On the Agile Nature of the European Digital Identity Framework: Happily Marrying Privacy, Innovation, and Democracy?

Thijmen van Gend[1][0000−0001−9157−9107]

Netherlands Organisation for Applied Scientific Research (TNO)
thijmen.vangend@tno.nl

Abstract. The European Commission proudly proclaims that the European Digital Identity Framework *"was created in a more agile way"*. This departure from more traditional multi-year lawmaking cycles is the manifestation of the EU's pursuit of harmonisation and desire to accommodate technological developments without having to enact whole new regulations. But how does this *"agile way"* (re)shape issues of privacy, fragmentation, legal certainty, and democratic accountability? This paper sets out to answer that question through a qualitative inductive study of policy documents and grey and academic literature. It finds that the agile nature undermines the effectiveness of traditional checks and balances, largely attributable to the Commission's significant executive power. Moreover, the agility makes the regulatory framework a continuously moving target, which undermines its ambition of harmonisation and is resource-intensive for others in the ecosystem to keep track of – from parties wishing to offer trust services, to those that have to accommodate them or wish to hold the ecosystem to account. On top of that, concerns around privacy and reliance on Google and Apple remain unaddressed and are aggravated by more recent regulatory initiatives that contradict protections promised or codified earlier, and by a tight deadline for Member States to offer EUDI wallets by the end of 2026. In sum, while the EDIF's agile nature at points improves harmonisation and security across Member States, it raises new challenges interesting for both policy and privacy scholars.

Keywords: European Digital Identity Framework · EUDI wallet · Agile lawmaking · Privacy · Innovation.

1 Introduction

Technical and policy advancements enable increasingly secure and versatile *"identity wallets"* on smartphones. With their roots in the Self-Sovereign Identity phi-

Draft paper prepared for the 21st IFIP Summer School on Privacy and Identity Management 2026. Please do not distribute without the author's consent. Submitted July 31 2026.

losophy [82], these wallets are supposed to give users agency over whom they share their attributes and credentials with in online and offline interactions. The European Union (EU) subscribes to this vision. On May 20 2024, Regulation No 2024/1183 *"establishing the European Digital Identity Framework (EDIF)"* entered into force.[1] With it, the EU pursues the development of EU Digital Identity (EUDI) Wallets, defined as *"an electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals"* (art. 3(42)). The aim is that all people *"have secure, trusted and seamless cross-border access to public and private services, while having full control over their data"* (art. 5a(1)). The eIDAS prescribes that Member States (MSs) must offer their citizens access to at least one EUDI wallet by 24 December 2026 (art. 5a(1)) and that organisations required to do *"strong user authentication"* accept these wallets as one method hereto by 24 December 2027 (art. 5f(2)). Also, the European Commission (EC) positions wallets as a fundamental enabler for age verification [e.g. 39, 41].

The EU push for EUDI wallet adoption is thus clear. However, as both technical and institutional maturity vary significantly among MSs, multiple countries are set to miss the end-of-2026 deadline [45, 64, 66]. A presumed factor to these delays is the EU's self-proclaimed unique *"agile approach"* to lawmaking [36]. Whereas the typical EU lawmaking cycle spans 5 to 10 years, with the EDIF the EU uses a new *"Toolbox process"* to keep up with the rapidly changing technology and standardisation landscapes. Instead of hammering out all requirements for EUDI wallets in the ordinary legislative procedure for the EDIF, the EDIF codifies significant agency for the EC, MSs, and industry groups to lay down policy and technical requirements after the Regulation had already been adopted [36]. Still, the EDIF is not free of contention. This paper sets out to answer the research question: ***How does the EDIF's "agile" regulatory process affect issues of privacy, fragmentation, legal certainty, and democratic accountability?***.

2 Methods and structure of the paper

The research employs a qualitative inductive study. Concretely, it answers three subquestions. The question *What are the main arguments for agile regulation?* (§3) is answered through an unstructured academic literature review, searching Google Scholar for *(agile OR adaptive OR anticipatory OR "future-proof")*

[1] This Regulation amends Regulation No 910/2014 *"on electronic identification and trust services for electronic transactions in the internal market"* (known as eIDAS1, abbreviating Electronic IDentification, Authentication and trust Services) and is hence also known as *"eIDAS2"* or *"eIDAS 2.0"*. If no number is indicated, the paper refers to eIDAS2.

AND ("policy_making" OR governance OR regulation OR "law_making" OR "decision_making").

The next part studies: *What makes the EDIF 'agile'?* (§4). It compares the former academic literature against grey literature about the EDIF. This grey literature is mostly legal and policy documents, with a smaller role for technical documentation.

The final subquestion is: *What critiques of EDIF are affected by regulatory agility?* (§5). It adds more grey literature, namely NGO and industry whitepapers, blogs, open letters, and identity-related news reports. These sources were identified through GitHub; LinkedIn pages and posts of individuals and organisations; journalistic outlets; and discussion fora; and backwards snowballing across them. Furthermore, additional academic literature was included, via Google Scholar searches and backwards snowballing. Search strings included combinations of EDIF, EIDAS, EUDI, and EUDIW on the one hand, with privacy, democracy, legal, accountability, and governance on the other. Section §6 presents the conclusion of the paper.

3 Arguments for agile and adaptive lawmaking

Many mature policy streams on governance in the face of (technological) uncertainty exist. §3.1 briefly surveys these. The goal is not to systematize this knowledge (some of the referenced works already do so), but to illustrate the richness of this literature and present arguments for and against agile and adaptive regulation, as well as present characteristics that make governance agile or adaptive. §3.2 then discusses how the EU argues in favour of 'agile' policymaking for the EDIF.

3.1 Agile and adaptive policymaking in academic literature

Three (partially overlapping) concepts that may structure the trove of relevant literature are decision-making, governance, and regulation. *Agile decision-making* can allegedly help deal with the *"turbulent world"* [78] and accommodate technical developments [27]. Decision-making under uncertainty strives to handle the unknowns of climate change, natural disasters, or stakeholder behaviour [e.g. 60, 67]. Decision-making under deep uncertainty is suitable for situations with deep uncertainties, many policy options and high system complexity [68]. Its approaches (robust decision-making; dynamic adaptive planning; dynamic adaptive policy pathways; info-gap decision theory; and engineering options analysis [68]) have been fruitfully applied in infrastructure cases (e.g. for traffic and water) and may – like decision-making under uncertainty [60] – use computational models to select optimal policy alternatives from multiple scenarios [67].

Adaptive governance may contribute to *"a stable, accountable and responsive government"* [56] and is closely tied to yet different from agile governance: where adaptive governance's main objective is to learn and maintain the fit between governance and the subject of this governance, agility is primarily about sensing

and addressing events quickly through continuous small improvements [57]. Agile and adaptive governance can contradict each other, as *"adaptive governance calls for both decision speed and sound analysis, for both centralized and decentralized decision-making, for both innovation and bureaucracy, and both science and politics"*" [57, p. 1]

Specifically in (technology) regulation scholarship, concepts include future-proof legislation [e.g. 24, 53, 76, 77, 80, 83], agile regulation [14, 27, 55, 74], anticipatory regulation [16] and (Un)planned Adaptive Regulation [17, 80]. For instance, Brass and Sowell [20] propose a model based on the latter, that *"integrates the benefits of centralized risk regulatory frameworks with the operational knowledge and mitigation mechanisms developed by epistemic communities that manage day-to-day Internet security ... facilitating the feedback necessary to address evolving IoT security risks"* (p. 1092). Schrepel [80] uses a four-dimensional framework to assess the adaptiveness of EU regulations: 1) monitoring infrastructure (data collection obligation, real-time monitoring, machine-readable format), 2) triggering logic (indicators defined, update frequency, discretion), 3) adaptation (mechanism type, secondary instruments, scope of modification, type of modification), and 4) institutional learning (learning institutions, actors involved, stakeholder input, impact assessments).

Whether regulations should be formulated *"technology neutral"* has been debated since the late 1990s [61, 70], with this principle now a staple of the EU's General Data Protection Regulation (recital 15) and AI Act [75]. Prevalent undertones in this literature are the fear that regulation stifles innovation, and that technological progress may outpace or disrupt current regulatory frameworks and processes [e.g. 16, 53, 61, 80]. Others reject these fears as too simplistic and rhetorical tricks to serve the agendas of tech companies [e.g. 19]. At the same time, policy robustness (i.e. the extent to which policies remain effective across different scenarios) poses an inherent paradox with adaptive policy-making: *"mechanisms intended to enable ongoing adjustment can generate entrenchment and opportunistic behavior through coalition stabilization, self-reinforcing feedback, institutional friction, and strategic agenda setting"* [26, p. 1].

3.2 How the EU argues for an agile EDIF

The eIDAS Regulation entered into force on September 17 2014, with most articles applying from July 1st 2016. The Regulation prescribed the Commission to review its application by July 2020, considering inter alia technological, market and legal developments (art. 49). The main finding of the evaluation, published in June 2021 [32, 33], was that *"needs to be improved in terms of effectiveness, efficiency, coherence and relevance to deliver on new policy objectives, user expectations and market demand also taking into account recent developments in digitalisation"*; it suffers from *"inherent limitations to the public sector, the complexity for online private providers to connect to the system, its lacking availability in all Member States and its lack of flexibility to support a variety of cases"* [33, p. 7]. According to the evaluation, over "70% of trust service providers and

supervisory bodies considered that there are areas of the eIDAS Regulation that requires [*sic*] further harmonization" [32, p. 77]. eIDAS1 was already formulated *"technology neutral"* to anticipate *"technological, scientific and social developments"*, but its regulatory outcome proved subpar: *"the speed of implementation did not turn out to be high enough to roll out innovation in time"* [32, p. 51].

For one, its objective of technology neutrality provided MSs, authorities and conformity assessment bodies space to interpret legal requirements themselves. For instance, the majority of supervising tasks took place at MS level [32]. While eIDAS1 already provided the Commission the ability to enact acts, the evaluation found that it did not sufficiently follow through to achieve its goals of harmonisation and keep up with technical developments. Across MSs, the adoption of CIRs, interpretations (e.g. in conformity assessment, and regarding the definitions of 'substantial' and 'high' levels of assurance), and strictness and protection levels differed, leading to forum shopping and *"a regulatory race to the bottom"* [32, p. 82]. To increase both harmonisation and adaptiveness to technological developments in these contexts, the evaluation makes two proposals. First, the EC could specifically reference standards and requirements in CIRs to make accreditation of CABs, conformity assessments and certification of eID schemes more concrete. This would enable asserting compliance of e.g. notified eID schemes with the functional requirements of the regulatory framework in a structured way, address quality issues of CAB reports, and reduce market fragmentation caused by different interpretations and certification schemes across MSs . Second, a more formal mechanism for coordination and exchange of best practices between national supervisors should be set up [32].

The evaluation's messages fit in a broader pattern. The EU is pursuing speed and agility in law-making more broadly with its 'simplification agenda'. It speaks of a *"simpler and faster Europe"* [37] and *"an agile Digital Rulebook for the EU [aiming] to stimulate the competitiveness"* of the EU [40]. Digital identity is not the only *"fast-changing technical landscape where citizens have complex needs"* [36]. We may also expect to see similar agile policymaking by the EU in the future because of the concept of institutional mimesis [82].

4 What makes the EDIF 'agile'?

The Commission proudly proclaims that the EDIF *"was created in a more agile way"*, compared to the EU's typical 5-10 year lawmaking cycle [36]. But what makes the EDIF 'agile'? This section explores the major contributors, namely adaptation through the Toolbox Process (§4.1), national certification schemes (§4.2), and monitoring and institutional learning (§4.3).

4.1 Adaptation: The Toolbox Process

A number of the eIDAS1 evaluation's proposals have found their way to the EDIF. When the Commission published its amendment proposal for eIDAS 1 in

2021, it also published a Recommendation to start with a *"common EU Toolbox"* process [50, 9, 44] so that the necessary governance and technical work could be undertaken in parallel [36]. This Toolbox process mostly concerns the technical side of fostering wallet readiness across the EU. The Toolbox goes a long way to fill in the contours of the eIDAS2 – 43 articles empower the Commission to adopt implementing acts on particular topics – and has three major streams. First is establishing the European Digital Identity Cooperation Group (EDICG)[2] that superseded the already existing eIDAS Expert Group, to spearhead creating technical standards and best practices, and developing the Architecture and Reference Framework (ARF) together with MSs and the Commission. Similar to the EIDAS Committee, the EDICG is chaired by the Commission and consists of MS-appointed *"representatives responsible for European Digital Identity Wallets, notified electronic identification schemes and trust services"*, but also of Commission staff, with the latter lacking voting rights (art. 3 C(2024) 6132). It cooperates with and advises the Commission on relevant policy initiatives and implementing acts; supports supervisory bodies by fostering best practices and information exchanges with ENISA and other stakeholders; and organises peer reviews of electronic identification schemes that have to be notified (art. 46e(5) eIDAS).

The second stream is procuring industry experts to develop demo EUDI wallets and libraries based on the ARF. Third is funding large-scale public-private pilots to experiment with EUDI wallets across scenarios, with one series starting in April 2023 and another in 2025 [36]. The experiences gained in these streams informed both the other streams, and the legislative process up until the EDIF's ultimate entry into force on May 20 2024 – and beyond that date as well, in creating the many CIRs that the EDIF references. At the moment of writing, the EC has adopted 34 CIRs after passing the eIDAS2 [48]. This way, *"The legislative and technical work have occurred in tandem"* [36].

4.2 National certification schemes

Another agile aspect is that of national certification schemes. With identity primarily being a matter of national sovereignty [82], MSs logically have a big role to play herein. Offering citizens an EUDI wallet can be done directly by the government, by a mandated party, or by recognised private initiatives (art. 5a(2)). Before any such wallet may be provided, their conformity with the legal requirements must be certified against a certification scheme by conformity assessment bodies (art. 5c). As for cybersecurity aspects, an EU certification scheme adopted persuant to the Cybersecurity Act [3] shall be used (art. 5c(2)). Adoption of this scheme may take several more years [65]. To not halt EUDIW adoption in the meantime, MSs must devise their own national certification schemes (art. 5c(3)), though progress varies significantly at this stage [45, 64, 66]. In December 2024, the EC adopted a Commission Implementing Regulation (CIR)

[2] The Commission's obligation to establish the EDICG is codified in eIDAS art. 46e and effectuated with effectuated with Commission Decision C(2024) 6132 [34]

to outline minimum requirements for these national certification schemes [35]. It prescribes that the schemes must be reviewed periodically, *"taking into account feedback from stakeholders"* (art. 6(1) [4]). Countries must also account for national legislation. Dutch examples include the implementation act for the GDPR, regulation on valid identity documents (*Wet identiteitsmiddelen*) and regulation on digitalisation in and of government (*Wet digitale overheid*). The CIR furthermore references multiple other regulations and industry standards that national certification schemes may or must account for.[3] The national certification scheme, a foundational component of the EDIF, thus become an intricate linkage of country-specific rules, and references multiple ISO/IEC standards, the EU Common Criteria (EUCC) scheme, EUCS, FITCEM, SOC2, MDSCert, and more.

By deferring certification scheme creation to MSs, the eIDAS2 risks once again aggravating fragmentation and interoperability issues [65]. In response – and perhaps also to make meeting the December 2026 deadline more feasible – some MSs are bundling expertise and capacity to set up a joint certification scheme: Nordic and Baltic countries will develop one by the end of 2026 [73]. These countries are also collaborating with other MSs, such as The Netherlands and Spain [81]. Another option for MSs is to (partially) adopt the generic certification scheme that ENISA has been creating at the Commission's request since February 2026. ENISA also does so in cooperation, having launched a public consultation for a draft version in April 2026 [28].

Another initiative that contributes to harmonisation is the Functional Conformance Assessment Framework (FCAF) that was published as part of ARF version 3.0.0 in July 2026 [23, 49]. Conformance tests serve as *"shared, reusable set of test cases for the functional requirements that Wallet Solutions must support"* [23] and are thus instrumental to the certification schemes, though this framework is only initial and still under development.

4.3 Monitoring and institutional learning

The EDIF also establishes monitoring and learning institutions, contributing to regulatory adaptiveness [80]. For instance, MSs must maintain public lists of registered relying parties (art. 5b) and certified EUDI wallets (art. 5d); inform stakeholders about security and data protection incidents (art. 5e(1)); and publish statistics about adoption, complaints and incident statistics and report about them to the Commission yearly (art. 48a). Supervisory bodies must also report on their activities yearly to the Commission, who shares the report with the Parliament and Council (art. 46a(6)). As for reviews, the Commission shall report to the Parliament and Council whether the eIDAS should be adjusted to accommodate experiences in applying it or technological, market, and legal developments by 21 May 2026, and at least every four years thereafter report on achieving the goals of the Regulation (art. 49).

[3] Most obviously in Annex II (*"Criteria to Assess the Acceptability of Assurance Information"*) that non-exhaustively (Annex IV art. 7(2)) mentions certification schemes.

5 Discussion: Agility-affected EDIF Critiques

While the EDIF's deadline for EUDIW availability is less than 4 months away at the moment of writing, not all contours of the EDIF have been filled in yet. And even parts that are filled in, remain subject to critiques. This section discusses critiques that can be related to or affected by the EDIF's agile nature.

5.1 Agile nature at odds with traditional checks and balances

Comitology With its CIRs, the Commission gains significant power in the practical translation of the EDIF. 'Comitology' applies checks and balances to this power [51, 2] As per EIDAS art. 48, the Commission must have its draft CIRs voted on by a committee (called the eIDAS committee [52]). The committee has one representative per MS and is chaired by the Commission. MS representatives as well as additional experts authorised by the chair may attend meetings, though only the representatives have voting power (art. 5, 7 of its rules of procedure [25]).[4]

If a qualified majority votes in favour, the Commission must adopt the draft. When there is no qualified majority, the Commission can adopt the draft or submit an altered version for reconsideration. Should a qualified majority vote against, the Commission may not adopt the act, but may submit an amended version for reconsideration or submit the original draft to the appeal committee. This appeal committee similarly consists of one representative per MS [15], *"but at a higher level of representation"* [51].

Beyond this committee, the EU Council and Parliament have a right of information (i.e. the Commission must share its drafts with the Parliament and Council at the time of submitting them to the committee for discussion) and of scrutiny (i.e. the Parliament and Council may find the Commission to exceed its powers when the CIR inches too close to legislative acts passed by ordinary legislative procedure; the Commission must then review its proposal, but may still proceed).

Challenges for democratic accountability Regardless, the Commission holds a significantly stronger position than in the ordinary legislative procedure wherein the EDIF was created. And *"Centralisation may promote coherence, but it imposes high reliance on the expertise, bandwidth, and political will of a single supranational institution"* [80, p. 13].

Furthermore, the agile nature makes policymaking less transparent. For one, multiple technical standards referenced in the EDIF are paywalled, which courts have deemed a breach of the public right to information [79], and undermines privacy as well, for it makes it harder for people to know the legal rules that

[4] Notably, while articles 10 and 11 of the committee's rules of procedure prescribe publishing meeting minutes and attendance lists, these were not available online for all meetings at the time of writing .

should be protecting them. Others critique standards organisations for supposed captured by large industry players [] or influence of non-European bodies . This critique could be extended to the role that such companies play in the large-scale pilots, too.

On top of that, the legitimacy of other bodies than the Commission that the EDIF vests power in, is at times questionable. For one, the EDICG's practical conduct is hard to grasp. According to the group's webpage, only three meetings have been conducted, all in 2024 [47]. Also, there is no public list of group members; even though a call for participants to a subgroup that closed in May 2026 [46] speaks of publishing meeting materials and group composition. Lampoltshammer et al. [63] expect the EDICG to be composed of national experts in the field of trust services and digital identities and call the EDICG *"a suitable vehicle to represent public sector interest"* as it is public sector-led (p. 198). Yet, because of its composition, they doubt whether it sufficiently represents the many other private stakeholders in this field (e.g. relying parties, qualified trust service providers, software companies wishing to offer (services for) wallets, and consumer and privacy organisations). This is hard to verify. Besides, Weigl and Reysner [82] point out that the EDIF barely codifies requirements for maintaining independence of regulators and supervisors, hampering accountability – especially considering the *"democratic backslide"* (p. 8) of some MSs.

5.2 A moving 'big, hairy, audacious goal'

Besides their technical nature, the high frequency and amount of standards and policy developments challenges those who wish to hold policymakers to account: the EDIF and related services remain moving targets. NGOs are generally already highly resource-constrained; having to keep up poses a high burden on their organisational bandwidth. This is similar for academia. Academic publishing generally has long cycles compared to the velocity of policy and technical specification updates.[5] Once an article is published, the onus is on the reader to examine whether critiques or recommendations have not become outdated.

MSs are no exception. In a May 2026 meeting[6], the EC presented to MSs new draft IAs to be voted on [38]. (At least) one of the acts was not shared before; three MSs protested that voting on them in that same meeting left them insufficient time to consider its ramifications [54]. According to epicenter.works, countries also condemned obligating additional and complex standards mere months before the December 2026 deadline, which would make "a robust and safe product unrealistic" [30]. This presents an interesting trade-off between stability on the one hand (prioritised by epicenter.works [29]) and the latest agreed upon standards for (securely) enabling identity use cases. The Commission then

[5] For instance, Abellán Álvarez et al. [11] conducted a privacy evaluation of ARF version 1.5 (published in February 2025 [23]). They published their preprint online in May 2025 [12] and the revised peer-reviewed publication was in October 2025 [11]. At these times, the ARF had already reached version 1.10 and 2.6, respectively [23].

[6] Minutes of this meeting are not published [43]

pulled the draft before a vote took place [54], before tabling it again in June where it met a positive vote [42].

Naturally, its dynamics also affects relying parties and companies wishing to offer or accommodate trust services. In an industry survey of 49 respondents across the ecosystem, *"unclarity of ecosystem realisation"* was seen as a major hurdle to achieving the December 2026 deadline, with almost 50% of respondents signalling *"an unclear vision for how the national wallet ecosystem should function (...), the complexity of establishing national certification schemes, and ongoing changes to legislation and the ARF on the EU level"* [69, p. 16]. Indeed, national maturity differs significantly across MSs, according to industry reports [64, 66] and the Commission. In a December 2025 event, the Commission assessed the *"maturity and readiness"* of 17 participating MSs. It found that 8 countries are building technical foundations but still lack a national wallet; 2 countries see a national wallet emerging with a solid technical basis; 3 countries with a well-adopted national wallet that is only partially aligned with EUDI frameworks; and 4 countries with a widely adopted national wallet according to the EUDI specifications. [45]. To illustrate: at the time, national EUDI wallets of the Netherlands, Spain and Germany had planned their releases for early 2027; while the French and Austrian wallets had already been used in millions of authentications.

Also, the fact that the July 2026 CIRs [6, 7, 8] update references to standards and technical specifications across other CIRs, is a testament of both the EDIF's adaptability to technical developments, and the long time it takes to provide legal clarity, considering that they come just half a year before the December 2026 deadline. The same can be said for the publication of Conformance tests in the ARF in July 2026.

National certification schemes play another key role herein: many will likely not be ready by December 2026. While not waiting for the EU-wide cybersecurity certification framework means that EUDIW adoption can move forward, the national certification frameworks do increase risks of fragmentation, and raise compliance complexity and costs if the European framework would require recertification [65].

5.3 Privacy and democratic concerns

At present, multiple privacy concerns of the EDIF remain. *To be elaborated.* While privacy-enhancing technologies (PETs) such as zero-knowledge proofs can mitigate some privacy issues, others are inherent to certain functionalities and use cases envisioned under the EDIF [11, 59]. Issues include linkability, identifiability, and excessive disclosure [11], as well as discrimination and profiling [59], and exclusion of people lacking sufficient income or capable devices [59, 13]. User binding and sole control, i.e. making sure that proofs about a person can only be provided by this person upon their discretion, remain relevant challenges herein [21, 58]: biometrics provide an unparalleled level of assurance [72, 58], yet incur severe privacy concerns [13, 58].

NGO epicenter.works has been closely following (draft) CIRs and outlined multiple instances of CIRs walking back earlier privacy protections. For instance, eIDAS2 art. 5a(16) dictates that the technical framework of EUDIWs must *not allow* linkability and traceability, whereas CIR 2025/1569 [5] and the recently adopted CIR 2026/1735 [8] that slightly amends the former, only prescribe *"hindering"* (art. 4(4)), which is a weaker protection [29]. In another example, the Parliament was assured during trilogue that EUDIWs would not inherently contain biometrics, so they agreed on dropping legal provisions against this. However, with the recently adopted CIRs, States must issue user portraits that can be used as optional fields unless users opt out [30]. The right to use pseudonyms as defined by eIDAS is also undermined in more recent CIRs [30, 29]. Besides an issue for privacy, these contradictions also undermine democratic policymaking by violating the EU law principle of hierarchy of norms; and conflicting with promises made to the Parliament in the ordinary legislative procedure whereas the Parliament is barely involved in enacting CIRs [31].

On the plus side, the organisation celebrates that the CIR requires registration certificates for relying parties, to prevent parties asking more attributes from users than they need; which *"would not have happened without sustained pressure from civil society and a coalition of member states"* [30]. While this could be considered a testament to public engagement positively impacting the eventual regulations, it proved insufficient to resolve all points they contend.

5.4 Reliance on Google and Apple

Another contestation is the reliance of EUDIWs on Google and Apple, as it centres big American tech companies with questionable privacy practices and significant market power at the heart of digital identity [62, 1, 10]. Many implementations (including national wallets from France, Germany, Italy, and The Netherlands) use their libraries to verify that the device generating an attestation is trustworthy and not tampered with (e.g. Google Play Integrity, Apple App Attest) . The EC claims that the ARF does not prescribe to use these services over platform-agnostic alternatives [71, 22], though the Italian developers think that is actually the case [18]. While countries such as the Netherlands refer to this as *"will be looking into these alternative measures, evaluate their security and implement them, if they are deemed reliable, before the NL Wallet goes into production"* [10], the question is whether they can do so under the looming December 2026 deadline.

6 Conclusion

This paper investigated: *How does the EDIF's "agile" regulatory process affect issues of privacy, fragmentation, legal certainty, and democratic accountability?* Following an evaluation of eIDAS1, the EU set out to do a better job at fostering harmonisation across MSs and keeping up with technological, scientific, market, social and legal developments with its *"agile"* EDIF. While the EDIF indeed

features many principles of agile or adaptive regulation proposed by both the eIDAS1 evaluation and academic literature, these principles have also stirred critiques of the legal framework. The agile nature undermines the effectiveness of traditional checks and balances, by reducing transparency (e.g. concerning technical standards and the EDICG) and amplifying the Commission's executive power.

The EDIF constitutes what may be called a *moving* 'big, hairy, audacious goal'. Citizens, journalists, academics, NGOs, and organisations that want to or must operate within this ecosystem, or hold others herein to account, must reckon with highly technical and frequently updated policy documents and standards. Thus, analyses run the risk of quickly becoming outdated; verifying whether this is the case puts a burden on these generally already strained actors. Another consequence is legal uncertainty for companies wishing to offer or having to facilitate trust services.

Furthermore, privacy discussions remain open. Thorny matters include the use of biometrics for user binding and sole control, linkability, the right to use pseudonyms, discrimination and exclusion. Optimistically, the agile nature provides opportunity to resolve these issues; but it has also proven to cause them, with recent CIRs undercutting protections offered in trilogue and by eIDAS2.

A final major pain point is the reliance of EUDIWs on Google and Apple. While some countries have expressed this to be temporary, it remains to be seen whether these temporary fixes do not become permanent.

All in all, while no hard claim can be made, these ongoing contestations beg the question whether the EU felt comfortable with setting the – what now appears to be a premature – deadline for wallet availability across MSs in December 2026; knowing it could hammer out technical and policy details even after adoption the EDIF in the ordinary legislative procedure. Further research with policy experts at national and EU level could set out to test that hypothesis. Until then, to what extent the EDIF will achieve its goals of harmonisation and interoperability while protecting fundamental rights, remains to be seen.

Disclosure of Interests. This study was conducted with a general grant from the Dutch Ministry of the Interior and Kingdom Relations supporting TNO's research on the Dutch national EUDI certification scheme. The views expressed are the author's own and have not been discussed with the Ministry prior to submission.

Bibliography

[1] Do not add Google Play Integrity integration · Discussion #19, https://github.com/eu-digital-identity-wallet/av-doc-technical-specification/discussions/19

[2] Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by Member States of the Commission's exercise of implementing powers (Feb 2011), http://data.europa.eu/eli/reg/2011/182/oj

[3] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) (Apr 2019), http://data.europa.eu/eli/reg/2019/881/oj

[4] Commission Implementing Regulation (EU) 2024/2981 of 28 November 2024 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and the Council as regards the certification of European Digital Identity Wallets (Nov 2024), http://data.europa.eu/eli/reg_impl/2024/2981/oj

[5] Commission Implementing Regulation (EU) 2025/1569 of 29 July 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards qualified electronic attestations of attributes and electronic attestations of attributes provided by or on behalf of a public sector body responsible for an authentic source (Jul 2025), https://eur-lex.europa.eu/eli/reg_impl/2025/1569/oj/eng

[6] Commission Implementing Regulation (EU) 2026/1730 of 15 July 2026 amending Implementing Regulation (EU) 2025/848 as regards applicable standards and specifications (Jul 2026), http://data.europa.eu/eli/reg_impl/2026/1730/oj

[7] Commission Implementing Regulation (EU) 2026/1731 of 15 July 2026 amending Implementing Regulations (EU) 2024/2977, (EU) 2024/2979, (EU) 2024/2980 and (EU) 2024/2982 as regards applicable standards and specifications (Jul 2026), http://data.europa.eu/eli/reg_impl/2026/1731/oj

[8] Commission Implementing Regulation (EU) 2026/1735 of 15 July 2026 amending Implementing Regulation (EU) 2025/1569 as regards applicable standards and specifications (Jul 2026), http://data.europa.eu/eli/reg_impl/2026/1735/oj

[9] European Digital Identity Wallet Toolbox (Feb 2026), https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/2.8.0/

[10] Incompatibility on operating systems not using Google Play Integrity · Issue #34 (2026), https://github.com/MinBZK/nl-wallet/issues/34
[11] Abellán Álvarez, I., Hölzmer, P., Schönrich-Sedlmeir, J.: Privacy evaluation of the European Digital Identity Wallet's Architecture and Reference Framework. Computers and Security **160** (Oct 2025). https://doi.org/10.1016/j.cose.2025.104707
[12] Abellán Álvarez, I., Hölzmer, P., Schönrich-Sedlmeir, J.: Privacy Evaluation of the European Digital Identity Wallet's Architecture and Reference Framework (May 2025), https://papers.ssrn.com/abstract=5248779
[13] Agencia Española de Protección de Datos: eIDAS2, the EUDI wallet and the GDPR (V) | AEPD (Jul 2026), https://www.aepd.es/en/press-and-communication/blog/eidas2-the-eudi-wallet-and-the-gdpr-v
[14] Almond, S., Broekaert, K.: Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators. Tech. rep., World Economic Forum, Geneva, Switzerland (Dec 2020), https://www3.weforum.org/docs/WEF_Agile_Regulation_for_the_Fourth_Industrial_Revolution_2020.pdf
[15] Appeal Committee: Rules of procedure for the appeal committee (Regulation (EU) No 182/2011) (Mar 2011), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32011Q0624(01)
[16] Armstrong, H., Gorst, C., Rae, J.: Renewing Regulation: 'anticipatory regulation' in an age of disruption. Tech. rep., Nesta (Mar 2019), https://www.nesta.org.uk/report/renewing-regulation-anticipatory-regulation-in-an-age-of-disruption/
[17] Bennear, L.S., Wiener, J.B.: Adaptive Regulation: Instrument Choice for Policy Learning over Time. Tech. rep., Harvard Kennedy School of Government (Feb 2019), https://www.hks.harvard.edu/sites/default/files/centers/mrcbg/files/Regulation%20-%20adaptive%20reg%20-%20Bennear%20Wiener%20on%20Adaptive%20Reg%20Instrum%20Choice%202019%2002%2012%20clean.pdf
[18] Bognolo, L.: Please remove the requirement for Google Play Integrity · Issue #287 (Jun 2025), https://github.com/eu-digital-identity-wallet/eudi-app-android-wallet-ui/issues/287
[19] Bradford, A.: The False Choice Between Digital Regulation and Innovation. Northwestern University Law Review **19**, 377–453 (Oct 2024), https://scholarship.law.columbia.edu/faculty_scholarship/4548/
[20] Brass, I., Sowell, J.H.: Adaptive governance for the Internet of Things: Coping with emerging security risks. Regulation & Governance **15**(4), 1092–1110 (Jul 2020). https://doi.org/10.1111/rego.12343, https://onlinelibrary.wiley.com/doi/abs/10.1111/rego.12343
[21] Burt, C.: AEPD makes case for alternatives to EUDI Wallet, biometric authentication (Jul 2026), https://www.biometricupdate.com/202607/aepd-makes-case-for-alternatives-to-eudi-wallet-biometric-authentication
[22] de Rosa, P.: Do not add Google Play Integrity integration · Discussion #19 (Jul 2025), https://github.com/eu-digital-identity-wallet/av-doc-technical-specification/discussions/19

[23] de Rosa, P.: Architecture and Reference Framework Releases (Jul 2026), https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/releases#release-v3.0.0
[24] Duivenvoorde, B.: Consumer Protection in the Age of Personalised Marketing: Is EU Law Future-proof? European Papers **8**(2), 631–646 (Nov 2023). https://doi.org/10.15166/2499-8249/679, https://www.europeanpapers.eu/e-journal/consumer-protection-age-personalised-marketing
[25] eIDAS Committee: Rules of Procedure of the eIDAS Committee (Oct 2020), https://ec.europa.eu/transparency/comitology-register/core/api/integration/ers/rulesProcedure/C47300
[26] El-Taliawi, O.G., Goyal, N.: The Politics of Policy Robustness: A Central Paradox and Computational Review of Adaptive Policymaking. Public Administration and Development (Jan 2026). https://doi.org/10.1002/pad.70054, https://doi.org/10.1002/pad.70054
[27] ElZarrad, M.K., Lee, A.Y., Purcell, R., Steele, S.J.: Advancing an agile regulatory ecosystem to respond to the rapid development of innovative technologies. Clinical and Translational Science **15**(6), 1332–1339 (Feb 2022). https://doi.org/10.1111/cts.13267, https://onlinelibrary.wiley.com/doi/abs/10.1111/cts.13267
[28] ENISA: ENISA advances the certification of EU Digital Wallets (Apr 2026), https://www.enisa.europa.eu/news/enisa-advances-the-certification-of-eu-digital-wallets
[29] epicenter.works: Analysis and Amendments to the Implementing Acts 4 (rev8) (Mar 2026), https://epicenter.works/content/eidas-amendments-to-the-implementing-acts-batch-4-rev8
[30] epicenter.works: EU Digital Identity: The Law Cannot Fix What Technology Has Broken (Jun 2026), https://epicenter.works/en/content/eu-digital-identity-the-law-cannot-fix-what-technology-has-broken
[31] epicenter.works: Rejoinder: Reply Open letter concerning the latest batch of eIDAS Implementing Acts. Tech. rep., epicenter.works (Jun 2026), https://epicenter.works/content/response-and-rejoinder-eidas-open-letter
[32] European Commission: COMMISSION STAFF WORKING DOCUMENT Accompanying the document REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). Tech. Rep. SWD/2021/130 final, European Commission, Brussels, Belgium (Jun 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021SC0130
[33] European Commission: REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the evaluation of Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). Tech. Rep. COM/2021/290 final, European Commission, Brussels, Belgium (Jun 2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021DC0290

[34] European Commission: COMMISSION DECISION of 5.9.2024 establishing the European Digital Identity Cooperation Group and amending Commission Implementing Decision (EU) 2015/296 (Sep 2024), https://ec.europa.eu/newsroom/dae/redirection/document/109838
[35] European Commission: EU Digital Identity Wallet milestone reached as Commission adopts implementing regulations (Dec 2025), https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/844759146/EU+Digital+Identity+Wallet+milestone+reached+as+Commission+adopts+implementing+regulations
[36] European Commission: The European Digital Identity Regulation was created in a more agile way (Sep 2025), https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/915931909/The+European+Digital+Identity+Regulation+was+created+in+a+more+agile+way
[37] European Commission: A simpler and faster Europe: Communication on implementation and simplification. Tech. rep. (Feb 2025), https://commission.europa.eu/document/download/8556fc33-48a3-4a96-94e8-8ecacef1ea18_en?filename=250201_Simplification_Communication_en.pdf
[38] European Commission: 20260506 AGENDA_eIDAS Committee meeting (May 2026), https://ec.europa.eu/transparency/comitology-register/screen/documents/115252/1/consult
[39] European Commission: The Age Verification Manual (Feb 2026), https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/930450954/The+Age+Verification+Manual
[40] European Commission: An agile Digital Rulebook for the EU (Mar 2026), https://digital-strategy.ec.europa.eu/en/policies/digital-rulebook
[41] European Commission: Commission urges fast rollout of age verification app - European Commission (Apr 2026), https://commission.europa.eu/news-and-media/news/commission-urges-fast-rollout-age-verification-app-2026-04-29_en
[42] European Commission: eIDAS Committee Meeting, 18 June 2026 (Jun 2026), https://ec.europa.eu/transparency/comitology-register/screen/meetings/CMTD%282026%29986/consult
[43] European Commission: eIDAS Committee Meeting, 6 May 2026 (May 2026), https://ec.europa.eu/transparency/comitology-register/screen/meetings/CMTD%282026%29728/consult
[44] European Commission: EU Digital Identity Wallet Toolbox process (Jun 2026), https://digital-strategy.ec.europa.eu/en/policies/eudi-wallet-toolbox
[45] European Commission: EUDI Wallets Launchpad Event Report: Conclusionos & Key Takeaways (Mar 2026), https://ec.europa.eu/digital-building-blocks/sites/download/attachments/964167040/EUDI%20Wallets%20Launchpad%20-%20Event%20Key%20Takeways%20report.pdf

[46] European Commission: European Commission seeks participants for European Business Wallet Technical Work Sub-Group (Apr 2026), https://digital-strategy.ec.europa.eu/en/news/european-commission-seeks-participants-european-business-wallet-technical-work-sub-group
[47] European Commission: European Digital Identity Cooperation Group (Jun 2026), https://digital-strategy.ec.europa.eu/en/policies/european-digital-identity-cooperation-group
[48] European Commission: The European Digital Identity Regulation (Apr 2026), https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/915931811/The+European+Digital+Identity+Regulation?all=1#sec-6-regulations
[49] European Commission: Functional Conformance Assessment Framework (Jul 2026), https://conformance.eudi.dev/draft/
[50] European Commission: About the initiative (nd), https://ec.europa.eu/digital-building-blocks/sites/spaces/EUDIGITALIDENTITYWALLET/pages/694487832/About+the+initiative
[51] European Commission: Comitology (nd), https://commission.europa.eu/law/law-making-process/adopting-eu-law/implementing-and-delegated-acts/comitology_en
[52] European Commission: eIDAS Committee (nd), https://ec.europa.eu/transparency/comitology-register/screen/committees/C47300/consult?lang=en
[53] Fenwick, M.D., Kaal, W.A., Vermeulen, E.P.M.: Regulation Tomorrow: What Happens When Technology Is Faster than the Law? American University Business Law Review **6**(3), 561–594 (Jan 2017), https://digitalcommons.wcl.american.edu/aublr/vol6/iss3/1
[54] Henning, M.: Capitals at odds with Brussels over EU identity wallets (Jun 2026), https://www.euractiv.com/news/capitals-and-berlaymont-at-odds-over-eu-identity-wallet-details/
[55] Hernández, G., Amaral, M.: Case studies on agile regulatory governance to harness innovation: Civilian drones and bio-solutions. Tech. rep., OECD (Aug 2022). https://doi.org/10.1787/0fa5e0e6-en, https://www.oecd.org/en/publications/case-studies-on-agile-regulatory-governance-to-harness-innovation_0fa5e0e6-en.html
[56] Janssen, M., van der Voort, H.: Adaptive governance: Towards a stable, accountable and responsive government. Government Information Quarterly **33**(1), 1–5 (Jan 2016). https://doi.org/10.1016/j.giq.2016.02.003, https://www.sciencedirect.com/science/article/pii/S0740624X16300156
[57] Janssen, M., van der Voort, H.: Agile and adaptive governance in crisis response: Lessons from the COVID-19 pandemic. International Journal of Information Management **55**, Article 102180 (Dec 2020). https://doi.org/10.1016/j.ijinfomgt.2020.102180, https://linkinghub.elsevier.com/retrieve/pii/S0268401220309944
[58] Kjørven, M.E., Gjøsteen, K., Wærstad, T.L.: Safe and inclusive or unsafe and discriminatory? European digital identity wallets and the

challenges of 'sole control'. Computer Law & Security Review **60**, 106235 (Apr 2026). https://doi.org/10.1016/j.clsr.2025.106235, https://www.sciencedirect.com/science/article/pii/S2212473X25001075

[59] Knabenhans, C., Veitch, S., Raynal, M., Stadler, T., Chatel, S., Lueks, W., Troncoso, C.: On the (Privacy) Harms of the European Digital Identity Framework (2026), https://eprint.iacr.org/2026/867

[60] Kochenderfer, M.J.: Decision Making Under Uncertainty: Theory and Application. MIT Lincoln Laboratory Series, The MIT press (2015). https://doi.org/10.7551/mitpress/10187.001.0001, https://web.stanford.edu/group/sisl/public/dmu.pdf

[61] Koops, B.: Should ICT Regulation Be Technology-Neutral? In: Koops, B., Lips, A., Prins, J., Schellekens, M. (eds.) Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners, IT & Law Series, vol. 9, pp. 77–108. T.M.C. Asser Press, The Hague (2006)

[62] Lämmerhirt, D.: Waag Futurelab (Jun 2026), https://waag.org/en/article/european-digital-id-wallets-are-gift-google-and-apple/

[63] Lampoltshammer, T.J., Leitold, H., Schmidt, C., Zefferer, T.: Future Outlook and Research Ideas. In: Homburg, V., Lampoltshammer, T.J., Solvak, M. (eds.) From Electronic to Mobile Government, pp. 195–207. Springer Nature Switzerland, Cham (2025). https://doi.org/10.1007/978-3-031-64471-9_12, https://doi.org/10.1007/978-3-031-64471-9_12

[64] Lenz, J.: EUDI Wallet: How prepared are the various EU countries? (Apr 2026), https://www.namirial.com/en/blog/stories/status-check-eudi-wallet/

[65] Loutocký, P., Stupka, V., Kasl, F.: Certification of the EU Digital Identity Wallets and its Challenges in the Era of AI. In: 2025 MIPRO 48th ICT and Electronics Convention. pp. 1636–1641. IEEE, Opatija, Croatia (Jun 2025). https://doi.org/10.1109/MIPRO65660.2025.11131771, https://ieeexplore.ieee.org/document/11131771

[66] Manaila, V., Makaay, E.: EUDI Wallets – Only One Year to Launch: Where are the Member States at? (Dec 2025), https://www.signicat.com/blog/eudi-wallets-only-one-year-to-launch

[67] Marchau, V.A.W.J., Walker, W.E., Bloemen, P.J.T.M., Popper, S.W. (eds.): Decision Making under Deep Uncertainty: From Theory to Practice. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-05252-2, http://link.springer.com/10.1007/978-3-030-05252-2

[68] Marchau, V.A.W.J., Walker, W.E., Bloemen, P.J.T.M., Popper, S.W.: Introduction. In: Marchau, V.A.W.J., Walker, W.E., Bloemen, P.J.T.M., Popper, S.W. (eds.) Decision Making under Deep Uncertainty: From Theory to Practice, pp. 1–20. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-05252-2_1, https://doi.org/10.1007/978-3-030-05252-2_1

[69] Marsman, H., Sieders, J.: Expert Opinions on The State of the EU Digital Identity Wallet: 2026 Survey Report. Tech. rep., SonicBee (Jun 2026), https://www.sonicbee.eu/2026-state-of-the-eu-digital-identity-wallet-expert-survey-report/

[70] Maxwell, W.J., Bourreau, M.: Technology Neutrality in Internet, Telecoms and Data Protection Regulation. Computer and Telecommunications Law Review (1) (2014), https://www.hoganlovells.com/~/media/hogan-lovells/pdf/publication/201521ctlrissue1maxwell_pdf.pdf

[71] Miranda, P.: Require a platform-agnostic alternative, an Android or iPhone smartphone is not a reasonable requirement · Issue #577 (Jul 2025), https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/issues/577#issuecomment-3140422940

[72] NIST: SP 800-63A.5: Identity Verification (Jul 2020), https://pages.nist.gov/63A/verification/

[73] Nordic Co-operation: Nordic-Baltic ministers take important step towards introducing digital identity wallets (Nov 2025), https://www.norden.org/en/nyhet/nordic-baltic-ministers-take-important-step-towards-introducing-digital-identity-wallets

[74] OECD: Regulatory Experimentation: Moving Ahead on the Agile Regulatory Governance Agenda. OECD Public Governance Policy Papers 47, OECD (Apr 2024). https://doi.org/10.1787/f193910c-en, https://www.oecd.org/en/publications/regulatory-experimentation_f193910c-en.html

[75] Ojanen, A.: Technology Neutrality as a Way to Future-Proof Regulation: The Case of the Artificial Intelligence Act. European Journal of Risk Regulation **16**(4), 1440–1455 (Jun 2025). https://doi.org/10.1017/err.2025.10024, https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/technology-neutrality-as-a-way-to-futureproof-regulation-the-case-of-the-artificial-intelligence-act/B4B5FD9D31DEB2B7B31C5745C68032D1

[76] Ranchordás, S., van 't Schip, M.: Future-proofing legislation for the digital age. In: Ranchordás, S., Roznai, Y. (eds.) Time, Law, and Change: An Interdisciplinary Study, pp. 347–366. Hart Publishing (Apr 2020). https://doi.org/10.5040/9781509930968.ch-016

[77] Robinson, G., de Vries, S., Duivenvoorde, B.: Introduction: Future-proof Regulation and Enforcement for the Digitalised Age. European Papers **8**(2), 579–582 (Nov 2023). https://doi.org/10.15166/2499-8249/676, https://www.europeanpapers.eu/e-journal/introduction-future-proof-regulation-enforcement-digitalised-age

[78] Room, G.: Complexity, Institutions and Public Policy: Agile Decision-Making in a Turbulent World. Edward Elgar Publishing (Jul 2011). https://doi.org/10.4337/9780857932648, https://www.elgaronline.com/monobook/9780857932631.xml

[79] Rutkowski, A.M.: Recent Advancements in the Rights to Public Knowledge: Technical Standards. Tech. rep. (May 2026)

[80] Schrepel, T.: Adaptive Regulation. European Journal of Risk Regulation (Mar 2026). https://doi.org/10.1017/err.2026.10087, https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/adaptive-regulation/10984D9EE8FE563187E0F28AB31FA6EA

[81] van Zuuren, E.: Hoe borgen we het vertrouwen in EDI-wallets in Nederland? In: Meet up EDI – BLSP 21 Mei 2026, pp. 10–43. Netherlands Ministry of the Interior and Kingdom Relations, Utrecht, The Netherlands (May 2026), https://edi.pleio.nl/file/download/eccd007c-19dc-4545-81d1-0722ea809a53/20260521_-_Totaalpresentatie_Meet_up_EDI_-_BLSP_21_mei_2026_Utrecht.pdf

[82] Weigl, L., Reysner, M.: The Governance of the European Digital Identity Framework Through the Lens of Institutional Mimesis. Regulation & Governance (May 2025). https://doi.org/10.1111/rego.70032, https://onlinelibrary.wiley.com/doi/10.1111/rego.70032

[83] Weldon, M.N., Thomas, G., Skidmore, L.: Establishing a Future-Proof Framework for AI Regulation: Balancing Ethics, Transparency, and Innovation. Transactions: The Tennessee Journal of Business Law **25**(2), 253–416 (2024). https://doi.org/10.70658/4486-1457.1660, https://doi.org/10.70658/4486-1457.1660