Google

October 2025

Call for evidence
Digital Omnibus

Content

1. Introduction and general principles for simplification

We welcome the European Commission's launch of the Digital Omnibus Simplification Package and fully support the ambitious goals to bolster Europe's economic competitiveness and capitalize on the AI revolution and digitalization. We believe that regulatory simplification and coherence should be treated as strategic priorities for Europe to create an environment where businesses, people, and innovation can thrive.

The Commission's acknowledgement of the need to streamline existing regulation is timely, as the last few years have seen an increased amount of digital legislation resulting in a dense, fractured, and unevenly enforced regulatory landscape. This complexity increases compliance burdens and undermines legal certainty, making it difficult for digital services to scale across the Single Market. We appreciate the Commission looking into the policy areas identified by this process (AI, Data, Privacy, Cybersecurity and Digital Identity) and we believe that several

others would benefit from the same exercise. We are therefore including suggestions on how rules in the space of competition (DMA) and content moderation (DSA) could also be streamlined to unleash growth and innovation potential.

It is crucial for the EU to take affirmative steps to re-energize its economy by accelerating the deployment of best-in-class technologies and promoting investment in cutting-edge innovation. Europe needs to channel more investment into compute infrastructure, digital networks, and digital skills—the foundations of a thriving digital economy. Additionally, the EU should refrain from introducing new regulations that will add further layers of overlapping rules, thereby impacting competitiveness. It is important to fully untangle, clarify, and implement all recently approved legislation before adding to the pile. Simplification principles should therefore be applied to upcoming legislation as well, such as the Digital Fairness Act and the Digital Networks Act, as we are suggesting in this paper.

These simplification efforts should be holistic and ambitious, transcending mere procedural adjustments to fundamentally restructure the rulebook to be coherent, proportionate, and workable. While supporting small and medium-sized enterprises is vital, simplification cannot be limited to one segment or slice of the economy. The digital world is an interconnected ecosystem; friction at any point in the value chain creates drag for all, from startups to large enterprises. The objective should not be a two-tiered system, but a trust-based framework, giving citizens confidence that their rights are consistently upheld across the Union, and letting businesses rely on clear, coherent, and predictable rules of the road.

We believe that Europe can become a global leader in AI and future technology innovation, but that will require a strategic shift away from an over-regulated approach and toward one that prioritizes a cohesive, innovation-ready environment. Accelerating European innovation also demands trade openness, as raising trade or regulatory barriers would hurt EU competitiveness by disrupting access to best-in-class digital services. We are committed to continuing our constructive work with the European Commission to unlock Europe's full digital potential.

Drawing from our experience in developing and deploying secure technologies and services globally, we offer detailed suggestions and concrete recommendations to support the Commission in assessing what regulatory challenges to address and how to ensure the digital environment is innovation-ready.

2. Policy recommendations

• AI Act

To secure its position as a global leader in responsible AI, the EU should ensure the AI Act protects fundamental rights while fostering innovation.
The Act's current ambiguity, already outdated technical thresholds, and potential for unworkable timelines create legal uncertainty and unnecessary regulatory burdens. This hinders the development and deployment of competitive, world-class AI within the Union.
The solution is not an overhaul, but targeted, strategic simplifications focused on five key areas.

1. Update compute thresholds and develop a capabilities-based process for systemic risk models

- *Situation/issue:* Regulation should target genuine risks, but the current compute thresholds are outdated and create an inaccurate scope. The current 10^25 FLOPs compute threshold risks becoming over-inclusive by capturing models no longer at the cutting-edge and under-inclusive by missing highly capable models built more efficiently. This dilutes the AI Office's focus and burdens innovators unnecessarily.
- *Proposed solution:* We propose increasing the threshold to 10^26 FLOPs, to better reflect the scale of today's frontier models, align with international discussions, and allow regulatory resources to be targeted more effectively. We also suggest determining whether it is possible to establish a capabilities-based process to identify potentially high-impact models that show equivalent or better performance to 10^26 (and higher) models despite being trained on less compute due to the use of distillation, quantization or similar techniques.

2. Ensure proper implementation timelines for AI transparency obligations (Art.50)

- *Situation/issue:* The proposed 10-month finalization period for the new Code, announced in September, leaves organizations with less than one month to prepare for compliance. This compressed schedule creates significant legal uncertainty, hindering the ability of companies to undertake the extensive preparations required. Without clarity on the final requirements, crucial work—such as establishing new governance frameworks, or implementing operational changes—cannot begin. Consequently, organizations face an elevated risk of non-compliance by the deadline, exposing them to potential legal action and business disruption.
- *Proposed solution:* To ensure workable compliance, the AI Office must establish reasonable implementation periods for any AI Act provisions that are contingent on future

guidance. This applies specifically to obligations linked to Codes of Practice, implementing acts, or standards that have not yet been finalized. This approach incorporates key lessons from the significant delays experienced with the GPAI Code of Practice and prevents a scenario where crucial guidance is released just days before a compliance deadline. Specifically, we recommend that the obligations under Article 50 of the AI Act become applicable no sooner than six months following the official finalization and publication of the relevant Code of Practice on Transparency.

3. Limit the territoriality of copyright rules to align with Union Law

- *Situation/issue:* The Act's current ambiguity on copyright creates significant legal uncertainty for AI developers globally.
- *Proposed solution:* It is important to clarify that EU copyright obligations apply only to activities only where Union copyright law governs the relevant act, like placing a model on the EU market. This approach is critical because world-class AI models are trained on global datasets across multiple legal jurisdictions. Applying EU law to all AI development that occurred outside the Union would not only undermine the principle of copyright territoriality but would create unworkable compliance friction and legal uncertainty, deterring leading developers from releasing their models here and ultimately harming European innovation and competitiveness.

4. Streamline the assessments of high-risk AI systems as part of the upcoming guidelines

- *Situation/issue:* The Commission is currently working on the guidelines for high risk AI systems, which obligations enter into force in August 2026. The target date for the guidelines is Feb. 2026.
- *Proposed solution:* The Commission should expedite its guidelines well before the February 2026 deadline and/or defer the deadline. These guidelines need to provide clear, practical criteria and concrete examples of systems that are not high-risk, such as those performing narrow procedural or preparatory tasks without replacing human review. This should be built on three core principles:
    - *Presumption of Accuracy in Good-Faith Documented Self-Assessments*: A provider's documented self-assessment, conducted in good faith against clear criteria, should be considered a sufficient basis for applying an exemption. Regulatory focus should be on the adequacy of the assessment, not on second-guessing a provider's conclusion without evidence.
    - *Clarity of Purpose*: An AI system should be classified as high-risk only if its provider positively states it is intended for that particular use in its documentation or marketing materials. A general advertising tool, for instance,

should not become high-risk just because it is occasionally used to place a job ad.

- *Flexibility in Spirit*: The ultimate test is whether a system poses a significant risk to health, safety, or fundamental rights. The guidelines should clarify that the specific exemption categories in the Act are illustrative examples, not an exhaustive list.

5. Permit broader data processing to proactively address bias mitigation

- *Situation/issue:* The EU aims to lead in AI that does not infringe fundamental rights, yet the AI Act currently restricts the processing of special categories of personal data for bias correction to only high-risk systems, ignoring the AI lifecycle.
- *Proposed solution:* We propose extending the allowance in Article 10(5) to permit the necessary data processing for bias detection and correction across all AI systems and general purpose AI models. Extending this provision will provide a harmonized legal basis for developers to proactively build the fair, representative, and trustworthy AI that aligns with the EU's core values and benefits all citizens. It will also reduce the risk of AI models and systems perpetuating or amplifying societal discrimination, irrespective of their specific AI Act risk classification.

● Privacy and Data

The Digital Omnibus presents a critical opportunity to modernize rules designed for a previous technological era and fulfill the European Commission's ambitions for a vibrant, AI-first economy. To secure its global leadership in AI, Europe should modernize its data protection framework. While the GDPR is a cornerstone of digital legislation, its full potential is undermined by fragmented implementation and interpretations that predate the age of AI.

The core issue is the misalignment between overlapping regulations, chiefly the GDPR, the outdated 2002 ePrivacy Directive, and the Data Act. This legal fragmentation creates significant legal uncertainty and administrative burdens, which hinder innovation and delay access to new technology for European citizens and businesses, putting the EU at a competitive disadvantage. The problem is particularly acute for AI development, where conflicting approaches from national Data Protection Authorities on fundamental issues slow progress and increase risk.

This regulatory complexity has also proven counterproductive for consumers. Requiring multiple, granular consents fosters "consent fatigue" and creates a user experience at odds with the seamless expectations of the AI era. This dynamic threatens to limit the creation

and adoption of new services, especially next-generation agentic AI products in Europe.

Any meaningful simplification requires reforming the ePrivacy Directive and making targeted, smart changes to the GDPR and Data Act. The recent withdrawal of the ePrivacy Regulation proposal presents a major opportunity to do this effectively. By pursuing these targeted measures, the EU can build the clear, holistic, and future-proof data protection framework needed to foster a thriving European AI ecosystem while upholding its fundamental values.

GDPR

1. Explicitly recognise the proportionality principle in the GDPR

- *Situation/issue:* The absence of a general, overarching proportionality principle in the GDPR has led to absolutist interpretations and enforcement practices by some Data Protection Authorities. This can place potentially unlimited and disproportionate compliance burdens on organisations, regardless of the actual risk to individuals. This deviation from the original risk-based approach of GDPR results in businesses having to divert resources from mitigating high-priority risks to address low-risk, "tick-box" compliance exercises.
- *Proposed solutions:* Explicitly recognize a general principle of proportionality within Article 24(1) of the GDPR. This would codify that compliance efforts should be weighed against the associated costs, operational needs, and the actual risks to individuals. This empowers organizations to focus resources on what matters most and fosters a more flexible and effective approach to both compliance and enforcement.

2. Reaffirm legitimate interests for AI training

- *Situation/issue:* Europe's AI development is being stifled by legal uncertainty around the use of 'legitimate interests'. Developers are required to produce voluminous compliance documentation, including granular risk assessments (LIAs), for even low-risk activities. Conflicting guidance from national Data Protection Authorities creates a fragmented landscape, delaying the deployment of beneficial AI models in Europe.
- *Proposed solution:* Amend Article 6(1)(f) of the GDPR to authorize the Commission to adopt an implementing act that creates a 'whitelist' of low-risk processing activities where the balancing test is presumed to favor the controller (e.g., product improvement, security, anti-abuse measures). This change should also codify existing EDPB guidance confirming that training AI models on publicly available data can be a legitimate interest, providing a necessary 'margin of appreciation' for responsible innovators and aligning the legal framework with Europe's strategic AI ambitions.

3. Modernizing the framework for special category of data (SCD)

- *Situation/issue:* Expansive interpretations by courts and regulators have broadened the scope of "special category data" to the point where almost any data can be considered

sensitive if an inference can be drawn from it. This has a chilling effect on responsible innovation, as organizations—particularly SMEs—are unsure whether they have a lawful basis to conduct vital scientific research or process data to detect and mitigate algorithmic bias.

- *Proposed solutions:*
  - First, amend Article 9(1) to clarify that its scope is limited to data that is explicitly sensitive or is processed with the intent to infer sensitive characteristics.
  - Second, expand the exemptions in Article 9(2) to create a clear, harmonized legal basis for processing data that has been manifestly made public and for scientific research, explicitly recognizing the development of general-purpose AI models as a qualifying research purpose.

4. Ensuring stable international data flows

- *Situation/issue:* The current regime for international data transfers, particularly following the *Schrems II* judgment, imposes significant and often duplicative compliance burdens on organisations. The requirement for case-by-case transfer impact assessments creates friction for the global digital economy without a proportional increase in data protection.
- *Proposed solutions:* Streamline the international data transfer regime to reduce operational overhead and restore legal predictability:
  - **Establish an intra-group transfer certification regime.** Enshrining a self-certification mechanism by amending Article 46 of the GDPR accordingly would allow multinational organisations to streamline internal data flows under a unified set of safeguards, obviating the need for case-by-case assessments and significantly reducing compliance burdens for routine global operations.
  - **Allow for consolidated transfer impact assessments (TIAs).** Recognising in Article 46(1) that a single, robust assessment can cover a set of similar transfers using the same safeguards would reduce the significant burden of conducting multiple, often duplicative, assessments and allow organisations to focus resources on substantive risk mitigation.
  - **Address the gap in the current Standard Contractual Clauses (SCCs).** An amendment to the Article 1 of the Annex regarding SCCs to cover transfers to third-country organisations already subject to the GDPR would close a recognised legal gap, providing immediate certainty without the need to adopt an entirely new instrument.

5. Incentivise the use of Privacy enhancing technologies (PETs)

- *Situation/issue:* While the GDPR supports data protection by design, it does not explicitly incentivise the use of PETs such as federated learning, differential privacy or synthetic data techniques. This lack of clear recognition creates legal uncertainty for

innovators and means organisations that invest in these state-of-the-art safeguards see no clear benefit in their compliance or risk-assessment activities.

- *Proposed solutions:* Explicitly recognise PETs within the GDPR as a key measure for data protection by design to push for adoption and foster privacy-preserving innovation, such as in AI development.
  - Recognize Privacy-Enhancing Technologies (PETs) alongside pseudonymisation in Article 25 as a key element of 'data protection by design.'
  - Amend Article 6(1)(f) to give the use of PETs significant weight in the 'legitimate interests' balancing test.
  - Clarify that using PETs in good faith will be a mitigating factor in enforcement actions.

ePrivacy directive

1. Tackling consent-fatigue by modernizing ePrivacy "cookie rule"

- *Situation/issue:* The current Article 5(3) applies a rigid, one-size-fits-all consent requirement to all on-device storage or access to information already stored, regardless of purpose or privacy impact. This over-reliance on consent has produced significant unintended consequences. Firstly, it has devalued the concept of consent itself, turning a meaningful choice for users into a routine, low-engagement task that has led to widespread 'consent fatigue'. Secondly, it has discouraged privacy-enhancing innovation by subjecting all technologies, regardless of their risk or benefit, to the same rigid consent requirements. Finally, the difficult coexistence with the GDPR, absent a modernised ePrivacy Regulation, has created persistent legal uncertainty and fragmented interpretations, undermining the predictability of the Digital Single Market.
- *Proposed solutions:*
  - The most effective simplification is to delete Article 5(3) from the ePrivacy directive and govern all data processing related to cookies under the GDPR risk-based framework. This would eliminate legal fragmentation and user fatigue from low-risk consent requests, establishing the GDPR as the single standard. Crucially, it would restore the meaning of consent by reserving it for processing, like personalized advertising, where users expect meaningful choice and control.
  - Alternatively, a significant step toward simplification would be to amend Article 5(3) to extend the scope of permitted exemptions to allow specific, low-risk processing activities that are essential both for the functioning of a safe and sustainable digital ecosystem as well as for user experience. This would create clear exemptions for functions such as first-party audience measurement, ad frequency capping, and anti-fraud measures—allowing them to operate without generating unnecessary consent requests. This targeted reform would reduce friction for users, restore the significance of consent for processing like personalized advertising where people expect to have a reasonable amount of choice and control, and create positive

incentives for privacy innovation.

2. Streamlining ePrivacy directive with other legal frameworks

- *Situation/issue:* The ePrivacy Directive has become a patchwork of rules with disparate policy goals, creating legal uncertainty and hindering innovation. Its outdated, telecoms-era provisions overlap confusingly with the more modern, comprehensive framework of the GDPR, while its rigid principle of confidentiality has not kept pace with the evolution of digital communication services that rely on automated processing to deliver essential security features and user benefits.
- *Proposed solutions:* We propose three targeted actions to create a simpler, more effective, and future-proof framework:
  - **Consolidate Telecoms Rules in the EECC:** Relocate the Directive's legacy telecoms-specific provisions (e.g., itemised billing, line identification) to their natural home in the European Electronic Communications Code (EECC), allowing the ePrivacy framework to focus on its core purpose of ensuring confidentiality of communications
  - **Rely on the GDPR for Data Processing Rules:** Remove legal duplication by deleting the Directive's now-redundant rules on traffic and location data, and rely exclusively on the GDPR's comprehensive, risk-based framework for governing the lawful processing of all personal data, thereby creating a single, harmonised standard.
  - **Modernise the Principle of Confidentiality:** Update the core confidentiality principle to clarify that automated processing necessary for ensuring network security (e.g., blocking spam and malware) and providing innovative, pro-user service features is permissible, and confirm that data stored on a user's device after a communication is complete is governed by the GDPR.

Data Act

1. Resolving the Data Portability Conflict Between the Data Act, DMA, and GDPR

- *Situation/issue:* The Data Act's restrictions on gatekeepers have inadvertently created a significant legal contradiction that paralyzes the GDPR right of data portability. Article 5(2) of the Data Act bars companies designated as gatekeepers under the DMA from acting as data recipients. This prohibition is in direct conflict with a user's fundamental right to port their data under Article 20 of the GDPR and with the continuous data portability obligations enshrined in Article 6(9) of the DMA. This legislative clash places data holders in an impossible position. When a user requests to transfer their data to a service operated by a designated gatekeeper, the data holder is faced with a legal trilemma: honoring the user's request could breach the Data Act, while refusing it would violate their clear obligations under the GDPR and the DMA. This stalemate negates the user's control

over their own data, creates friction in the market, and directly undermines the EU's goals of fostering competition and preventing user lock-in.

- *Proposed Solution:* The European Commission should issue urgent and clear guidance to resolve this legal conflict. This guidance needs to establish a clear hierarchy of rules, affirming that the restrictions in the Data Act cannot invalidate the pre-existing, fundamental rights of users under the GDPR or the explicit obligations for gatekeepers under the DMA. It is essential to clarify that companies should facilitate all user-directed portability requests to ensure that the right to data portability remains effective and that the pro-competitive objectives of the digital rulebook are upheld.

2. Address Duplicative Rules for Consumer Data

- *Situation/issue:* The Data Act's obligations for consumer products (Chapter II) overlap almost entirely with consumer rights already established under the GDPR, such as data access and portability. This creates conflicting legal regimes that are difficult for businesses to navigate and confusing for consumers, without providing meaningful additional protections.
- *Proposed Solution:* The most effective simplification is to carve consumer data out from the scope of the Data Act's Chapter II portability and information requirements. The GDPR already provides a robust, well-understood framework for consumer data rights. Relying on the GDPR as the single standard would eliminate legal fragmentation and reduce unnecessary compliance overhead.

3. Clarify and Narrow the Scope of "Connected Product"

- *Situation/issue:* The Act's definitions of "connected product" and "related service" are so broad they could apply to nearly any item that generates data, including general-purpose devices like smartphones and PCs. This ambiguity massively expands the Act's scope beyond its intended focus on industrial data, creating legal uncertainty and significant compliance burdens for a vast range of consumer technologies.
- *Proposed Solution:* Amend the definition of "connected product" in Article 2(5) to explicitly exclude devices whose primary function is not the storing and processing of data on behalf of others, such as personal computers, tablets, and smartphones. This provides immediate legal certainty and focuses the Act's obligations where they are most relevant.

4. Confine Vague Business-to-Government (B2G) Data-Sharing Obligations

- *Situation/issue:* The novel and broadly drafted B2G data-sharing obligations in Chapter V create significant legal uncertainty. It is unclear what data is in scope and which of the myriad public authorities are empowered to request it, opening the door to potentially limitless and unclear requests in cases of "exceptional need."

- *Proposed solution:* First, confine the scope of Chapter V to "product data" and "related service data" only, providing clarity on *what* can be requested. Second, require the Commission and Member States to create and maintain a prescribed, public list of the specific bodies empowered to make such requests, clarifying *who* can make them. These changes would provide essential legal certainty and limit the operational burden on companies.

● Cybersecurity

1. Streamlining certification process for market access

- *Situation/issue:* Product certifications present significant challenges for manufacturers. Under the Radio Equipment Directive (RED), late-delivered harmonized standards necessitated testing against anticipated specifications, causing uncertainty and potential redundancy. Moreover, the linkage of hardware certification to often-delayed software release schedules creates problematic scheduling gaps (e.g., three months) before production. The upcoming Cyber Resilience Act (CRA) is similarly hampered by the lack of harmonised standards, disrupting development and increasing uncertainty. Finally, the potential requirement to retest all RED-certified devices under CRA would impose a massive and arguably unnecessary overhead on the industry.
- *Proposed solutions:* Streamline certifications for market access.
  - *Provide timely standards:* Harmonized standards should be released at least 12 months before the enforcement date. If standards are delayed, the enforcement date should also be delayed.
  - *Create smooth transition pathways:* Devices certified under Radio Equipment Directive (RED) should be grandfathered or pre-approved for the Cyber Resilience Act (CRA). CRA compliance could then focus on verifying the manufacturer's secure development lifecycle, which is the core differentiator between the two acts.
  - *Recognise industry and international standards:* The EU should recognise established industry certification programs as a means of demonstrating compliance (e.g., GSMA's MDSCert) and make greater use of international standards.This reduces duplicative efforts, lowers costs, and speeds up the implementation of regulatory requirements.
  - *Decouple hardware and software certification:* For devices like phones and tablets, the certification of hardware and software should be decoupled under RED and, where applicable under CRA, to align with practical development cycles. Software is often finalized much closer to product launch, whereas hardware certification is needed before production can begin, resulting in significant scheduling gaps (e.g., a 3-month gap where hardware teams require RED certification while software

development is still ongoing).

2. **Harmonising reporting requirements and reducing unnecessary reporting burden**

- *Situation/issue:* A single security incident can trigger reporting obligations under multiple EU regimes (e.g., GDPR, NIS2, CRA), each with different criteria, timelines, and authorities. This diverts critical resources from incident response to administrative compliance and does little to advance the intended goal of enhancing cybersecurity and incident response capabilities across the EU. In addition, a requirement in the CRA to report on actively exploited vulnerabilities, including those that are unpatched, creates significant cybersecurity risks by potentially exposing attack vectors and unintentionally creating a massive database of zero-day vulnerabilities. And reporting requirements to legacy products and potentially products beyond the stated support period impose a disproportionate and unnecessary burden.
- *Proposed solutions:* Harmonise incident reporting requirements and reduce unnecessary reporting burden.
  - *Establish a single EU Reporting Mechanism:* Authorise a single, Europe-wide entity to create a unified portal and a single, harmonized template for reporting incidents, and vulnerabilities, where applicable, under regulations like GDPR, NIS2, DORA, CRA, and the AI Act. The single reporting platform to be established by ENISA as mandated by CRA could be utilised for this purpose.
  - *Implement the "Report Once, Comply Many" principle:* Clarify that reporting an incident under one key regulation (e.g., NIS2) satisfies the requirements for that same incident under other relevant regulations (e.g., CER).
  - *Harmonize timelines and thresholds:* Standardise reporting timelines around a 72-hour deadline and align thresholds for reportable incidents (e.g., harmonize what is considered "significant" vs. "severe"). The calculation for when the reporting clock starts should also be harmonised ensuring it only happens when the incident is confirmed.
  - Limit the reporting requirement in CRA on actively exploited vulnerabilities to those where a mitigation is already available.
  - CRA's reporting obligations under Article 14 should be limited to the declared *support period* and only for products that were put on the market after 11 December 2027.

3. **Optimising cybersecurity governance**

- *Situation/issue:* The proliferation of cybersecurity governance requirements across multiple EU legislative acts creates an administrative burden that does not always improve cybersecurity posture, especially when they overlap with established global frameworks. Furthermore, the potential for individual EU Member States to adopt their own, dissonant cybersecurity certification schemes adds another layer of complexity.
- *Proposed solutions:*

- *Leverage existing international frameworks*. Encourage the use of globally recognized standards like ISO 27001 as a baseline for demonstrating compliance with EU governance requirements. This promotes global interoperability and allows companies to build on their existing security investments.
- *Discourage dissonant national certification schemes*. Actively discourage EU Member States from creating their own national cybersecurity certification schemes that diverge from harmonized EU or international standards. ENISA could play a stronger role in promoting this harmonisation.
- *Maintain a voluntary certification framework*. Ensure that certification remains voluntary and any mandatory certification remains limited to well-defined high-risk use cases, subject to impact assessment with meaningful stakeholder engagement and as a last resort option.

4. Strengthening ENISA's role

- *Situation/issue:* Technology policies, even those not primarily focused on cybersecurity, can have far-reaching and unintended negative impacts on the security of digital services used by EU citizens. The need to comply with a wide array of disparate technology regulations can lead to situations where product design choices, made to ensure security and integrity, need to be modified in ways that introduce new security risks or weaken existing protections. Security should be taken into account at every step in the legislative or regulatory process to guarantee digital security for all.
- *Proposed solutions:*
  - *Independent security impact assessments of the EU tech regulations*. The revised Cybersecurity Act should grant ENISA an explicit and elevated role to serve as an impartial evaluator of all new EU technology laws and regulations. Just as the EU assesses economic and social impacts, this "security impact assessment" would provide policymakers with expert analysis on potential security risks *before* legislation is passed, ensuring better outcomes for citizens' security and privacy. In line with the EU better regulation principles.
  - *Align mission with resources*. ENISA's mandate as an independent, technical, and consultative body should be strengthened while providing supplementary resources to support its evolving mission as well as the work it does on stakeholder engagement like the Cyber Partnership programme (CPP).

● Digital Identity

We believe that emerging digital identity frameworks are a pivotal moment in our collective journey toward a more user-centric Internet, where the user benefits from rapid innovation in a more trusted, safe and privacy preserving way. Our vision is to ensure all users have

access to secure, privacy-preserving, and interoperable digital credentials for trusted interactions in-person and online.

We support the introduction of the EU Digital Identity Wallet (EUDI Wallet) as part of the necessary shift toward secure, interoperable digital identity solutions that prioritize user control, privacy, and industry standards. This framework represents an important future trend, offering both convenience and enhanced control for users over their personal information. We are dedicated to ensuring our online services are ready to integrate and interoperate with national EUDI Wallet implementations and the evolving eIDAS 2.0 framework. While we align with the EUDI's goal of offering a secure, user-centric, and widely accepted means for digital identification and authentication, we want to suggest some areas of improvement:

1. **Fragmentation and competing standards**

- *Situation/issue:* If legal digital identity frameworks and jointly developed standards by the Industry (like the Digital Credentials API within the W3C working group) develop as separate, non-interoperable systems, it will lead to user confusion as well as click and verification fatigue, increased compliance burdens for businesses, and, most importantly, a less effective solution for protecting users and children online.
- *Proposed solution:* We can prevent this by ensuring our respective technologies are interoperable. By integrating standards like the **Digital Credentials API** into the technical specifications of the EUDI framework, we can create a single, powerful standard that benefits everyone globally. This would reduce the burden on developers, especially smaller businesses, and ensure a seamless, secure user experience online and offline.

We are actively working towards integrating standards, such as the **Digital Credentials API,** into the EUDI framework. We believe that the Digital Credentials API is a better way to handle digital identity than custom URI schemes because it is more secure, easier for people to use, and interoperable across different platforms. It also prevents phishing and gives users a clear, unified way to share their credentials, avoiding the security risks and usability problems of the old custom URI schemes. We are also supporting **OpenID for Verifiable Presentations (OpenID4VP)** since we believe this is a superior standard for digital identity compared to Annex C (which is part of ISO/IEC 18013-7). To create a truly universal digital identity ecosystem, we need widely adopted, interoperable protocols. We champion the adoption of **OpenID4VP** as the preferred strategic protocol. This approach will enable all browsers and apps to support a wide range of use cases — from simple age verification to complex, secure transactions — by leveraging the **Digital Credentials API**.

2. **Fragmentation and competing standards**

- *Situation/issue:* Mandating broad age checks on low-medium risk services would create significant user hurdles and could even lead to consumer backlash against digital IDs.

- *Proposed solution:* We strongly advise that strict ID checks for age verification purposes are only mandated for high-risk activities like watching pornography, or buying alcohol. When it comes to digital identities and online safety for minors specifically, we believe this is a shared responsibility that requires a nuanced and multi-layered approach, not a one-size-fits-all solution. We follow a framework where the degree of age assurance is directly proportional to the nature and risks posed by a service, a context that developers are uniquely positioned to understand.

3. Maintaining browser security and authentication standards (QWACs):

- *Situation/issue:* At a technical level, we should urgently address the requirements for Qualified Website Authentication Certificates (QWACs). The proposed immediate entry into force is unfeasible due to the multi-month distribution and testing processes of web browsers and the reliance on Qualified Trust Service Providers (QTSPs) for adoption.
- *Proposed solution:*
  - A minimum six-month implementation period following the normal entry into force is needed. Web browser providers need access to standardized testing endpoints (servers with valid/invalid 1-QWAC and 2-QWACs) from QTSPs at least 90 days before the regulation takes effect to verify their conformant implementations.
  - Any new technical requirements should allow us to preserve and impose sufficient security measures to effectively protect users from threats like phishing and man-in-the-middle attacks.

3. Relevant policy areas: competition and content regulations

For the simplification package to re-energize European competitiveness, we believe its focus should be more ambitious. Complexity and fragmentation in the digital *acquis* create operational burdens and legal uncertainty, hindering digital service scaling. To address these systemic frictions and ensure a coherent, predictable, and innovation-ready digital rulebook, we suggest the simplification effort should also cover other policy areas, on top of the five areas already identified by the EU Commission, to be addressed in further omnibus packages.

A. Competition and Digital Markets Act

To achieve its goal of a fairer and more contestable digital single market, the EU should ensure the Digital Markets Act (DMA) works for everyone.

DMA's current enforcement architecture has created unintended negative consequences. This **creates significant user friction** for consumers, **disadvantages Small and Medium-sized Enterprises (SMEs)**, and **generates legal uncertainty** for all market participants, undermining the very pro-competitive goals the DMA was designed to achieve.

The solution is a strategic course-correction focused on integrating key principles into the enforcement process. This means:

- Introducing a formal **"SME and Consumer Friendliness Test."**
- Reinforcing the DMA's single-enforcer model to prevent regulatory fragmentation and clarifying **procedural safeguards** for all parties.

These targeted changes will provide the necessary balance and certainty to make the DMA a workable framework that fosters competition *and* a thriving, user-friendly digital ecosystem.

1. Adopt Consumer- and SME-friendly Implementation Guidelines via a "Digital Omnibus" Regulation

- *Situation/issue:* The current application of DMA self-preferencing rules is degrading user experience and harming SMEs. Smaller companies who rely on Google Search for visibility see traffic being driven away from them. There is no formal mechanism to weigh these negative impacts against compliance measures, and the view that this is acceptable "short-term pain" ignores the long-term risk of alienating users and harming Europe's economic interests.
- *Proposed solution:* We propose introducing **guidelines** for self-preferencing rules. These guidelines shall introduce an **"SME and Consumer Friendliness Test"** for any compliance solution, ensuring that pro-competitive measures do not come at the expense of consumers and small businesses. This builds on the established precedent of developing guidelines on interplay between GDPR and DMA and the EU's SME Test whose purpose is to analyse the effects of upcoming EU legislative proposals on small businesses. The guidelines would offer a politically feasible path to a more nuanced and effective DMA.

2. Reinforce the DMA's Single-Enforcer Model and Procedural Safeguards

- *Situation/issue:* The DMA's objective of a fully harmonised Single Market rulebook is being undermined. The overlap between the DMA's *ex ante* rules and traditional *ex post* competition law (Article 102 TFEU) allows for parallel enforcement tracks and strategic "forum shopping" by litigants. Furthermore, parallel investigations and private litigation at the national level are reintroducing the very regulatory fragmentation the DMA was designed to eliminate. This is compounded by a lack of clarity on procedural safeguards, creating an unpredictable environment where weak complaints can trigger investigations.
- *Proposed solution***:** The Commission should reinforce its role as the **sole enforcer** of the DMA. This requires issuing clear guidance on the delineation between the DMA and

traditional competition law to ensure they are not interchangeable routes. To improve regulatory certainty, the Commission should also clarify procedural rules based on three core principles:

- **Predictability:** Provide clear notice of enforcement priorities and compliance expectations.
- **Proportionality:** Ensure regulatory actions are evidence-based and narrowly tailored.
- **Fair Process:** Implement a more rigorous vetting of complaints to filter out weak or speculative claims, allowing regulators and businesses to focus on credible concerns.

B. Digital Services Act and content regulations

1. Legal uncertainty and fragmented enforcement on recommender systems

- *Situation/issue:* The Digital Services Act (DSA), particularly Article 27 and Article 38, requires disclosure of main parameters and offering non-profiling options. Similar obligations exist under Article 6a(1) of the Consumer Rights Directive (CRD) and Article 7(4a) of the Unfair Commercial Practices Directive (UCPD), which focus on ranking transparency for consumers. Furthermore, Article 5 of the Platform to Business (P2B) Regulation imposes parallel transparency duties concerning business users. This convergence of regulatory requirements, each enforced by different regulators, creates a complex compliance landscape. We are concerned by proposals for a Digital Fairness Act to further regulate recommender systems and urge the Commission to prioritize simplifying the existing framework instead of adding to it.
- *Proposed solution:* The Commission should remove overlapping obligations related to disclosures around the main parameters of recommender systems and ranking transparency from CRD, UCPD, and P2B Regulation., given the comprehensive regulation of recommender systems for both consumer and business users under the DSA.

2. Redundant and overlapping regulation of "dark patterns"

- *Situation/issue:* So called “dark patterns” are regulated by Article 25 of the DSA, the Unfair Commercial Practices Directive (UCPD), the GDPR (Recital 32), and Article 13 of the Digital Markets Act (DMA). These overlaps raise the risk that similar types of techniques may be assessed differently by the Commission, national consumer protection authorities, and national data protection authorities. This may lead to fragmentation of compliance solutions, to the extent these authorities do not agree on interpretative aspects. We are also concerned about even more dark patterns rules being explored as part of the Digital Fairness Act proposals.
- *Proposed solution:* The Commission should consider withdrawing Article 25 of the DSA to simplify the regulatory framework, given the existing regulation of dark patterns

under EU consumer protection and data protection legislation. Broadly, the Commission should provide guidance on how the various provisions regulating dark patterns across different EU frameworks should be consistently interpreted by different regulators to ensure legal certainty.

3. Overlapping reporting and transparency obligations

- *Situation/issue:* Providers of intermediary services are subject to a patchwork of EU laws that impose transparency reporting requirements, each with its own set of slightly different metrics and reporting frequencies. This creates legal uncertainty and high compliance costs.
- *Proposed solution:* Reporting obligations should be harmonised, leveraging the DSA's framework. Additional suggestions include:
  - Standardising Timelines: Align reporting cadences across instruments, allowing at least a two-month publication window after the reporting period ends.
  - Annualising Disinformation Code of Conduct Reporting: Shift the Code of Practice on Disinformation reporting to an annual cycle.
  - Withdrawing Duplicative Reporting: Eliminate the redundant transparency requirements found in the P2B Regulation and the TCOR, which the DSA now covers.
  - Upholding DSA Harmonisation: Issue clear guidance ensuring the DSA's full harmonisation effect prevents Member States from imposing new transparency reporting requirements, specifically via the national implementation of directives such as the AVMSD.

4. Minors' protection online

- *Situation/issue:* While Article 28 DSA requires high levels of privacy and safety for minors on online platforms, the pre-existing Article 28b of the AVMSD mandates specific protection measures for video-sharing platforms. Member States continue to adopt national implementing laws for the AVMSD, contradicting the DSA's fully harmonized framework and imposing disproportionate, diverse burdens on service providers. Again, the Digital Fairness Act risks adding overlapping regulations around minors protections especially on the topics of addictive designs, feature restrictions and age assurance/ verification
- *Proposed solution:* The Commission should simplify the legal framework by withdrawing Article 28b of the AVMSD, as Article 28 of the DSA already provides a comprehensive, fully harmonized framework for minors' protection on online platforms.

5. Risk assessment

- *Situation/Issue:* Articles 34 and 35 of the DSA require VLOPs/VLOSEs to assess and mitigate systemic risks, a duty which overlaps with similar, but distinct, requirements across

various EU laws. These include the DSA Minors Guidelines (risk reviews for minors), the AI Act (Articles 55(1)(b) and 9(2)), the GDPR (DPIAs), and the risk management obligation embedded in TCOR (Article 5(2)). This patchwork creates ambiguity, leading to duplicate compliance work and hindering the effective operationalisation of risk management duties.

- *Proposed solution:* The Commission should issue clear guidance to harmonise overlapping risk assessment duties (DSA, AI Act, GDPR, TCOR, etc.), permitting a single assessment to fulfil multiple legal requirements. Additionally, the Commission should exempt VLOPs/VLOSEs from any new or existing content-related risk assessments already covered by Articles 34 and 35 of the DSA.

6. DSA Codes of Conduct

- *Situation/Issue:* The current voluntary DSA Codes of Conduct, specifically the Disinformation Code and the Illegal Hate Speech Code, which have been converted into DSA ones under Article 45 of the DSA, present significant overlaps with the Digital Services Act (DSA) requirements. This creates legal uncertainty and imposes additional compliance costs on providers. For instance, the Illegal Hate Speech Code's commitments regarding terms and conditions and notice-and-action systems directly overlap with Articles 14 and 16 of the DSA. Similarly, Commitment 19 of the Disinformation Code, which addresses the transparency of recommender systems, overlaps with Article 27 of the DSA. Also, Commitment 27 of the Disinformation Code states that a third-party body funded by signatories will vet researchers and research proposals. This directly contradicts Article 40 of the DSA, which assigns this vetting responsibility to Digital Services Coordinators.
- *Proposed Solution:* To address these issues, we suggest that the European Commission take steps to ensure Codes of Conduct do not overlap with DSA requirements. This would reduce legal uncertainty and alleviate the burden of additional compliance costs on providers, who currently need to demonstrate compliance with overlapping requirements repeatedly under independent third-party audits.

4. Upcoming legislation: Digital Fairness Act, Digital Networks Act, Cloud and AI Development Act

a. Digital Fairness Act

To empower consumers and traders and to foster a truly competitive digital economy, a renewed focus on simplification and harmonisation across the EU and streamlined governance is essential. However, currently many regulations seem to overlap or their boundaries and interplay with other regulations are unclear, which also leads to different enforcement authorities with different conditions and mechanisms having jurisdiction.

This is particularly true with regard to topics which shall be addressed by the Digital Fairness Act, including dark patterns (regulated by UCPD, GDPR and DSA), minors protection, advertising and recommender system transparency (regulated by DSA, CRD, UCPD and P2B, whereby particularly the latter seems superfluous). The overlap leads to confusion and increased efforts, particularly for companies operating across borders.

The DFA is a chance to embed simplification principles early on in the legislative cycle, and look at any potential interventions through a competitiveness-focused lens.

Therefore, **we advocate for prioritising the effective and efficient implementation of existing digital legal frameworks.** We believe that this could be achieved through strengthening enforcement and more educational measures aimed at promoting users' self-determined and safe use of digital services. Furthermore, clearer legal guidance and improved business feedback mechanisms are crucial to facilitate compliance, ensuring consistent and transparent interactions that build consumer trust.

In addition, we believe that specific adjustments to individual regulations are also necessary. These include:

1. **Reduce requirements for duplicative consumer information**

- *Situation/Issue:* We believe that consumer information requirements can be reduced in case of repetitive transactions with the same provider or those concluded via AI assistants. Specifically for account-based transactions where the consumer enters into a framework agreement covering future transactions upon creation of an account, the

repetition of most of the information set out in Article 6 CRD seems superfluous as they apply likewise to all transactions.

- *Proposed solution:* Not displaying this type of information increases the attention on the information essential for the consumer when making another transaction: The main characteristics of the goods or services and the price (and, in case of subscriptions, the duration of contract and conditions for terminating). The repetition of all other information is unnecessary because the consumer knows these are laid down in the framework agreement.

2. Modernize information requirements

- *Situation/Issue:* Moreover, the requirement in the CRD to provide a phone number and email for pre-contractual information is outdated. Likewise, the requirement to provide a withdrawal form for e-commerce purchases seems outdated. It does not reflect consumer expectations in digital environments nor consumer's market practice (e.g., simply returning goods without declaring a withdrawal first, using available means in their account or contacting customer support via electronic means).
- *Proposed Solution:* Real-time chat support is more aligned with what consumers expect and prefer.

3. Rebalance right of withdrawal for digital services

- *Situation/Issue:* For services that cannot be provided completely within a period shorter than 14 days, consumers may consume or "binge" the most valuable content they are interested in within the right of withdrawal period (e.g., over a weekend) and would then only incur the compensation obligation of a very small amount if calculated on a pro-rata basis from the monthly/annual/etc. price of the service (which may be way more costly to calculate and provide than issuing a full refund). As of now, the only way to mitigate these risks would be to introduce a rule that access to a digital media subscription service will only be granted 14 days after purchase. However, this would neither be in the interest of the consumer nor the business. This burden seems particularly heavy when it is borne solely out of uncertainty, because an offer cannot be clearly classified as a digital service or digital content due to a lack of sufficient guidance, and in case of doubt, it should be assumed to be a digital service.
- *Proposed solution:* We would welcome that the right of withdrawal for digital services can be excluded under similar circumstances as the right of withdrawal for digital content, at least with regard to digital services providing access to digital content.

b. Digital Networks Act

The simplification efforts should be applied to upcoming digital legislation as well. However, the

approach to the new Digital Networks Act (DNA) suggested in the European Commission's Call for Evidence (July 2025) appears to present challenges to the Commission's goals of simplification and deregulation. It proposes new regulatory requirements in addition to the recently adopted GiA and the recently implemented EECC. The DNA proposal seems inclined to include full regulation of Internet interconnection, even price regulation, despite this market consistently demonstrating high functionality and competitiveness, with no systemic market failure.

Therefore, we ask for the following to be taken into consideration ahead of the publication of the DNA:

- **Avoid unnecessary and costly regulation of IP interconnection**: We urge the Commission to avoid unnecessary proposals to impose new telecom regulation to the IP interconnection. The market remains highly competitive and functioning well, with no systemic market failure that would justify regulatory intervention like price regulation or dispute resolution/arbitration/coordination or similar mechanisms, which would, in practice, be the same as introducing network fees.
- **Maintain BEREC supervision**: BEREC should continue to monitor the IP interconnection market as it has done helpfully and expertly over a decade.
- **Oppose regulatory extension to cloud**: Cloud is not 'competing' with telcos, but rather becoming an integral, supporting technology for network operators. These services are already subject to appropriate and tailored regulation, like NIS2, DORA, DMA, etc, as decided by EU legislators. There is no evidence to suggest that the European telecom legislative framework should be extended to these providers. Doing so would only increase legal uncertainty and bureaucracy to operators.

c. Cloud and AI Development Act

We encourage the European Commission to prioritize regulatory simplification and coherence while designing and proposing CAIDA. To foster European growth, regulatory simplification should also prevent asymmetric and discriminatory regulations. It is crucial to **avoid new, overlapping rules** in an already crowded regulatory space and to fully implement existing EU legislation before introducing new initiatives.

Where CAIDA addresses sustainability and energy, we encourage consistency with the existing Energy Efficiency Directive (EED) and caution against Minimum Performance Standards (MPS) under CAIDA, as they could limit innovation and competitiveness. Instead, we call for the Commission's support of the modernization of European electricity grids and **investment in affordable, reliable carbon-free energy technologies**.