Submission of the European Digital Rights (EDRi) network to the European Commission's call for evidence on "Simplification – digital package and omnibus"

Brussels, 14 October 2025

This submission has been prepared by the EDRi office. We are grateful to our network for their work and reviews, which form the basis of this submission, and in particular the inputs from: Access Now, Danes je nov dan, Electronic Frontier Norway (EFN), the European Center for Not-for-profit Law (ECNL), epicenter.works, IT-Pol (IT-Political Association of Denmark). Additionally, we are grateful to our partner AlgorithmWatch for their contribution.

EDRi is Europe's biggest network of over sixty civil society groups working together for the protection of human rights in the digital age. Whilst EDRi has always called for clear, coherent and enforceable tech and data laws, **we are extremely concerned that the Commission's "simplification" push will undermine the EU's digital acquis and erode the legal certainty and vital protections it provides**. On 1 October, Commission President Ursula von der Leyen confirmed that the Commission's simplification agenda is, as feared, a political push for "deregulation".

Along with 470 other public interest actors across environmental, corporate accountability, workers' rights, non-discrimination policy and more, EDRi has warned that **the broad "simplification" agenda will weaken trust in the EU's democratic framework** at a time when threats from corporations and state actors are at an all-time high. It would also signal that the EU is letting itself be driven by corporate interests, instead of putting people and society at its heart.

The ePrivacy Directive and the General Data Protection Regulation (GDPR) provide a foundation for people's personal data and information to be shared only if and when they choose – ensuring dignity and autonomy in a digitalised world. They protect our private conversations and prevent arbitrary surveillance by private and public entities, providing essential checks-and-balances against powerful interests. Whilst their benefits and ambitions have not yet been fully realised, we see time and again that this is a problem of resources and political will for enforcement.

Building on the ePrivacy and GDPR's gold-standard foundation, more recent laws such as the Artificial Intelligence Act have taken further steps towards making the fundamental rights to privacy and data protection (Articles 7 and 8 of the EU Charter) a tangible reality in an increasingly digitalised world. **Without even being fully in force, EDRi is alarmed that the Commission would undermine the will of the co-legislators by already reopening this law**. Similarly, the Data Governance Act (DGA) remains relatively novel.

EDRi therefore expresses our disappointment that the Digital Omnibus – and the broader digital package – could be set to undermine the democratically-agreed guardrails that the EU has spent the last decade building up – especially as the call for evidence explains that the omnibus is only "a first set of measures". The "simplification" of the data acquis, read alongside the broader digital simplification package (e.g. midcaps omnibus), suggests **a willingness from the Commission to reopen core fundamental rights protections**.

We additionally perceive that with the many Omnibuses, the Commission seems to be taking an arbitrary approach focused on the volume of laws, rather than their quality. Extremely short consultation timelines, "reality checks" aimed at industry, and a systematic lack of impact assessments, cast a shadow on the democratic legitimacy of the process. Perhaps most alarmingly, **this call for evidence for the Digital Omnibus states that there will be no negative impact upon fundamental rights, despite reopening laws with serious rights impacts**.

As research has shown, the EU's digital laws have had a huge social and economic benefit for Europe. The Commission's lack of aspiration and boldness to protect digital regulation is therefore more than just disappointing – it puts 500 million people at risk of increased privacy, data protection, equality and security breaches.

Whilst it is undeniable that the EU digital framework needs improvement, there are many things that could help foster regulatory compliance, such as better guidance. Instead of allowing corporations to set the agenda, the Commission should focus on enabling access to justice for individuals and communities that have been harmed.

1. “The data acquis (Data Governance Act, Free Flow of Non-Personal Data Regulation, Open Data Directive)”

EDRi is concerned that the proposal to merge the Open Data Directive (ODD) and Chapter II of the Data Governance Act (DGA) risks blurring the essential distinction between *open by default* datasets and *protected by default* datasets. This distinction must remain intact and therefore should not be in the scope of any Omnibus: non-confidential data may be openly re-used, while access to confidential or personal datasets must remain exceptional, subject to specific necessity and proportionality assessments, and strong safeguards.

Because the Digital Omnibus is expected to address interlinked data laws, the weaknesses already visible in the DGA illustrate how poor alignment between instruments can undermine the GDPR’s coherence in practice. We further highlight that weaknesses in the current DGA framework could undermine the GDPR in practice, even though it is *prima facie* outside of the scope of the Digital Omnibus. In the DGA, consent provisions are vague and use inconsistent terminology (‘permission’ instead of ‘consent’); purpose limitation is not properly safeguarded; mixed datasets lack clear rules; and protections after data leaves the public body remain undefined. Anonymisation is presented as a safeguard, yet when applied robustly it often renders datasets unusable. The DGA compounds this problem by creating an exception if anonymisation would make data ‘useless,’ which risks incentivising weaker safeguards and raising reidentification risks.

These DGA shortcomings are a cautionary example of how simplification and inconsistent terminology can erode data protection in practice. Similar deregulatory changes under the Omnibus would therefore risk the same outcome.

Public authorities designated with oversight of these laws and of broader data protection rules also face resource gaps that purported “simplification” could worsen. Expanding reuse obligations for data, without providing funding, expertise, or tools, simply transfers risk onto under-resourced bodies. This will make the process less simple. Instead, the European Commission should focus on enabling and resourcing these bodies.

True simplification would harmonise procedures and reduce fragmentation, but only with explicit alignment to GDPR, additional resources for public bodies, and robust fundamental rights and environmental impact assessments. Given the current deregulatory landscape, the plans for more digital “simplification” and the Omnibuses proposed by the Commission thus far in 2025, we fear that this is not the aim of the Digital Omnibus.

Evidence:

- See the following paper, which further evidences the insufficiencies of the data acquis : da Rosa Lazarotto, B., Trigo Kramcsák, P., Chomczyk Penedo, A., & Stalla-Bourdillon, S. (2025). The Future of Data Governance in the EU: A response to the Call for Evidence on the Data Union Strategy Initiative. (1 ed.) Brussels Privacy Hub Working Papers. https://brusselsprivacyhub.com/wp-content/uploads/2025/07/White_Paper_Response-to-the-Public-Consultation-A-European-Data-Union.pdf.

2. "Rules on cookies and other tracking technologies laid down by the ePrivacy Directive"

Article 5(3) of the ePrivacy Directive is a cornerstone of the EU's digital rights framework. It protects two distinct but interlinked Charter rights - privacy and the confidentiality of communications - by requiring prior consent for any storage of or access to information on a user's device, unless this is strictly necessary to provide a service explicitly requested by the user. The provision is not just about cookies. It applies to tracking in all its forms, including fingerprinting, device identifiers, Software Development Kits (SDKs), and emerging server-side techniques on the company's own infrastructure, aimed at circumventing consent requirements. Without this rule, the integrity of devices and the confidentiality of communications would be left exposed to covert surveillance from both state and commercial actors.

Article 5(3) of the Directive has always functioned as *lex specialis* to the GDPR. The GDPR regulates the processing of personal data before and after storage in devices, but it does not regulate the very act of accessing devices. Article 5(3) also applies to non-personal data which means that controllers cannot circumvent the provision by arguing that identifiers are not 'personal' until linked to other datasets, escaping safeguards in the meantime.

But ePrivacy is more than a technical carve-out. It protects a distinct right: the privacy and confidentiality of communications, which applies regardless of whether the information in question is personal data. Article 5(3) applies even when the information accessed is not personal data, because the core guarantee is the inviolability of the device and of communications themselves.

This makes ePrivacy both a specialised layer of data protection law and an independent constitutional safeguard, historically rooted in the secrecy of correspondence and designed to constrain both commercial actors and state authorities. Diluting Article 5(3) under the guise of 'alignment' with GDPR therefore risks hollowing out protections that were deliberately set at a higher level for communications privacy. Attempts to introduce legitimate interest as a legal basis for device access would invert the logic of the

provision: people would no longer be able to prevent interference *ex ante* but would be left only with an *ex post* right to object to this most intrusive invasion of their digital private life.

Genuine simplification is very different from deregulation, whereas any weakening of Article 5(3) would clearly deregulate the EU's privacy acquis and must be opposed. Claims of "consent fatigue" are misleading. What frustrates people is not the act of giving consent but the manipulative design of banners that pressure them to accept tracking.

The solution is not to weaken consent requirements, but to enforce the legal standard properly and to operationalise tools already foreseen in EU law. Recital 66 of Directive 2009/136/EC amending Article 5(3) to its current form and Article 21(5) GDPR both anticipate automated, technical specifications that allow people to exercise their choices globally (i.e. without having to click 'accept' or 'reject' for every single website they visit). Binding privacy signals of this kind would eliminate cookie banner overload, reduce compliance costs, and give regulators a clear enforcement benchmark. This would amount to a genuinely simpler and rights-respecting experience for people in the EU, whereas the Digital Omnibus seems set to reopen core protections.

Exemptions to Article 5(3) are the most serious risk. Any broadening of carve-outs would quickly become a Trojan horse for invasive practices. Proposals for exemptions under 'statistics' or 'audience measurement' are particularly dangerous, because they would legitimise forms of tracking that are already central to the surveillance advertising economy. If exemptions are considered at all, they must be exhaustively-defined and strictly limited to genuinely innocuous, first-party analytics without persistent identifiers, cross-website tracking, sharing, or profiling, and with very short retention periods.

The dysfunction of today's online environment stems not from the standard being too strict, but from inconsistent enforcement and fragmented national transpositions. This has allowed systemic non-compliance to become normalised, eroding trust in EU law. Addressing the so-called 'cookie fatigue' is not about playing whack-a-mole with banners or lowering standards that we all rely on to be safe and secure online. It requires a multi-pronged approach: consistent enforcement against unlawful practices, clear bans on deceptive design in consent interfaces, and regulation of the adtech ecosystem that drives the proliferation of trackers.

True modernisation of the ePrivacy rules should therefore mean closing enforcement gaps, embedding legally-binding privacy signals, and ensuring that any change is subject to a thorough Fundamental Rights Impact Assessment. Anything short of this will only make access to rights and justice more complicated for the 500 million people across the EU.

Evidence:

- EDPB, Guidelines 2/2023 on the Technical Scope of Article 5(3) ePrivacy Directive (7 Oct 2024); Danish Agency for Digital Government, Who is Tracking EU Citizens, and How? (Dec 2024) https://digst.dk/media/txae4k4u/who-is-tracking-eu-citizens-and-how-wcag.pdf. These two documents clarify that Article 5(3) applies to all forms of device access - not just cookies - and empirically demonstrate the widespread, covert tracking practices that such protection is meant to prevent.
- EDRi, Targeted Online: An industry broken by design and by default (2023) https://edri.org/wp-content/uploads/2021/03/Targeted-online-An-industry-broken-by-design-and-by-default.pdf; Karegar, Santos et al., Dark Patterns in Cookie Banners: Emotions, Framing and User Decision Making (2022). Together they document how deceptive interface design manipulates users into consenting to tracking, showing that so-called 'consent fatigue' stems from unlawful design, not from the legal standard itself.
- Nouwens et al., 'Dark Patterns After the GDPR' (2020) Proc. CHI Conf. on Human Factors in Computing Systems; Bielova, Santos & Gray, 'Two Worlds Apart! Closing the Gap between Regulating EU Consent and User Studies' (2024) Harvard J.L. & Tech. 37(3) 1296–1332; Gray et al., 'Dark Patterns and the Legal Requirements of Consent Banners' (2021). These interdisciplinary studies bridge legal analysis and user-experience research, providing robust evidence that most consent banners violate GDPR and ePrivacy requirements through manipulative design.
- Degeling et al., '(Un)informed Consent: Studying GDPR Consent Notices in the Field' (2019) Proc. ACM on Human–Computer Interaction 3(CSCW) 1–23; Utz et al., '"This Website Uses Cookies" – Users' Perceptions and Reactions to the Cookie Disclaimer' (2019) Computers in Human Behavior 97 206–217. These early empirical studies establish that most users neither read nor understand consent banners, highlighting the structural impossibility of informed consent within current adtech interfaces.
- Santos & Pandit (2022), How could the upcoming ePrivacy Regulation recognise enforceable privacy signals in the EU? This paper outlines a concrete legal and technical framework for recognising privacy signals such as Global Privacy Control as binding expressions of consent or refusal, offering a credible path to genuine simplification.
- Bielova, Santos & Gray (2024) at 1328–1331; EDPB, Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces (v 2.0, 14 Feb 2023). Both sources define and classify manipulative digital design, providing the regulatory and empirical foundation for banning deceptive consent interfaces under EU fundamental-rights law.
- Berjon (2021), GPC under the GDPR https://berjon.com/gpc-under-the-gdpr/. This paper demonstrates how Global Privacy Control signal can operate legally within the GDPR as an automated means of exercising the right to object or withdraw consent, validating its recognition in EU law.

- AWO (2023), Study on the Impact of Recent Developments in Digital Advertising https://op.europa.eu/en/publication-detail/-/publication/8b950a43-a141-11ed-b508-01aa75ed71a1/. This EU-commissioned study evidences how recent adtech practices blur boundaries between measurement and profiling, reinforcing the need to preserve strict consent requirements under Article 5(3) ePrivacy.

3. "Cybersecurity related incident reporting obligations"

When addressing incident and breach reporting obligations under the Network and Information Security Directive (NIS 2) and the GDPR, it is essential to ensure that the distinct purposes of these frameworks are respected. The GDPR sets out clear, risk-based duties to notify supervisory authorities and, where necessary, affected individuals when personal data are compromised. This mechanism is central to the protection of fundamental rights and freedoms in the digital environment. By contrast, NIS 2 reporting is focused on system integrity and resilience. These are complementary but not identical functions, and it is vital that the Digital Omnibus does not collapse them into one. This would not be "simpler", but would in fact erode or obfuscate core protections and avenues for redress, which we see as a key risk in this part of the Omnibus.

The Commission's call for evidence refers to streamlining compliance and the use of reporting tools. While genuine simplification and harmonisation could in theory reduce administrative overhead, there is a risk that excessive integration (for example through a single reporting tool or entry point, as suggested by some stakeholders) could blur the line between cybersecurity incidents and data breaches, thus deregulating core protections. If reporting systems are designed primarily around technical incidents, they risk downgrading the GDPR's human rights-centred safeguards. At the same time, directing all notifications through one channel could overwhelm supervisory authorities with reports outside their mandate, while depriving them of timely, targeted information they need to enforce Articles 33 and 34 GDPR. This again points to the fact that sufficient methods of and resources for compliance and enforcement are lacking, rather than the original laws themselves.

A more proportionate approach would be to pursue interoperability between reporting processes, not merge them. Interoperability means aligning the systems so that relevant information can flow efficiently between competent authorities without changing the underlying legal duties. This approach could avoid double reporting while keeping the safeguards and enforcement channels distinct, focusing instead on coordination and technical alignment and thus helping organisations comply more easily while preserving the integrity of the GDPR's rights-based system and the NIS 2's focus on network resilience.

Without reopening the core protections, these processes can be better aligned so that organisations do not need to duplicate work, while maintaining distinct gateways to

ensure that supervisory authorities continue to receive what they require under the GDPR. This would strike a better balance between easing specific compliance processes for businesses and upholding the EU's commitment to protect fundamental rights.

Evidence:

- See the EDPB Guidelines 9/2022 on personal data breach notification under GDPR. Version 2.0. Adopted 28 March 2023 https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en, which clarify how personal data breach notifications must be assessed and reported under the GDPR, providing a concrete benchmark for ensuring that any interoperability with NIS 2 reporting preserves the GDPR's distinct, rights-based purposed and procedural safeguards.

4. "The smooth application of the AI Act rules"

The AI Act is an important step towards the rights-respecting use of AI in the EU. While it contains several grave loopholes when it comes to the protection of fundamental rights — particularly in the areas of policing and migration — it nevertheless presents an important system of checks, balances and red lines against the most harmful uses of AI. Rolling back or delaying the Act before it is even fully implemented will impede any crucial improvement on rights protections. It will also damage the credibility of the law, the lawmaking process and the Commission as an oversight entity, as any law's effectiveness and strength lies in its strong enforcement and good implementation.

Further, the AI Act is not yet fully in force, meaning that we do not yet have meaningful evidence of its impact nor of any possible shortcomings. The EU's commitment to Better Regulation requires a fact-based assessment of laws, whereas any changes that could be made at this stage can be merely hypothetical and not fact-based.

We are concerned that the proposed "simplification" measures will exacerbate the issues that they claim to resolve, and instead create more barriers to people's timely access to their rights. Adhering to the implementation timeline and process laid down in the Act, as well as predictable and strong enforcement, are the basis for legal certainty, as companies and public authorities have been preparing for the AI Act for more than a year, including developing processes and safeguards in line with the Act. Potentially pausing or rolling back parts of the AI Act in the middle in the implementation and enforcement phase would create legal uncertainty and more complexity for everyone. Proposed "simplification", without evidence-based evaluation of existing measures, creates more uncertainty for businesses and may even "punish" early adopters of legislation, creating a dangerous precedent for the future. With many EU companies having invested significant resources in preparing for the Act, European industry may

have the most to lose from AI deregulation. What businesses and public authorities need instead is clear, relevant and thorough guidance.

Whilst some stakeholders have complained that the AI Act will stifle innovation, it is clear that many of the AI Act's key requirements will help providers and deployers to avoid infringements of fundamental rights, avoid breaking other laws (such as the GDPR or the Law Enforcement Directive), and guide them through basic due diligence processes that will lead to better products and services with fewer unforeseen risks.

Additionally, Member states are well underway with the implementation of the AI Act and the establishment of national authorities, with some having passed national legislation in recent weeks and others on the verge of doing so. Any changes to relevant obligations under the AI Act or to the law's implementation timeline would potentially create different regimes or zones of exceptions within EU, creating more complexity, uncertainty and undermining the central objective of harmonisation.

Lastly, as the EU's standards watchdog, ANEC, has emphasised, there is a serious risk that delays to the development of AI Act standards is being used to justify a postponement of the Act's implementation. Such a delay would run contrary to the rights protections and redress framework that the law promises. Standard-setting is also a process outside the democratic control of the co-legislators, with an ongoing ombudsperson complaint against the Commission due to lack of transparency and industry over representation. Hence, delays can end up being self-fulfilling prophecies for stakeholders that want to see the AI Act weakened.

Evidence:

- **The European Agency for Fundamental Rights Report on Artificial intelligence and fundamental rights**, https://fra.europa.eu/sites/default/files/fra_uploads/fra-2020-artificial-intelligence_en.pdf. This report clearly points towards the varied fundamental rights implications of the use of Artificial Intelligence across sectors and use cases in Europe and the need for an AI Act to fill legislative gaps. Additionally it shows the essential role of fundamental rights impact assessments (FRIAs) when using AI systems – a key novelty enshrined in the AI Act.
- **Public opinion polls also show the strong public support for legislative protections against AI harms**. In a public opinion poll across 12 EU countries conducted in 2022, the majority of people expressed being concerned about the fundamental rights impact of AI across all areas of public life (https://ecnl.org/news/new-poll-public-fears-over-government-use-artificial-intelligence). Another public opinion poll across Spain, Germany and France shows that the overwhelming majority of people believe that EU tech rules should be enforced as they are, even amidst geopolitical pressure. This is particularly relevant with respect to the geopolitical pressure that has been

exercised on the AI Act by third countries. Third, the 2025 IPSOS AI monitor shows that more than half of people are nervous when using AI across most studied EU countries. These polls speak to the necessity of laws which center people's rights to privacy and non-discrimination in the context of AI.

- **Recent breaches of the AI Act.** Recent breaches of a key provision of the AI Act on the use of real-time Remote Biometric Identification (RBI) have garnered far reaching public criticism, specifically at the banned Pride in Budapest earlier this year. This shows the wide support and how essential and well-supported fundamental rights safeguards in AI legislation are:
  - In an attack on the EU fundamental rights of freedom of peaceful assembly and freedom of expression, Hungary's Parliament passed a package of amendments banning and criminalising Pride marches and their organisers, and permitting the use of real-time facial recognition technologies for the identification of protesters, which marks a significant infringement on privacy and personal freedoms. This amendment is in violation of key provisions of the AI Act laying down applications of AI that are fundamentally incompatible with fundamental rights. Having failed to fully rule out all biometric mass surveillance practices, the AI Act has already created a perceived margin of discretion which has legitimised the use of RBI in Hungary. Any weakening or delay of the AI Act would only widen this grey area and make it more likely that we would see rights-violating deployments of AI, in contradiction to the will of the co-legislators.
  - In Austria, police authorities have made use of ex-post facial recognition in connection with assemblies and protests. These measures have been applied without an explicit statutory basis and in the absence of effective safeguards, despite repeated criticism from academia, civil society, and parts of the political sphere and the forthcoming entry into force of the AI Act's restrictions on ex-post RBI. The legal uncertainty surrounding biometric surveillance in Austria has created a situation where fundamental rights are exposed to disproportionate risks. Several recent incidents highlight the dangers of this practice. In one case, a climate activist was detained after being identified via facial recognition, although no criminal offence had been committed. In another, in 2023, a person was wrongfully imprisoned for two months due to a faulty facial recognition match. To avoid the continuation of this legal uncertainty, it is vital that the AI Act's full provisions enter into force as initially foreseen.
  - These examples from Hungary and Austria underscore the urgent need for the timely implementation of harmonised and enforceable EU rules on biometric technologies and AI in order to clearly and consistently rule out practices that would amount to AI-charged mass surveillance. What's more, the timely implementation and enforcement of the AI Act would increase the safeguards, transparency, accountability and redress measures (including financial penalties) for the use of AI which are sorely needed.

- **The AI Act helps companies to comply with Charter**. The prohibitions in Article 5 of the AI Act are there to clearly outlaw the most egregious violations of fundamental rights that can occur through the use of AI systems (such as biometric categorisation which seriously undermines people's right to non-discrimination). This has not created a new legal standard, but rather applied well-established fundamental rights protections to the specific context of AI. By directly prohibiting such dangerous practices, the AI Act can be seen to help stop providers and deployers of AI systems from being involved in some of the most serious infringements of fundamental rights and thereby spare them from significant legal consequences and reputational risk.
- **Similarly, the requirements for high-risk uses of AI systems apply to uses of AI which, if not done with sufficient due diligence, can lead to high risks of infringement of fundamental rights, as well as health and safety**. For example, if not done with the utmost care, the use of AI systems in the judiciary could lead to serious miscarriages of justice, or procedural errors which could invalidate court proceedings. The AI Act's requirements for high risk AI systems put in place measures to minimise the risk of such issues occurring, including requirements on data governance, risk management, as well as accuracy, robustness and cybersecurity. These are all key considerations that should be foundational to any system being developed for use in a sensitive context such as law enforcement or the administration of justice and democratic processes. The introduction of the fundamental rights impact assessment (FRIA) for deployers also ensures that deployers take account of the unique contextual risks in their country or deployment context. Without undertaking a FRIA, deployers risk overlooking key contextual considerations and inadvertently contributing to the infringement of fundamental rights. By mandating such due diligence standards for high-risk areas, the AI Act sets a foundation of basic quality control for AI systems on the market in the EU. 'Simplifying' any of these requirement will mean lowering the bar for high-risk areas, and will in fact disadvantage providers who wish to adhere to the highest standards of responsible development by allowing less diligent competitors to undercut them, resulting in less trustworthy systems on the market across the EU.

5. "Other aspects related to electronic identification and trust services under European Digital Identity Framework, including in view of the regulatory alignment with the forthcoming proposal for an EU Business Wallet and applying the 'one in, one out' principle"

As EDRi member epicenter.works writes in their submission: "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."

"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 further add that for the eID Wallet to be adopted by individuals, it is essential to acquire their trust – in particular, trust that the Wallet will not link their identity to their online activities, which is a serious concern when it comes to any system that may persistently identify people online and could therefore violate people's right to privacy in online spaces. To increase accountability, a list of core principles were baked into the eID Regulation, such as unlinkability (where attestation of attributes do not require the identification of the user), the selective disclosure of data, or the prevention by design of tracking, linking or correlating transactions and user behaviour. While trust toward the Wallet architecture itself is essential, so is the trust toward the relying parties, the qualified trust service providers, and other key actors involved wherever they have reporting obligations or need to undergo an audit.

This potential for trust has already been seriously impacted by some of the implementing acts. Given the Commission's aspirations to amend provisions around relying parties and qualified trust service providers, EDRi is concerned that the proposed "simplification" will in fact mean deregulation of the core principles that are designed to enable trust in the eID framework. In particular, we want to underline the importance of the Art. 5b obligation for relying parties to register in advance the attributes they intend to request from the users, as this streamlines the use of the wallet and effectively prevents over-burdening the user (who would otherwise need to make an informed assessment for every piece of information requested by each relying party). The Commission's proposal must not re-open this core provision.

The Call for Evidence also mentions a need for regulatory alignment between the eIDAS II Regulation and the forthcoming proposal for an EU Business Wallet. For the EU Digital Identity Framework, the focus was primarily on identification and authentication to support natural persons; if the Commission wants to extend this to companies through an EU Business Wallet, the latter should be built in a way which is compatible with the eID Wallet (and which does not apply to natural persons), *not* the other way around. There is no need for simplifying and eliminating overlaps with existing rules, since the EU Business Wallet is yet to be proposed and therefore can be designed so as not to have overlapping rules in the first place. The overlap does not (yet) exist, and it is within the power of the Commission to propose a future EU Business Wallet that does not create overlaps.

Further, if the Commission wants to enable the secure exchange of electronic documents on top of the eID Wallet's identification and authentication features, it should ensure that this initiative leaves no leeway for the underlying architecture of the Wallet to be amended.

More broadly, the use of the eID Wallet should always remain voluntary, and those who choose alternatives to it should not be discriminated against, whether directly or indirectly. This, regardless of the costs involved with maintaining alternatives, in particular in light of the digital divide and the risks of exclusion. Further, we note that a (perceived) move toward making the use of eID mandatory could have a chilling effect on people's rights and freedoms. EDRi therefore warns that the Digital Omnibus must in no way undermine these provisions – and we question the very premise of reducing compliance obligations for providers of the eID ecosystem when the risk of violating privacy and data protection rights, which would also have a knock-on effect on rights to access information and to free expression, is high.

Evidence:

- On 25/09/2025, the Belgian Constitutional court enshrined the right to alternatives to digital public services in order to ensure inclusiveness and accessibility in the face of the digital divide (https://fr.const-court.be/public/f/2025/2025-126f-info.pdf). The court underlined that while there are some requirements which public administrations may dispense with where these are disproportionately burdensome, this is not the case of the individual's right to an alternative to digital means.
- The UK government plans to launch a digital ID and make it mandatory for anyone wanting to work; it is allegedly aimed at curbing illegal immigration and simplifying access to government services. Polls show how this policy (in particular the mandatory element and the political aim of repressing a particular activity) sparks major backlash and disapproval – article from the Guardian (https://www.theguardian.com/politics/2025/oct/01/keir-starmer-labour-collapse-public-support-digital-id-cards). More than 2.8 million people have signed a petition against introduction of the UK eID (https://petition.parliament.uk/petitions/730194?ref=ed_direct).

Conclusion: Simplification for whom?

With this Digital Omnibus – and the broader digital simplification package – EDRi fears that the European Commission is 'putting the cart before the horse'. Laws like the AI Act and the DGA are being "simplified" before we have robust evidence about their effectiveness. In the case of the Business Wallet, it is being "simplified" before it even exists. This is a trend that permeates the whole deregulatory agenda, whereby European

Commissioners are tasked with cutting laws for the sake of cutting laws, rather than substantively engaging with the actual barriers that stand in the way of people across the EU from being able to access their rights. This calls into question the legitimacy, as well as the evidence base, of the "simplification" agenda.

We are wary of the claims that the Digital Omnibus will "simplify" the lives of people across the Union such as by tackling annoying cookie banners/cookie walls, or making it easier to share official documents digitally. These seemingly innocuous measures may obfuscate the fact that the Digital Omnibus (and likely future steps under the broader package) risks undoing years of digital rights progress, and undermining key protections in the areas of AI, surveillance and data sharing which are much further reaching than they may initially seen.

We see similar patterns across other areas of digital simplification, for example the risk that the forthcoming Digital Networks Act would reopen Net Neutrality protections as part of purportedly routine telecoms harmonisation, even though this would deprive people in Europe of their choice and freedom in internet services. We also perceive that the Commission's proposed massive uptake of AI (as in the AI Continent and Apply AI strategies) relies on weakening protections against harmful AI (as in the AI Act) as well as broader corporate due diligence and environmental protections which would otherwise constrain the extractive mining of raw materials and the environmental harms caused by AI use and proliferation.

However, our experience suggests that what those subject to the EU's rules (companies, authorities) really need from EU is robust guidance. Clear, relevant, predictable, simple guidance regarding various obligations, their interplay etc. would be the most effective, straightforward and rights-compliant way to streamline and ease compliance.

As already noted, we remain particularly alarmed that the call for evidence dismisses the chance of any potential negative consequence on fundamental rights from the Omnibus:

> *"The adjustments proposed in the Digital Omnibus are not expected to modify or have negative impacts on the underlying acts as regards other areas such as the protection of fundamental rights or the environment."*

We hope that this submission contributes to redressing this error, given the very significant potential impacts on fundamental rights to privacy, data protection and non-discrimination, as well as other rights to which these can be a gateway. The description of the call for evidence further explains that the aim of the digital omnibus is to "quickly reduce the burden on businesses", again highlighting that people and communities are not being served by the Commission's deregulation agenda.

EDRi is further concerned by the democratic deficit in this procedure. The call for evidence of the Digital Omnibus is closing just five weeks before the proposal is slated to

be adopted by the Commission, making it unlikely that our inputs and evidence can be meaningfully analysed and incorporated. This serves to strengthen the voices of industry players, who have had a privileged seat in the "reality checks" on the Digital Omnibus and other omnibuses, while giving limited input to civil society. By rolling so many distinct digital laws with different purposes and aims together into one Frankenstein's monster of an Omnibus, the Commission also makes it harder for the relevant lawmakers to exercise appropriate scrutiny, instead presenting a 'take-it-or-leave-it' package deal.

The urgency process which has been used in the European Parliament for some Omnibuses already in 2025 further compounds our concerns that these processes are being rushed, eliminating the possibility for proper democratic scrutiny on the basis of a manufactured urgency to "cut red tape". This also creates – rather than mitigates – legal uncertainty, as companies and public bodies suspend implementation of rules in case they are to be cut.

Genuine simplification, which asks how access to fundamental rights protections and justice can be enhanced for people and communities, and how businesses and state authorities can more easily protect and respect our rights, is welcome. Regulatory coordination, procedural innovation, and increased enforcement resources are all needed to boost the EU's digital rulebook. This is especially important given that the EU's fundamental rights regime has never been accessed or applied equally, and minoritised communities disproportionately face the brunt of tech harms.

Yet across policy areas, laws that protect people, democracy and the planet from abuses by corporations, shareholders, police, public administration and migration authorities are being cut, whilst those that punish, surveil, manipulate and exploit people are on the rise. This call for evidence, along with the Omnibuses that have already devastated environmental and corporate accountability protections, suggests that streamlining access to rights and justice is not what is on the table. With this digital omnibus, and future steps under the broader digital simplification package, the EU's global role as a digital policy leader could be undermined.

For more information, please contact:

- Ella Jakubowska, head of policy, ella.jakubowska@edri.org;
- Itxaso Domínguez de Olazábal, PhD, policy advisor, itxaso.dominguez@edri.org;
- Blue Duangdjai Tiyavorabun, policy advisor, blue.tiyavorabun@edri.org;
- Simeon de Brouwer, policy advisor, simeon.debrouwer@edri.org.