easy to use, widely accepted, secure and protects their privacy and data.

Summary

The establishment of a European Digital Identity system is a welcome initiative. A robust and secure method of electronic authentication and attestation of attributes is becoming increasingly important for consumers to be able to access digital services, both public and private; a need that has increased even further during the COVID-19 pandemic.

At the same time, the European Digital Identity brings a set of risks and challenges which must be carefully addressed to minimise unforeseen consequences, particularly in terms of user agency, robustness, privacy and data protection.

In this regard, the following concerns need to be put forward, to ensure creation of a robust European Digital Identity scheme.

Privacy/safety risk areas:

- The system must safeguard that the storage of official documents, biometric data or attestations of attributes does not create security risks;
- individuals must not be tracked on the basis of their use of the European eID by issuers of attestations and other service providers;
- implementation of the system must avoid disruption of the security systems of web browsers, on which consumers depend on for their safety, security and privacy;
- issuance and revocation of attributes, as well as suspension and revocation of the eID must not carry risks to privacy of the holder;
- preventing exclusion and discrimination of those consumers who do not wish or are not able to use the system, in particular by ensuring that the use of the European eID remains voluntary for consumers.

Other considerations:

- It is important to ensure a robust and simple revocation of attributes on request of holders of the European Digital Identity Wallet, with a single point of contact;
- civil society and academics should be involved in the implementation process alongside representatives of the industry.

1. Why an EU digital identity solution is needed

Consumers rely heavily on online products and services in their daily lives. Digital companies have become important intermediaries and often the cornerstone of social interaction, shopping, education, employment or public services.

Navigating the digital environment can rarely be done anonymously. Service providers often require consumers to set up an account and establish their identity, asking for information such as name, contact details, gender and age. Surfing hundreds of user accounts established with various services is a chore and a data protection risk. Users rely to an increasing degree of digital entities provided by Big Tech companies, which is not optimal from the perspective of avoiding commercial surveillance.

At the same time, while over the past years there has been a clear push towards the development of eGovernment services, the ability to use public services online has gone from convenient to crucial during the time of the COVID-19 pandemic. This further highlighted the need for a trustworthy and safe electronic identification system, built on a public service stricture, which could also be recognised EU-wide, to facilitate use in cross-border settings.

Therefore, the Commission's ambition to create a secure, interoperable EU-wide electronic identification with the functionality of a trusted electronic portfolio of documents is laudable and comes at a time of particular need. It is also very important in the context of the EU digitisation objectives. According to the Commission's 2030 Digital Compass, by 2030, all key public services should be available online, all citizens should have access to electronic medical records and 80% citizens should be using an eID solution.[1]

2. What is the European Digital Identity Wallet and how does it work?

The proposal for the European Digital Identity[2] builds on and amends the existing eIDAS framework[3] established in 2014 and regulating Europeans' digital identity documents and services. Under the proposed new scheme, every Member State is to launch at least one smartphone app that will integrate the functionality of existing state-issued ID with strong authentication for purposes of interacting with public and private services, working both online and offline (the European Digital Identity Wallet). This authentication would then be valid throughout the Community.[4]

The Wallet should also allow to sign documents electronically and have the functionality of an electronic file cabinet, integrating digital attestations of attributes (also legally recognised in a cross-border setting) to serve as a portfolio of the individual's attributes such as medical certificates, diplomas, licences or certificates of birth. Using the Wallet to prove one attribute (e.g., age) would not require sharing other data, such as e.g., name

[1] See https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en.

[2] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity {SEC(2021) 228 final} - {SWD(2021) 124 final} - {SWD(2021) 125 final}, (the '**Proposal**'), https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-regulation.

[3] EIDAS is an acronym for electronic IDentification, Authentication and trust Services. https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.

[4] Already under Article 6 of the existing eIDAS Regulation, mutual cross-border recognition of eIDs was conditional upon being notified to the Commission and included in the list published by the Commission.

or address. Cross-border recognition of qualified attestations of attributed is made mandatory under the Proposal.[5]

While integration with national identity documents means that Europeans will be using the eID to at least identify themselves to public authorities, no obligation exists for use of the Wallet by consumers when interacting with private actors.[6] Some private actors would also be obliged to recognize the European eIDs, including very large online platforms and service providers in areas such as transport, energy, banking and financial services, communications or health.[7]

3. Main issues from a consumer perspective

3.1. EU-wide persistent identifiers as risk to consumer privacy?

Under Article 11a of the Proposal, a unique EU-wide citizen identification number is to be assigned to effectively every user of its authentication feature. Authentication is a core functionality of the European Digital Identity Wallet and forms part of the interoperability framework.[8] This number forms part of the minimum data set necessary to uniquely and persistently represent a natural or legal person.[9]

Using the Wallet for identification means that this government-verified, permanent personal identifier will be disclosed by the Wallet to third parties wishing to access the Wallet's data ('relying parties'), such as in the case where a car rental company will want to verify our driver's licence or an online platform. The user is to be in control over whether they wish to identify themselves (save for where identification is required by law). However, there is considerable risk that such disclosure can be easily or unfairly obtained due to the digital asymmetry[10] that consumers face in the online world, particularly if the consumer needs to quickly access a service or start using a connected device they purchased.[11]

This raises concerns over how easily this unique and lifelong identifier will be exploited by rogue actors. In particular, Big Tech and ad-tech companies will find a way to add this to existing personality profiles to further increase ability to track users' activities. The vagueness of the Proposal's formulations does not alleviate these concerns. Furthermore, the 2014 eIDAS Regulation requirement for ensuring privacy by design was not carried over to the Proposal.

Separation of authentication and attribute attestation is fundamental. The Wallet is intended to offer selective disclosure of attributes[12] (e.g., allowing age verification without disclosing the legal name).[13] However, under Article 6a (4) (d), the Wallet is to provide a mechanism to ensure that the relying party is able to 'authenticate the user **and** to receive electronic attestations of attributes' (emphasis added). This prompts the question of

[5] Article 45a.
[6] Recital 28 of the Proposal.
[7] Recital 28 of the Proposal.
[8] New Article 11a in connection with Article 12 (4) of the existing eIDAS Regulation (EU) No 910/2014.
[9] This requirement of Article 12 of the original eIDAS Regulation has only been updated to reference a 'persistent' identifier under the Proposal.
[10] See Micklitz, Helberger et al. (2021) Structural asymmetries in digital consumer markets, BEUC 2021.
[11] Epicenter.works and European Digital Rights (2022) eIDAS Policy Paper, 25 January 2022.
[12] Recital 29 of the Proposal.
[13] The variant implemented in the Proposal would "create positive impact on data protection by way of imposing a clear separation between the collection of personal identity data and the collection of other data for commercial exploitation." - Inception Impact Assessment, DG CNECT H4, Revision of the eIDAS Regulation – European Digital Identity (EUid), Ares(2020)3899583.

whether authentication and checking of attributes **can actually be separated**, so that disclosure of identity is not unavoidably connected with e.g. age verification.

If the cited provision indeed means that attestation of an attribute is preceded by a step that identifies and authenticates[14] the user, this puts in question whether it is actually possible to use select attributes to prove certain properties without revealing one's full identity. Notably, an explicit requirement that attribute verification must be possible **without full identification** of the Wallet holder **is not found** in the Proposal.

Concerningly, the provisions of the 2014 eIDAS Regulation mandating implementation of the principle of privacy by design and ensuring that personal data is processed in accordance with Directive 95/46/EC, are now removed from the Proposal and not replaced by a new reference to the General Data Protection Regulation.

BEUC recommendations

- The Proposal must address the privacy risks related with the issuance of unique persistent EU-wide identifiers to individuals and offer means of mitigating them. At the minimum, the functionality of selective disclosure of attributes must be embedded into Article 6a allow the Wallet holder to remain in control of whether their identity is disclosed to the relying party, so that they can still maintain anonymity in situations where full identification is not needed.
- Where such disclosure is not mandated by law, the Proposal should prevent disclosure of the unique identifier to a relying party. In such cases, the Wallet should offer means of trusted authentication without disclosure of the unique identifier.
- Article 11a of the Proposal should specify the format of the unique identifiers, the conditions of their change (e.g., in the event of theft) and justify how their use can be reconciled with national restrictions and prohibitions on use of unique identifiers[15] and the privacy by design requirements of Article 25 of the General Data Protection Regulation.

3.2. Insufficient safeguards against tracking activity of Wallet holders

One of the functionalities of the Wallet is to prove possession of certain attributes through electronic attestations stored in the Wallet.[16] These attestations will be issued by authorised entities in Member States. To safeguard consumers from tracking and harvesting of data on this basis, it is important to ensure that issuers of such attestations and other parties are systemically precluded from tracking and profiling the individual on how such certificates are later used by the individual ('unlinkability'). This should be ensured on the following levels:

- the attestation issuer should not have access to the final form of the signed credential, preventing tracing of usage ('issuer unlinkability')[17];
- relying parties should be precluded from tracking and profiling (otherwise anonymous) users across websites ('service-level unlinkability').

[14] Under Article 3 (5) of the original eIDAS Regulation which is not amended by the Proposal, 'authentication' in the context of individuals is equated to 'electronic identification' of a person.
[15] In Germany, the use of unique persistent identifiers is prohibited under the census ruling of 1983. 65 BVerfGE 1 (1983). See Sümer B, Schroers J (2021) The new digital identity Regulation proposal and the EU data protection Regime, https://www.law.kuleuven.be/citip/blog/the-new-digital-identity-regulation-proposal/.
[16] Recital 4, 27, Article 1 of the Proposal.
[17] Ringers S, Verheul E, Hoepman J (2017). An Efficient Self-blindable Attribute-Based Credential Scheme. 10.1007/978-3-319-70972-7_1 https://eprint.iacr.org/2017/115.pdf; see also https://privacybydesign.foundation/irma-explanation/

As mentioned above, the Proposal does not contain specific provisions that would protect the user of the Wallet from being linked to the data trail they leave behind. On the contrary, if a number of relying parties are given access to the same unique identifier, they could merge their data logs to track the given consumer's activity.[18]

The issue of unlinkability is insufficiently addressed in the Proposal. In its current wording, the Proposal states that the Wallet will 'ensure that trust service providers of qualified attestations of attributes cannot receive any information about the use of these attributes'.[19] This suggests that it is the task of the Wallet to deny issuers access to information about how the individual is actually using these attributes. This solution leaves a potential gateway for issuers accessing the issued credentials (with cooperation of the Wallet) and raises concerns as to the robustness of this approach.[20] In addition, the Proposal lacks technical measures to ensure full unlinkability including wallet apps and relying parties, that would protect the Wallet user from rogue actors.

Importantly, under Article 6b paragraph 4, screening and verification of relying parties, i.e., third parties willing to access data from the Wallet, is to be performed by the Member State of establishment – meaning it is effectively the Member State of choice for such a third party. The criteria for such a verification are to be published by the Commission six months after the Regulation has entered into force. No revocation mechanism, e.g., as contingency for a relying party being compromised or turning to rogue actions, is envisaged.

BEUC recommendations

- Article 6a (7) must ensure that robust technical safeguards are in place that will prevent Wallet users from being tracked by certificate issuers and across services by third parties.
- The system for authentication of relying parties of Article 6b must be complemented by a verification system at the level of a central eIDAS regulator, independent of procedures in individual Member States, along with a revocation mechanism.

3.3. Risk of discrimination, exclusion and limiting choice

To preserve individual choice, promote individual agency and prevent widening digital divides, it is equally important to respect the wishes of those consumers who want to use the Wallet, as it is in the case of those who do not want to or cannot use it. This principle should apply throughout the design and implementation of the whole framework.

The Proposal gives Member States 12 months to launch ('issue') European Digital Identity Wallets. Participation is to remain voluntary for citizens; however, according to the Commission's 2030 Digital Compass, by 2030, 80% citizens should be using an eID solution.

It is important to ensure that individuals who do not use an eID, for reasons of anonymity, data security or otherwise, are not put as a disadvantage.[21]

[18] Brussel Privacy Hub (2021) The European Commission Proposal Amending the EIDAS Regulation (EU) No 910/2014: A Personal Data Protection Perspective, p. 8.
[19] New Article 6a (4) (b).
[20] Hoepman J (2021) The European Digital Identity framework.
[21] For an account on how improper implementation of national ID schemes has led to social exclusion of vulnerable populations in Kenya, Uganda and India, see Privacy International (2021) Exclusion by design: how national ID systems make social protection inaccessible to vulnerable populations.

For example, an eID which is tied to a smartphone app runs the risk of exclusion for individuals who are not smartphone users, or simply do not have a sufficiently modern device. However, an alternative form of using the eID for such citizens is currently not envisaged in the Proposal.

A significant potential risk area exists for low-income consumers who will not have latest-model devices and may not have all the required security updates. Due to the vague provisions on storage of documents and biometric data, it is impossible to assess to what degree the Proposal ensures robustness of identity storage on older devices.

BEUC recommendations

- Choosing whether or not to get an eID must remain voluntary to individuals. The Proposal should contain specific anti-discrimination provisions to protect those who opt not to do so.
- To prevent exclusion, a simple alternative form of using the Wallet should be envisaged that does not require a smartphone app, such as a card reader and/or a key generator.
- Provisions must be included to prevent exposure of consumers using older devices.

3.4. Weakening of browser security

A browser is of fundamental importance in nearly all of our online experience. It is entrusted with storing, accessing and displaying private information. Importantly, it also verifies the identity of the website being accessed. Browsers use certain symbols, notably the padlock indicator, to confirm that the connection is encrypted and the identity of the given website has been confirmed by an independent party. This means the consumer can trust that their passwords and other information will not be stolen by a fake website disguised as the one they sought. This is a significant factor preventing identity theft, privacy violations and financial crimes.

The safety of consumers using a browser is strictly connected to the robustness of this system which is strictly reliant on the entities issuing websites with digital certificates ('certificate authorities' or 'CAs'). A single certificate issued without due procedural checks can have catastrophic consequences.

As a result, consumers' trust and safety are in the hands of the browser's internal vetting system that only accepts such CAs that continuously adhere to its security requirements to be added to the trusted certificate collection (root store) of the browser.[22]

This safety system is now put into question by the Proposal. Article 45 (2) mandates that browsers must automatically accept qualified certificates for website authentication,[23] effectively granting Member States automatic access to citizens' root stores. This would constitute a dangerous precedent breaching consumers' trust in their devices, potentially

[22] Hancock A 2021) EU's Digital Identity Framework Endangers Browser Security, EFF.org https://www.eff.org/deeplinks/2021/12/eus-digital-identity-framework-endangers-browser-security; Mozilla (2021) EU Digital Identity framework (eIDAS): November 2021 position paper on the European Commission's legislative proposal to revise the eIDAS Regulation.

[23] Since the original eIDAS Regulation, use of Qualified Certificates for Website Authentication (QWACs) has been flagged by browser vendors as carrying security risks (including by outsourcing security-critical choices to third parties) and in effect discontinued by widely deployed browsers. The proposed amendments would require their implementation. See Hancock A, Callas J (2021) What the Duck? Why an EU Proposal to Require "QWACs" Will Hurt Internet Security, EFF.org; see also ENISA (2019) Recommendations for technical implementation of the eIDAS Regulation, p. 22.

enabling more surveillance of encrypted web traffic and strengthening governments which do not respect fundamental rights.[24]

BEUC recommendation

- The proposed amendment to Article 45 must be dropped due to its potential for immense harm to consumer safety, security and trust.

3.5. Location of stored documents and biometric information

While the idea to combine identity authentication with a portfolio of official digital documents of the individual is welcome, the Proposal does not make it clear where exactly such documents would be stored. This is an important issue from a security perspective.

An electronic identity solution that integrates officially recognised documents, such as education diplomas or a driver's licence, could either:

- store only attestations (certificates) proving that the individual has been issued such attributes, or
- store such documents themselves in an electronic format, in a cloud service and/or the user's device.[25]

The Proposal does not make it clear which of the two solutions has been chosen. The wording of Recital 11 states that the Wallet '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' (emphasis added), suggesting that both approaches may be used.

In practice, this means the Wallet could have access to secure storage of biometric information on consumers' smartphones, containing data such as fingerprints or facial recognition patterns. This weakens the security of such storage and increases the risk of identity theft. No technical details concerning this solution or the security of cloud storage of such information are included in the Proposal as they are to arrive via delegated acts.

BEUC recommendations

- The Proposal should specifically envisage that the official documents of Wallet users shall be stored in the cloud, and ensure safeguards are to be in place to prevent unauthorised access and/or manipulation.

3.6. Potential risks in revocation of attributes

The Wallet allows revocation of attributes which have lost their validity, e.g., in the case of a person's driver's license being suspended. This is important also to the holders, who will need to remove outdated or incorrect attestations of attributes. In the current draft however, no specific provisions guide such user-initiated revocation which may leave consumers at a loss if they realise their Wallet contains incorrect entries about e.g. their diplomas or driver's licence.

[24] Hancock A (2021), EU's Digital Identity Framework Endangers Browser Security, EFF.org https://www.eff.org/deeplinks/2021/12/eus-digital-identity-framework-endangers-browser-security; Mozilla (2021) EU Digital Identity framework (eIDAS): November 2021 position paper on the European Commission's legislative proposal to revise the eIDAS Regulation; Epicenter.works and European Digital Rights (2022) eIDAS Policy Paper, 25 January 2022.
[25] See Hoepman J (2021) The European Digital Identity framework.

The Proposal states that such revocation has immediate effect (where a qualified electronic attestation of attributes has been revoked after initial issuance, it shall lose its validity from the moment of its revocation, and its status shall not in any circumstances be reverted', Article 45c of the Proposal).

The actual method of achieving this immediate effect is not specified in the Proposal.[26] This leads to the question of how this can be achieved, assuming that issuers of attributes have no access to, and cannot receive any information about, the use of such attributes. In an extreme scenario, revocation with immediate effect could indeed be achieved if attribute attestation was indeed preceded by identification of the Wallet user. This could then allow issuers to broadcast to relying parties 'black lists' of users whose attributes have been revoked,[27] but with a devastating effect on privacy.

BEUC recommendations

- The Proposal should contain a simple procedure with a single point of contact at Member State level to allow Wallet holders to efficiently request revocation or correction of outdated or incorrect data in the Wallet.
- The Proposal must at least underline that the revocation of attributes under Article 24 must be designed and implemented in a way that will not compromise privacy of affected Wallet holders.

3.7. Non-EU relying parties and sensitive data

The mechanism for identification and common authentication of relying parties wishing to rely upon the Wallet is enshrined in the new Article 6b, involving a mandatory communication to the relying party's Member State of establishment to ensure compliance with requirements set out in Union law or national law for the provision of specific services.[28]

This leaves open the question about relying parties which are not established in the European Union and thus have no Member State to report to.

A related issue lies in the wording of Recital 8 and Article 6b (3). Taken verbatim, these provisions envisage relying parties engaging in verification of processing of sensitive data:

> "In order to ensure compliance within Union law or national law compliant with Union law, service providers should communicate their intent to rely on the European Digital Identity Wallets to Member States. That will allow Member States 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 (Recital 8)
>
> 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 (Article 6b (3))."

[26] The Proposal links the procedure to Article 24 paras. (3) and (4) which speak of registration in a certificate database of the issuer and providing relying parties with information on the revocation. However, this method does not guarantee immediate effect at the level of the Wallet.
[27] See Hoepman J (2021) The European Digital Identity framework.
[28] Article 6b (1) - (2).

BEUC recommendations

- If non-EU entities are to be allowed to become relying parties under the Proposal, safeguards are necessary to ensure their compliance with the Regulation. Conversely, if non-EU entities cannot become relying parties, this should be stated explicitly.
- The provisions of Recital 8 and Article 6b (3) should be made clearer to state explicitly under which circumstances and in what form relying parties are to be engaged in verification or authentication of data, including processing sensitive data originating from the Wallet.

3.8. Revocation of compromised wallets

According to the proposal, if a European Digital Wallet is breached or compromised in a way that affects its reliability or the reliability of other European Digital Identity Wallets, the issuing Member State shall, without delay, suspend the issuance and revoke the validity of the affected Wallet and inform the other Member States and the Commission accordingly.[29]

The wording of the provisions does not make it clear what exactly is to be suspended and revoked in the event of a breach. A European Digital Identity Wallet is defined as 'a product and a service'[30] which does not shed light on the interpretation (i.e., the entire system, as per Article 6a(1), or the affected personal Wallets, or a class of such Wallets). Suspension and revocation (as well as reinstatement once the breach has been remedied) are to be communicated to other Member States and the Commission[31] without delay, which puts in question whether indeed this is envisaged to be done in the case of every single case of a breach at the level of an individual. Conversely, if a class or the entire service is meant to be suspended, this may significantly affect the trustworthiness and reliability of the service for users not affected by the breach.

BEUC recommendations

- The wording of Article 10a(1) should make it clear how the suspension and revocation process is to be conducted, as well as how it applies to and affects Wallet users who are not directly affected by a breach.
- For overall clarity and uniform application, the Proposal should name specific criteria for suspension or revocation of a Wallet in the event of a breach, such as where the breach must be reported to the Data Protection Authority under Article 33 of the General Data Protection Regulation.

3.9. Oversight of conformity assessments and overall robustness

With the potential adoption by 360 million people by the year 2030,[32] the envisaged eID system is of enormous dimensions, extremely complex and, not least due to the nature of the data it is to be entrusted with, highly dependent on all its elements meeting a high standard for robustness and interoperability.

[29] New Article 10a(1).
[30] New Article 3(42).
[31] New Article 10a(1)-(2).
[32] Based on predictions made in the 2030 Digital Compass; see Section 2.

Notably however, the Proposal still chooses to employ decentralised conformity safeguards. Recital 10 states that conformity with the overall requirements is certified at the level of individual Member States.[33] At the same time, Recitals 14 and 15 push for 'streamlining and acceleration' of the review and notification process to facilitate promotion of the system.[34]

Under these conditions, it is uncertain whether the individual implementations of the system at the level of Member States can ensure a necessary uniform level of robustness for protecting the data of all individuals who are predicted to use the Wallet by the year 2030.

BEUC recommendations

- The 'streamlining' of peer review, as well as the 'simplification' and 'acceleration' of notification processes for eID schemes under Recitals 14 and 15 should be complemented with oversight measures to minimise the risk of uneven implementation of the European Digital Identity system at the level of Member States.
- The robustness of the system must be rendered independent of potential compliance, conformity or security issues arising at the level of individual Member States. In particular, the Proposal should envisage be a Union safeguard procedure involved a central agency or the Commission to ensure the robustness of the system even in case of a faulty conformity assessment procedure at national level.

3.10. Involvement of civil society or academics

Implementation of the European Digital Identity framework is to be guided by a set of common standards and technical references as well as best practices and guidelines. This is regulated in the accompanying Recommendation for a Common Union Toolbox for a coordinated approach towards a European Digital Identity Framework[35] which accompanies the Proposal.

The Toolbox contains recommendations for collaboration that should 'lead to a technical architecture and reference framework, a set of common standards and technical references as well as best practices and guidelines as a basis for the implementation of the European Digital Identity framework'[36] through 'a structured process of cooperation between Member States, the Commission and, where relevant, private sector operators to develop the Toolbox.'[37] The Recommendation is to be implemented through the eIDAS expert group, involving standardisation bodies, relevant private and public sector stakeholders and external experts.[38]

Notably, the list of stakeholders does not include civil society organisations or academics, leaving the process in the hands of authorities and representatives of the industry.

[33] Recital 10 of the Proposal.
[34] Recitals 14 and 15 of the Proposal.
[35] Commission Recommendation of 3.6.2021 on a common Union Toolbox for a coordinated approach towards a European Digital Identity Framework ('Toolbox Recommendation'), https://digital-strategy.ec.europa.eu/en/library/trusted-and-secure-european-e-id-recommendation.
[36] Recital 10, Toolbox Recommendation.
[37] Toolbox Recommendation, recital 11.
[38] Toolbox Recommendation, p. 3, section 2 (2) et seq.

BEUC recommendations

- Considering the anticipated impact of the Digital Identity system on the lives of European citizens and societies at large, the implementation process under the Toolbox Recommendation must ensure equal representation of stakeholder groups as envisaged in Section 2(2) of the Recommendation, including consumer organisations, wider civil society groups and academics.

END

This publication is part of an activity which has received funding under an operating grant from the European Union's Consumer Programme (2021-2027).