Response to the Commission's call for evidence for the Digital Omnibus

Vienna, 14th of October 2025

Introduction

We want to thank the Commission for the opportunity to provide feedback in the call for evidence on the Digital Omnibus (Digital Package on Simplification)[1].

The current Call for Evidence on the Digital Omnibus appears to be guided by a misleading narrative. The recurring claim that Europe is stifling innovation and burdening businesses through excessive regulation in digital policy fields does not reflect reality. Regulation is too often made the scapegoat for deeper policy failures: missed opportunities in strategic funding[2], ineffective public procurement,[3] a widening digital skills gap[4], and a lack of long-term political vision. Blaming digital regulation may offer an easier and faster political win than addressing these structural challenges, but it does little to strengthen Europe's digital future.

In an increasingly digital society, well-crafted regulation is not a burden. It is a prerequisite for a secure and functional digital environment. The benefits of digitalisation, including a more inclusive society, technological innovation, and economic efficiency, can only be realised if people trust the technologies they rely on. That trust depends on the perception that data, infrastructure, and communications are protected from misuse, manipulation, and attacks.

These risks are not merely theoretical. Citizens across Europe already experience the consequences of insecure digitalisation: ransomware attacks on hospitals and municipalities, phishing campaigns targeting vulnerable populations, and serious vulnerabilities in everyday digital services. In the face of such growing threats, the appropriate policy response cannot be to "simplify" by lowering standards or weakening oversight. Instead, the solution is smart regulation, ensuring that security, accountability, and resilience remain at the core of Europe's digital transformation.

Good regulation in this context, however, does not mean increased bureaucracy. Rather, it means protection through clear responsibilities, enforceable standards, and stable mechanisms to reduce systemic risk. Properly designed regulation enables innovation by creating legal certainty, reducing market fragmentation, and fostering public trust. Simplification efforts that undermine these principles, such as weakening incident reporting requirements, reducing safeguards under the AI Act, or reopening the recently adopted eIDAS framework, would not strengthen Europe's competitiveness but rather erode the security and rights of its citizens. The stability of fundamental digital frameworks is essential to build confidence among users, businesses, and public institutions alike.

1 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14855-Digital-package-digital-omnibus- en
2 https://epthinktank.eu/2025/02/12/benefits-of-eu-strategic-investment-in-high-tech-digital-innovation/?utm_source=chatgpt.com
3 https://euro-stack.com/blog/2025/3/eu-procurement-for-open-source-digital-sovereignty-final
4 https://www.euractiv.com/video/code-to-competitiveness-how-can-digital-skills-power-europes-future/

This discussion also has a clear geopolitical dimension. European digital regulation, including the GDPR, NIS2, the AI Act, and eIDAS, was not developed in isolation but as a response to global technological dependencies and revelations of mass surveillance. Europe's regulatory approach represents an effort to assert digital self-determination and protect democratic values in an increasingly contested global digital space. Yielding to external pressures that promote deregulation risks deepening Europe's dependency on foreign technologies and undermining its strategic autonomy.

People want technology they can trust. Delivering that trust requires a digital policy framework that prioritises security, transparency, and fundamental rights, not deregulation. Europe should build on its regulatory successes and focus on effective implementation, enforcement, and coordination. The goal must be smarter regulation, not less of it.

Data Acquis

A crucial element in the current debate around the Digital Omnibus remains largely unaddressed: the General Data Protection Regulation (GDPR) itself. It is worth recalling that one of the key reasons for adopting the GDPR was the geopolitical context in which it emerged. **The Regulation was shaped by the revelations of mass surveillance of EU citizens by the U.S. National Security Agency[5],** and later reinforced by the Cambridge Analytica scandal in 2018, which starkly demonstrated the need for pan-European rules to protect personal data and, by extension, democratic processes[6].

It is therefore deeply concerning that, once again, geopolitical interests and pressure from the United States appear to be driving renewed attempts to question or weaken the GDPR. At present, policy making seems to be guided by short-term considerations rather than by long-term objectives, with the risk of further deepening Europe's digital dependency.

Instead of diluting the GDPR, the EU should reaffirm and strengthen the principles embedded within it. These principles could serve as the foundation for reducing dependence on dominant American technology corporations and for fostering European alternatives as well as the promotion of free and open-source software. In doing so, the often-invoked yet rarely substantiated concept of "technological sovereignty" would finally be given real substance.

Cybersecurity Incident Reporting

Cybersecurity incident reporting plays a crucial role in ensuring the security and resilience of Europe's digital infrastructure. Or to quote the European cybersecurity watchdog ENISA: "*Incident reporting is essential for understanding and analysing the EU cybersecurity threat landscape*[7]" It provides essential insights into systemic vulnerabilities[8], enables evidence-based policy making[9], and strengthens public trust in digital technologies.

A reduction or weakening of reporting requirements must not be seen as "simplification." Such an approach would not reduce complexity but rather increase insecurity. The absence of reliable and comprehensive incident data would leave policymakers, regulators, and the public blind to emerging

5 https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Fall%202019/CDR%20V4N2-Fall%202019_COYNE.pdf?ver=2019-11-15-104104-157
6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018IP0433
7 https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/threats-and-incidents
8 https://academic.oup.com/cybersecurity/article/11/1/tyaf019/8238596
9 https://www.sciencedirect.com/science/article/pii/S0740624X24000923

threats and trends. The World Economic Forum, in its *Global Cybersecurity Outlook 2025*[10], likewise underlines the importance of "*reinforcing ecosystem resilience through regulation*"[11] and emphasises that effective incident reporting fosters collaboration and a collective defence mindset, both of which are critical for addressing sophisticated and complex threats[12].

Already today, many organisations across Europe report being victims of cyberthreats[13], especially cyberfraud, with serious consequences for their operations, the economy, and societal trust in digital systems. Effective incident reporting mechanisms help to identify these risks early and enable coordinated responses.

Simplification efforts should therefore **focus on process efficiency**, not on lowering obligations. Measures such as **standardised formats**, **streamlined reporting channels**, or a **single point of contact** for multiple frameworks (e.g. NIS2, DORA, Cyber Resilience Act) can meaningfully reduce administrative burdens, while preserving the completeness and analytical value of reports.

In short: **fewer reports mean less security**. Europe needs better coordination and better data, not less transparency, to build a secure and trusted digital environment.

Smooth Application of the AI Act

Discussions about the "simplification" of the AI Act should be grounded in the current realities of its implementation. As of today, most EU Member States are delayed in establishing the national supervisory authorities required to oversee the Act's application. In many countries, no competent bodies are yet in place to enforce even the provisions already in force.

Against this backdrop, claims of "over-regulation" are clearly misguided. The real challenge lies not in excessive rules, but in insufficient enforcement and lacking institutional readiness. Without functioning oversight structures, the rights and safeguards established by the AI Act risk remaining purely theoretical.

Meanwhile, the societal impact of artificial intelligence, its benefits and harms alike, is already tangible. Several national examples demonstrate the urgent need for clear and enforceable EU-wide rules:

In **Austria,** police authorities have used ex-post facial recognition in connection with assemblies and protests without a clear legal basis or effective safeguards[14]. Despite repeated criticism from academia, civil society, and parts of the political spectrum, this practice continues to exist in a legal vacuum.
Recent incidents illustrate the risks: one climate activist was detained after a wrongful identification via facial recognition; in another case in 2023, **an innocent person was held in pre-trial detention for two months due to a false biometric match**[15].

In **Hungary**, civil society organisations and investigative journalists have documented the use of AI-assisted surveillance tools, including facial recognition and predictive policing, without sufficient transparency or judicial oversight[16]. Reports suggest that such technologies have been employed in politically sensitive contexts, raising serious concerns about abuse of power and lack of accountability.

10 https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf
11 Ibd page 27
12 Ibd page 32
13 https://resilienceforward.com/cyber-attacks-surge-21-globally-in-q2-2025-europe-sees-biggest-rise/
14 https://www.vol.at/data-protection-advocates-criticize-use-of-facial-recognition-at-climate-demonstration-in-vienna/9504071
15 https://www.derstandard.at/story/3000000215580/kampf-um-entschaedigung-nach-fehler-der-gesichtserkennung
16 https://www.liberties.eu/en/stories/hungary-facial-recognition-pride/45453

These cases underline the need for robust and uniform enforcement of the AI Act across the EU. Simplification must not be equated with deregulation: reducing compliance or lowering safeguards would only exacerbate the perils posed by high-risk AI systems.

A truly "smooth application" of the AI Act therefore requires Member States to establish independent supervisory authorities swiftly, allocate sufficient resources for enforcement, and ensure strong coordination at EU level. A credible implementation framework, not weaker rules, is key to ensuring that AI serves the people, democracy, and fundamental rights in Europe.

Rules on Cookies and Other Tracking Technologies

When the General Data Protection Regulation (GDPR) was adopted, it was always intended to be complemented by a dedicated ePrivacy Regulation providing specific safeguards for the confidentiality of electronic communications[17]. However, due to persistent lobbying by a small number of powerful industry actors[18], the adoption of this regulation was repeatedly delayed and ultimately blocked.

The resulting legal protection gap has left large parts of online communication insufficiently protected under EU law. Over the past years, the Court of Justice of the European Union has repeatedly intervened to clarify and strengthen individual rights in this area. While this jurisprudence has provided important guidance, judicial remedies cannot substitute the absence of a coherent, directly applicable legal framework.

It is therefore essential that the European Union continues its efforts to establish an ePrivacy Regulation that ensures comprehensive and harmonised protection for all forms of electronic communication.

It is unacceptable and cannot be justified that certain parts of online communication enjoy weaker protection simply because financially powerful publishing or advertising interests have managed to delay stronger privacy rules. Personal communication and metadata which often reveal highly sensitive information about an individual must not be treated as a commodity to be monetised at the expense of fundamental rights.

The Digital Omnibus initiative should therefore not be used to weaken the existing standards of the ePrivacy Directive, but rather to close the long-standing regulatory gap and to reaffirm the EU's commitment to ensuring strong, enforceable privacy rights in the digital environment.

eIDAS, Electronic Identification and Trust Framework and Business Wallet

No more Abandonment of Essential User Protections

We are concerned about potential deregulatory attempts in the recently adopted framework for the European Digital Identity Wallet. The eIDAS reform was concluded in May of 2024 and several important Implementing Regulations have been added to the framework. Member States are under a tight deadline to offer the EUDI Wallet to their citizens by the end of 2026. This is extremely unlikely to happen in many countries, particularly as the certification schemes for the Wallet have yet to be developed.

17 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52017PC0010&utm.com, Explanatory Memorandum Point 1.2

18 https://corporateeurope.org/en/power-lobbies/2018/06/shutting-down-eprivacy-lobby-bandwagon-targets-council

Any reform of the recently adopted rules would drastically add to the uncertainty and risk the stability of the whole project. Given the large investments required to meet the high IT-security and data protection standards, any legislative change by the European Commission at this point would further reduce the chances of a stable system that meets the deadline.

We have contributed significantly to the eIDAS reform since 2021[19]. While the adopted framework is not perfect, we would caution against renegotiating core user protections in the current political climate and under the framing of deregulation. Public trust in eIDAS is a vital success factor. Recent Implementing Regulations have already stripped citizens off essential protections by interpreting the right to use pseudonyms as only being applicable to logging into a service[20]. This choice by CONNECT.H.4 will lead to the Wallet becoming a dangerous tool for the proliferation of identity information to companies that fall under no obligation to identify the users (e.g. online services).

Further deregulatory attempts would break the neck of a system already faced with public backlash, unrealistic timelines and an increased risk of failure.

The importance of Relying Party Registration

The eIDAS regulation specifies in Article 5b an obligation for relying parties to register their intended use case of the Wallet including the attributes they intend to request from the users. The relying party is prohibited from requesting information going beyond what they registered. EUDI Wallets are required to warn the user about requests going beyond what is specified in the relying party registration certificate.

According to the call for evidence, the European Commission considers to "reduce compliance costs while keeping the same standards, and enhance legal clarity for key actors involved in European Digital Identity Framework, including relying parties".

The current framework of Article 5b was proposed under the French Council Presidency and found broad support in both Council and Parliament. It is a vital safeguard against the risk of over-asking and over-identification via the EUDI Wallet. Without the transparent registry of use cases and requested attributes too much burden would be placed on the user to decide about the proportionality of each and every request for their information.

Simply put, the European Digital Identity Wallet would become a dangerous tool of which data and consumer protection organisations would have to warn citizens and caution to better not use. The Wallet cannot be a trusted platform for the most sensitive identity, health and financial data, if anyone can request information going far beyond what is proportionate and legal for any given purpose. Europeans seem to have taken on the general habit to simply click 'okay' and 'yes' whenever faced with data protection questions, for example in the context of cookie banners. Since an ex-post regime has the known pitfalls and limitations in the GDPR enforcement, the Wallet would become a tool far too dangerous for most users to use safely.

Limit Business Wallet to B2B and B2G interactions

The upcoming proposal for a European Business Wallet should be clearly limited in scope to only apply to business to business (B2B) or business to government (B2G) interactions. Natural persons who fall under the GDPR should be excluded from the proposal. This would not just simplify the process but also help with the expedient roll-out of such a system.

19 https://epicenter.works/en/thema/eid-digital-public-infrastructures
20 https://epicenter.works/en/content/eidas-amendments-to-the-implementing-acts-batch-1-2-rev3

Hence, we are worried about what is intended with the 'one in, one out' principle being applied to the European Business Wallet and would like to reiterate how perilous any further reform on the eIDAs framework would be for natural persons.

Sincerley ,

epicenter.works – for digital rights