Insights

Open Loop | Meta

Simplifying the EU's Digital Rulebook

Open Loop Sprint EU Workshop Series 2025

Copenhagen • Brussels • Munich • Paris • Warsaw • The Hague

Contents

About Open Loop

Meta's Open Loop is a global program that connects AI experts, policymakers, and companies to help develop effective, evidence-based policies for AI and other emerging technologies. It does this by gathering detailed feedback on new or existing regulations, laws, or voluntary frameworks.

Starting in the Spring of 2025, we ran a series of Open Loop Sprint workshops on the topic of "Simplifying the EU's Digital Regulation", with a focus on the EU AI Act, the GDPR and the ePrivacy Directive. The series was conducted in Copenhagen, Brussels, Munich, Paris, Warsaw and the Hague from May to September 2025.

This report presents a synthesis of what we heard during those engagements both on identified challenges and proposed solutions for EU digital regulatory simplification.

How to cite this report?
Laura Galindo, Taja Naidoo "Simplifying the EU's Digital Rulebook: Insights Open Loop Sprint Workshop Series 2025", (December 2025), at https://openloop.org

The insights and recommendations contained in this report represent a synthesis of stakeholder input and policy analysis. These recommendations do not necessarily reflect the official positions of any participating people, organizations, host institutions, or government entities. Observing the Chatham House Rule, all quotations in this report have been anonymized.

Acknowledgements

The Open Loop team thanks those who participated in the workshops and shared their expertise and experience with us — this report is the direct result of their generosity.

Anne-Sofie Hansen, Legal Director, Lead of AI Legal, **Danske Bank**, Berglind Hallgrimsdottir, Senior Advisor, **Nordic Council of Ministers**, Daniel Fraga, Chief GenAI UXUI Designer, **Danske Bank**, Divya Dang, Senior Consultant, **KPMG**, Erik David Johnson, Chief AI Officer (CAIO), **Delegate**, Esbern Kaspersen, CTO, **KasparAI**, Frederik Refsgaard, Attorney-at-Law, Partner, **Hopp & Partners**, Geet Khosla, Co-Founder, CEO, **Proem AI**, Kenneth Gad, Head of Project Management, **Frankly**, Kristina Christensen, Manager, **KPMG PS**, Lars Bay Nielsen, Managing Director - Head of Public Sector, **Accenture**, Line Klit Olsen, CEO, **PUFIN-ID**, Mette Finnemann, Director, Digital Policy, **Danish Industry**, Mette Nikander, Associate Director-Security Lead DK, **Accenture**, Nanna Jannov, VP R&D Compliance, **Novo Nordisk**, Niels Torm, Associate Director, **Cognizant Technology Solutions Corporation**, Rasmus Bisgaard, Regional Business Lead Denmark, **Nvidia**, Roman Jurowetzki, Associate Professor, **Aalborg University / CAISA**, Simone Skovshoved, Head of Policy, **Danish Entrepreneurs**, Ulrik Vestergaard Knudsen, CCAO, **Netcompany**, Victoria Maria Cura Rodriguez, Consultant, **KPMG**, Alessandra Chiarini, Policy Adviser, **European Banking Federation**, Anna Sophia Oberschelp de Meneses, Special Council, **Covington & Burling LLP**, Boniface de Champris, Senior Policy Manager, **Computer & Communications Industry Association (CCIA)**, Charly Helleputte, Partner, **King & Spalding**, Elisa Lunardon, Innovation and Cybersecurity Trainee, **European Banking Federation**, Jerome Leclanche, CEO, **Ingram Technologies**, Jimmy Farrell, EU AI Policy Co-Lead, **Pour Demain**, Karolina Walczak, Director for Engagement, **Mastercard Europe**, Kristina Olausson, Policy Manager, **Volvo Cars**, Liselotte Dubois, Consultant, **Flint Global for Uber**, Marco Leto Barone, Policy Director, **ITI - Information Technology Industry Council**, Mariano Guillen, Head of Office, **Leidar**, Rafaela Nicolazzi, Head of Data & Privacy, **OpenAI**, Vasileios Rovilos, Senior EU Policy Manager, **Credo AI**, Arleta Adamus, Group General Counsel, **Inpost**, Aleksandra Czarnecka, Privacy & Data Protection Manager, **Agora S.A.**, Justyna Duszynska-Cichy, Deputy Director, **Ministry of State Assets Poland**, Sławomir Dziurzyński, Data Protection Expert, **Allegro**, Anna Jaworska-Kłosowicz, Data Protection Officer, **InPost**, Izabela Kowalczuk-Pakuła, Partner, **Bird & Bird Koremba**, Dziedzic i Wspólnicy sp.k., Krys Krol, Deputy Director, **UODO**, Mateusz Kupiec, Assistant Researcher, **Institute of Law Studies, Polish Academy of Sciences**, Adrianna Michałowicz, Assistant Professor, **University of Łódź**, Marcin Olender, Public Policy Director, **AI Chamber**, Szymon Sieniewicz, Counsel, Head of TMT/IP, **Addleshaw Goddard**, Ewa Stachowska, Head of Legal Compliance and Public Affairs, **Edenred Polska sp. z o.o.**, Emilia Stepien, Of Counsel, **Bird & Bird**, Anna Stępień, Lawyer, **Agora S.A.**, Monika Susałko, Partner, **Lubasz i Wspólnicy**, Blanka Wawrzyniak, Senior Regulatory Affairs Specialist, **Allegro**, Olga Zabolewicz, Regulatory Expert, **NASK- PIB**, Agnieszka Zachaj-Zafirow, Data Protection Officer, **PGE Polska Grupa Energetyczna S.A.**, Anna Popowicz-Pazdej, Partner, **Dentons**, Pawel Hajduk, Lecturer, **Cardinal Stefan Wyszynski University in Warsaw**, Alexandre Vagenheim, VP Global Legal Data, **Jus Mundi**, Ana Catarina De Alencar, Head of Legal and DPO, **EIT Manufacturing**, Clara Sikorski, Global Data Privacy Director, **Milliman**, Francesca Sheeka, EU Tech Policy Lead, **Talos Network**, Igor Versteeg, DPO, **Opella Healthcare Group**, Kévin Kok Heang, Chef de Projets IA, **DGE - Digital Economy Department - Ministry of Economy France**, Louise Bucaille, Global Public Affairs Manager, **L'Oréal**, Nathalie Laneret, VP, **Criteo**, Paola Galvez, AI Ethics Manager, **Globethics**, Riham Marii, Senior Policy Manager, **International Chamber of Commerce France**, Sebastián Rodríguez Alarcón, Business Engagement Practitioner, **OECD**, Sonia CISSE, Partner, **LINKLATERS LLP**, Thibaut Smouts, Partner Digital Risk, **EY**, Volha Litvinets, Responsible AI Manager | Digital Ethics Lead, **EY**, Wissem Addoun, AI & Data Privacy Attorney, **Franklin**, Nils Beers, CEO, **KickstartAI**, Annemarie Bloemen, Senior Strategic Advisor, **Directorate for Algorithm Coordination (DCA) - Autoriteit Persoonsgegevens (Dutch DPA)**, Freek Bomhof, Program Director, **TNO**, Maarten Botterman, Director, **GNKS Consult BV**, Patrick Das, VP of Finance & Legal, **Weaviate**, Tara Harris, Group IP Lead: Digital & Regulatory, **Prosus**, Andrew Harrison, GenAI Governance Advisor, **ABN AMRO**, Elisa Henry, Director of Global Privacy, **WSP Global Inc.**, Laure Jacquier, Director, **International Chamber of Commerce Netherlands**, Bart Karstens, Senior Researcher, **Rathenau Instituut**, Peter Kits, Partner, **KPMG**, Joy Koersen, Partner, **KPMG Cyber & TechLaw**, Cassandra Moons, Legal Director Compliance, **TomTom**, Lucas Noronha, Senior Privacy & AI Consultant, **DPO Consultancy**, Maartje Nugteren, AI Policy Fellow, **Mila - Quebec AI Institute**, Brend Plantinga, Senior Advisor, **Directorate for Algorithm Coordination (DCA) - Autoriteit Persoonsgegevens (Dutch DPA)**, Marijke Salters, Consultant Digital Transformation, **CIO Platform Nederland**, Marlou Snelders, Policy Advocate Digitalisation & Cybersecurity, **FME**, Kolja Verhage, Senior Manager AI Governance, **Deloitte**, Laurens Waling, Chief Evangelist, **8vance**, Brittany Hale, Senior Consultant, **Allianz Technology SE**, Catharina Glugla, Partner, **A&O Shearman**, Charlotte Schieler, Senior Associate, **Schürmann Rosenthal Dreyer**, Dr. Berndt Pilgram, Lead Product Data & Information Security Governance, **Fresenius Medical Care**, Elena Brandt, Senior Associate, **Freshfields**, Esthefania Vargas, Data Privacy Manager, **Carl Zeiss AG**, Florian Thoma, Sr Director, Data & AI Compliance, Privacy, **Accenture GmbH**, Frank Schemmel, Senior Director Privacy, Compliance & Public Policy, **DataGuard**, Kai Döpel, Data Protection Expert, **zooplus SE**, Luisa Reges, Data Governance, **BMW**, Marieke Merkle, Associated Partner, **Noerr PartG mbB**, Markus Sullivan, Corporate Data Protection Manager, **GLS**, Niels Beisinghoff, Senior Legal Counsel, **Allane SE**, Noha Lea Halim, PhD Candidate, **Technical University Munich**, Ozge Dulger, Privacy Monitoring Specialist, **Allianz**, Patrick Agostini, Co-Founder & CEO, **PRICOM**, Ronnit Wilmersdörffer, Senior Compliance Officer, **Aleph Alpha**, Sarah Klein, Legal Privacy Counsel, **Yoummday GmbH**, Stephan Dobrowolski, Director of EMEA Legal, **Onsemi (ON Semiconductor)**, Sven Hölzel, CTO, **Trail GmbH**, Wojciech Kleta, Privacy Counsel / Syndikusrechtsanwalt, **Allianz SE**, Andreas Preißer, Head of Business Relations, **Bayerische KI-Agentur / BAIOSPHERE**, Lejla Rizvanovik, CEO, **Servus Data Group GmbH**, Nicole Staub, Corporate Counsel, **Slalom GmbH**.

Acronyms and Abbreviations

This report utilizes the following acronyms and abbreviations for clarity and conciseness:

EU AI Act or EU AIA	European Union Artificial Intelligence Act
CNIL	Commission Nationale de l'Informatique et des Libertés
DMA	Digital Markets Act
DSA	Digital Services Act
DPA	Data Protection Authority
DSARs	Data Subject Access Requests
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
ePD	ePrivacy Directive
EU	European Union
FLOP	Floating point operation
GDPR	General Data Protection Regulation
GPAI	General-Purpose Artificial Intelligence
ISO	International Organization for Standardization
LLMs	Large Language Models
OSS	One Stop Shop
PIB	Public Information Body
SCD	Special Categories of Data (as per the General Data Protection Regulation, Article 9)
SMEs	Small and Medium-sized Enterprises

Executive Summary

This summary synthesizes findings from six co-creation workshops hosted by Open Loop between June and October 2025 across Copenhagen, Brussels, Munich, Paris, Warsaw, and The Hague. We brought together 120 participants — industry leaders, legal practitioners, data protection officers, AI developers, and governance experts — to discuss and identify implementation challenges related to the EU Digital Acquis. The workshops also sought to develop concrete solutions which can help simplify regulation and stimulate innovation and competition in the EU, and to make a contribution to the European Commission's efforts as part of the Omnibus Simplification Package.

Building on our previous Open Loop EU AI Act policy prototyping program,[1] our workshop methodology centered on structured co-creation: participants identified specific challenges through their own professional experiences, clustered themes to reveal systemic patterns, then brainstormed actionable solutions ranging from immediate technical fixes, to long-term structural reforms. The conversations were grounded in real-life scenarios and specific examples of regulatory barriers and issues, as well as practical proposals for improvement.

What emerged was a remarkably consistent picture across countries, sectors, and company sizes. The challenges posed to European business by the EU regulatory approach are numerous, systemic and impactful, and they emerge from a complex interplay of legal frameworks, structural issues and cultural orientation. While there are over 100 digitally-focused laws in the EU, the main concerns related to the implementation and interaction of the GDPR, ePrivacy Directive, EU AI Act, with the DSA and DMA also mentioned, though to a lesser extent. Companies who are not designed "gatekeepers" under the DMA or "VLOPs" under the DSA reported many fewer concerns with these Acts.

Therefore, we have focused on presenting insights related to overlaps and challenges with the GDPR, ePrivacy Directive and EU AI Act, as these three were deemed the most relevant and applicable to the European companies who participated in the workshop series.

1 https://openloop.org/programs/open-loop-eu-ai-act-program/

The Regulatory Iceberg Framework

The challenges identified in the workshops can be encapsulated in a mental model we call “The Regulatory Iceberg.” The visible problems represent the “tip” of this iceberg. Beneath, lie deeper structural and cultural barriers that reinforce and compound this legal complexity. The following chapters of this report explore these dimensions in detail. However in summary, The Iceberg framework has three interconnected layers of challenges, each requiring distinct solutions over different timeframes, and implementation by different actors in the regulatory and policymaking ecosystem In many cases we have suggested who the most relevant actor might be in terms of implementing a specific recommended solution, however in quite a number of cases further discussion is needed to understand the detailed action steps which would accompany each recommendation.

Layer 1

Legal Incoherence
Vague definitions and overlapping obligations undermine clarity within, and between, regulations

Layer 2

Institutional Fragmentation
Inconsistent rule application across authorities causes confuion

Layer 3

Innovation-averse Mindset
Exclusive focus on risk assessment and mitigation hampers innovation

LAYER 1:

Legal barriers — pervasive legislative incoherence

Europe's digital regulatory frameworks have become operationally incoherent. The EU AI Act contains many vague definitions—such as "AI Systems" and "AI Literacy"—that even legal experts dispute, while key GDPR concepts like "anonymization" remain unsettled. Overlapping provisions create direct conflicts: Article 9 of the GDPR restricts the use of Special Category Data (often colloquially referred to "sensitive data"), yet the AI Act would require the processing of data such as religion or ethnicity to engage in bias testing as a mitigation measure. Instead of clarifying, official guidance often deepens uncertainty rather than resolving it, with some participants describing it as "anti-guidance." Outdated provisions, including almost the entirety of the ePrivacy Directive, and the "FLOPs-based" threshold for GPAI in the EU AIA further highlight how regulation lags behind technology. The result is a costly and confusing maze of red tape, where businesses must invest heavily in legal services to understand and interpret which rules apply to them, when, and how.

LAYER 2:

Structural barriers — challenges in institutional fragmentation

Beneath the legal complexity and contradictions lies a fragmented governance and enforcement landscape. National sovereignty and divergent regulatory philosophies create inconsistent approaches to digital lawmaking and enforcement. Some member states “gold-plate” EU rules, requiring companies to go further beyond the measures outlined in the EU legislation, leading to compounding costs and confusion. New authorities, established under an ever-increasing number of national and European legal instruments, issue contradictory interpretations, especially of the GDPR. Enforcement approaches vary significantly across member states, sometimes creating tension rather than cooperation among authorities, while many lack the technical expertise to assess the technologies they oversee. The consequence is widespread uncertainty not just about the laws themselves but also who advises on them, who enforces them, and how: businesses struggle to obtain clear, consolidated answers, which hinders long-term planning and deters innovation and investment in Europe.

LAYER 3:

Cultural barriers — an innovation-averse mindset

Most fundamentally, participants identified a regulatory and enforcement culture that inhibits innovation. A “zero-risk” or fear-based mindset prioritizes theoretical risks and the demonstration of exhaustive ex-ante compliance work over practical, consumer-oriented solutions. Regulators are often reluctant to engage with companies, whether through lack of resources or due to concerns around impartiality, and this creates mistrust. Consequently companies are discouraged in the use of tools such as sandboxes, as they do not want to risk exposing themselves through trying new ideas in an environment which does not feel “safe”. It also deprives the regulator and relevant authorities of another communication channel through which to learn from companies and technologists, helping them stay up-to-date and informed about the latest technologies. This disconnect between policymaking and implementation leads to missed deadlines, wasted resources, and an overemphasis on “tick-box” exercises. Companies, especially SMEs, are forced to spend scarce resources on documentation rather than genuine risk assessment or product development. The cumulative effect is a stifled innovation pipeline, with Europe’s regulatory culture itself becoming a barrier to building new products and business models.

Key messages

1 The Regulatory Iceberg Reveals Deep, Systemic Challenges

The challenges to the EU's digital single market are not merely isolated legal conflicts but are rooted in a systemic confluence of legislative incoherence, fragmented institutional governance, and an innovation-inhibiting regulatory culture. Effective policy must address all three layers of the "Regulatory Iceberg" simultaneously to achieve sustainable simplification.

2 Current Simplification Efforts are Necessary but Insufficient for Effective Reform

While current simplification efforts are a start, the widespread and systemic nature of the challenges identified—including conflicts between the GDPR and EU AI Act—demonstrates that much more is required to boost European innovation. Urgent and ambitious reform is necessary to move beyond immediate fixes.

3 Achieving Digital Competitiveness Requires a Paradigm Shift in Governance and Cooperation

This must be the beginning, not the end—a renewed European digital social contract is essential. Europe's future success in fostering digital innovation will hinge on an ambitious shift from a reactive, 'zero-risk' enforcement model to a proactive, regulatory learning culture. This necessitates strengthening formal, robust cooperation mechanisms with the full ecosystem (industry, SMEs, researchers) to ensure policy design is evidence-based, future-proof, and technologically informed.

The insights captured in this Executive Summary underline the calls for urgent and radical regulatory simplification as outlined in the September 2024 “Draghi report”. The need for clarity, consistency, and a pro-innovation approach is particularly acute at the intersection of the EU AI Act and data privacy frameworks, and Europe must quickly change course. The current Digital Acquis, characterized by systemic complexity, institutional fragmentation, and innovation-adverse culture, is fundamentally undermining European digital competitiveness, while failing to deliver meaningful protection and opportunities for citizens and businesses alike.

The final Digital Omnibus package[2] (published on 19 November 2025) represents progress on several fronts, including centralized enforcement, harmonized DPIA and breach notification processes, and expanded support for SMEs. However, significant gaps remain—particularly regarding the lack of a comprehensive implementation pause, the absence of an explicit innovation mandate, persistent legal and operational fragmentation, and the need for deeper cultural and structural reform. The Digital Omnibus and Digital Fitness Check represent crucial moments to address these shortcomings—but only if they meet the level of ambition needed.

2 Digital Omnibus Regulation Proposal, European Commission: https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal

Introduction

Since the release of the Draghi report in September 2024,[3] which called for drastic efforts to drive European competitiveness and innovation, the Member States and industry of the European Union have been increasingly vocalizing calls to simplify and clarify existing regulations.

Building on the emerging recognition among European policymakers that Europe needs a fresh approach to governance in an age of increased technological innovation and competition, the Open Loop Sprint Co-design Workshop Series on Regulatory Simplification in the EU sought to understand what challenges European companies face as they try to innovate, and identify practical solutions to these challenges.

We engaged over 120 business leaders as well as AI governance and data protection experts from 6 countries. From these conversations, we identified a variety of concerns with the EU's fragmented and burdensome digital policy ecosystem. The workshops provided a platform for gathering companies and other stakeholders to participate in a structured, collaborative research effort on EU simplification and innovation strategies. Specifically, participants were invited to share their deep expertise and practical day-to-day experiences of building products to inform better policy making for AI and other emerging technologies in the EU.

This report is structured into two main parts: an Executive Summary is followed by three sections unpacking the 'Regulatory Iceberg' framework across legal, structural, and cultural layers. Each layer of the iceberg, includes succinct analysis boxes detailing ideas for a way forward as discussed during these workshop sessions and a short note assessing how the recently introduced Digital Omnibus package captured these, each are integrated under each layer.

3 European Commission (EC) 2025

This section of the report summarizes key insights shared about the challenges workshop participants are facing in implementing and preparing for European digital legislations, particularly the GDPR, ePrivacy Directive and the EU AI Act. The evidence suggests an urgent consensus that incremental regulatory adjustments cannot address the systemic failures undermining EU digital competitiveness. Current digital regulation creates a “Regulatory Iceberg” where visible compliance challenges mask deeper institutional issues. The workshops consistently identified fundamental ambiguities across multiple regulatory frameworks that create compliance uncertainty and regulatory fragmentation. These challenges manifest across distinct categories or layers requiring urgent interventions.

Layer 1

Legal Incoherence
Vague definitions and overlapping obligations undermine clarity within, and between, regulations

Layer 2

Institutional Fragmentation
Inconsistent rule application across authorities causes confuion

Layer 3

Innovation-averse Mindset
Exclusive focus on risk assessment and mitigation hampers innovation

Figure 1: The Regulatory Iceberg

Note: The Iceberg model illustrates why comprehensive reform requires addressing all three layers simultaneously. Like an iceberg, the most visible challenges— legal complexity and lack of clarity — represent only a small portion of the total problem. Just below the surface lies institutional fragmentation: the proliferating authorities, inconsistent enforcement, and capacity gaps that create systemic uncertainty. But the largest and most fundamental challenges lie deepest: the cultural barriers of technological inexperience, risk-averse enforcement, and innovation-adverse mindsets that pervade the entire digital ecosystem.

TOP LAYER OF THE ICEBERG

Legal issues

A severe lack of clarity, outdated technical guidance and friction between the EU AI Act and GDPR is preventing companies from effectively complying or innovating, and is limiting European economic development. The issues below have been identified and synthesized from across the six workshops we held, and were well-evidenced by the specific examples which the participants provided.

A Lack of clear definitions and concepts

Workshop discussions highlighted that the current EU digital regulatory landscape is marked by significant conceptual and definitional ambiguities. Three main areas of concern emerged. First, definitional ambiguity undermines the practical application of key concepts and, in some cases, produces internal contradictions. Second, procedural complexity generates uncertainty and administrative burdens that can inhibit effective implementation. Third, cross-framework inconsistencies and potential conflicts create overlapping or contradictory obligations (See subsection below).

See Annex II for a comparative table of key definitions and concepts identified as problematic by stakeholders.

The interaction between the AI Act and existing data protection legislation exemplifies these challenges. For instance, the EU AI Act contains vague definitions—such as 'AI Systems' and 'AI Literacy'— that even legal experts dispute, while key GDPR concepts like 'anonymization' remain unsettled. Divergent interpretations of core terms and obligations at this regulatory interface have contributed to legal uncertainty and operational inefficiencies. These issues risk discouraging innovation and investment in AI and data-driven technologies. As additional layers of digital regulation are introduced, the absence of a coherent and harmonized conceptual framework may further compound these difficulties.

B Conflicting obligations between the AI Act, GDPR and ePD

B1. Special category data (SCD) and bias mitigation

Participants identified one of the most prominent challenges as the direct tension between the requirements of the AI Act and those of the GDPR, which places organizations in a difficult compliance position. A frequently cited example concerns the use of special category data for bias testing in "high-risk AI systems" (see subsection C). The AI Act obliges developers to test for and mitigate bias—an activity that often requires processing sensitive personal data. However, participants noted a misalignment with the GDPR's provisions governing such processing. The AI Act applies a stricter necessity standard, requiring that data use be "strictly necessary," whereas the GDPR uses the broader term "necessary." This subtle but potentially significant divergence introduces legal uncertainty regarding the appropriate legal basis for processing, reflecting the broader issue of definitional ambiguity across frameworks.

Another confounding issue is with the definition of bias itself. The absence of a clear and operational EU-level definition—rooted in European fundamental rights principles rather than U.S. anti-discrimination frameworks—creates difficulties for global companies seeking to align their AI governance and testing methodologies. This conceptual uncertainty further reinforces the need for greater definitional coherence across the Digital Acquis.

Further complexity arises from the AI Act's requirement to delete data once bias testing is complete, which conflicts with the iterative nature of bias monitoring. Because bias detection is an ongoing process rather than a one-time event, organizations may be forced to repeatedly collect and process sensitive data, generating both operational inefficiencies and compliance risks.

B2. Anonymization

Participants consistently highlighted the difficulty of understanding whether they would need to apply GDPR principles in the context of AI development and deployment, or whether the usage is outside its scope. If data used in AI training is deemed "personal data", the near impossibility of achieving a compliant level of effective anonymization regarding this data essentially prevents companies from using it. As expressed in The Hague, "it feels absolutely impossible, so I think most of us are giving up [on developing products using AI foundation models]." This lack of clarity and general misapprehension around how data can be used in AI model training and development in the EU is a significant practical limitation that leaves companies in a state of ongoing legal uncertainty when working with the large datasets essential for innovation.

B3. ePrivacy Directive Conflicts

An additional concern raised related to the continued application of the ePrivacy Directive, which participants described as outdated and burdensome. Its implementation — particularly through pervasive cookie consent banners — was cited as a source of user fatigue and operational inefficiency. The Directive's overlap with the GDPR in areas such as consent management already creates confusion for organizations, prompting some participants to suggest integrating ePrivacy provisions into the GDPR to promote coherence and simplicity.

C Divergent definitions and assessments of risk

One of the most significant challenges identified by participants was the fundamental misalignment in how risk is defined, assessed and classified across the EU AI Act and GDPR. This divergence creates situations where companies face contradictory regulatory signals about the same activity, undermining legal certainty and compliance planning.

A company may determine that its AI system does not meet the criteria for a “high-risk” classification under the AI Act, while a Data Protection Authority (DPA) may independently assess the same activity as “high-risk” under the GDPR due to the nature of the data processing involved. As one participant remarked, this results in an untenable situation, actually experienced by one of the workshop participants, in which a business was effectively told by one legal regime that its processing was “compliant,” while another simultaneously categorized it as high risk — leaving organizations to reconcile contradictory assessments with limited guidance, and with the potential of being fined for non-compliance. This discourages innovation in the EU.

This tension is further exacerbated — again — by inconsistencies in core definitions across legal instruments. Terms such as “provider,” “deployer,” “personal data,” and “AI system” are defined differently depending on the regulatory context, complicating efforts to map obligations and risk management activities along the AI value chain. Participants noted that this misalignment makes it particularly challenging to ensure coherent compliance strategies, especially for multinational organizations operating across multiple jurisdictions.

The depth of frustration expressed across workshops—particularly in Copenhagen, Brussels, and Munich—was reflected in several proposals for substantial regulatory reform. Some participants suggested condensing and integrating the AI Act into the GDPR, perhaps as an Annex which should be viewed as AI-specific guidance. In terms of what else in the EU AIA could be condensed, participants suggested removing Chapter V on General-Purpose AI Models, which they viewed as likely to become irrelevant within a short time frame.

More moderate recommendations focused on developing a common risk classification framework applicable across the GDPR, the AI Act, and other digital legislation. Participants argued that such a harmonized approach could help prioritize regulatory focus on issues that matter most to individuals and to society, while reducing unnecessary duplication and conflict across legal instruments.

D Outdated legal provisions and lack of “future-proofing”

Workshop participants consistently highlighted that the AI Act "predates much of today’s AI innovation and the widespread adoption of foundational AI technology like large language models."

Specific obsolescence issues identified by participants include, for example:

- Capability Measurement Methods: Provisions for measuring AI capabilities that have become technically obsolete.
- GPAI Model Regulation: Chapter V regulations developed in just nine months without adequate scientific foundation.
- Technology-Specific Restrictions: Rules designed for earlier AI generations creating barriers for advanced systems.

Participants across all workshops emphasized that the length and vagueness of EU digital regulations often necessitate supplementary guidance to aid interpretation and implementation. However, this reliance on post-legislative clarification has created additional challenges. As one participant in Warsaw described, the current system is “anti-guidance,” producing more confusion than clarity, sometimes creating additional interpretive questions. Others observed that guidelines “come quite late or not at all,” and when they do appear, they are often too general or inconsistent to provide meaningful support.

One participant offered a pointed critique of the overall process: “You have the impression that you park issues to get a political agreement and then you hope to resolve those in guidelines, that kind of just reopen more discussion and create even less [clarity] compared to what they are supposed to create.” This sentiment was broadly endorsed by other workshop participants, reflecting discontent with the perceived overreliance on guidance as a substitute for the legislative precision.

D1. Timing and availability of guidance

The timing of guidance publication emerged as a central concern. Participants repeatedly noted that guidance is released too late to inform companies’ implementation strategies and typically lacks the practical detail required for compliance planning. When issued, guidance often reflects a single regulator’s interpretation rather than a coordinated, cross-framework perspective aligned with the realities of modern digital businesses. Several participants warned that the absence of timely guidance—particularly regarding high-risk AI—may discourage investment and slow Europe’s progress in emerging sectors such as AI in healthcare.

D2. Content and utility of guidance

Concerns also extended to the content and utility of existing guidance. Participants in Copenhagen stressed the need for “practical, implementable guidelines instead of composing so many theoretical concepts.” Many viewed current documents as overly abstract, focusing on broad legal principles rather than concrete examples or operational scenarios. This disconnect between regulatory intent and implementation practice leaves companies without actionable roadmaps, undermining both compliance and innovation.

Together, these discussions revealed a fundamental gap between the production of regulatory guidance and the practical needs of companies attempting to apply it, reinforcing calls for clearer, more timely, and more operationally grounded materials.

BOX 1

Resolve Legal Clarity and Incoherence

While participants called for considering a strategic implementation pause on the AI Act, the Digital Omnibus (published 19 November) instead created a grace period for high-risk AI systems, with deadlines contingent upon the Commission's confirmation of supporting measures. The package also introduced targeted clarifications, including expanding exceptions for processing special category data (SCD), clarifying legitimate interest grounds for AI development, and consolidating cookies rules under the GDPR and ePrivacy Directive. Despite this progress, the absence of a fixed pause for the General-Purpose AI Models (GPAIM) regime, the flexible timeline for high-risk systems, gaps remain on inference-based SCD, full alignment of the ePrivacy Directive with GDPR legal bases, and the continued discretion of national DPAs maintain a significant degree of uncertainty.

The Omnibus consolidates cookie and tracking rules under the GDPR for personal data, but a dual regime persists for non-personal data, and consent remains a bottleneck. Further simplification is needed to address these persistent complexities and to ensure a unified, user-friendly approach to data protection and privacy.

A more comprehensive, long-term strategy for regulatory harmonization is needed to align definitions and ensure consistent, risk-based application across all frameworks.

To counter the perception of "anti-guidance" being produced by regulators, participants strongly recommended that supervisory authorities issue joint, pre-aligned guidance to provide market certainty. The Omnibus makes progress on harmonizing DPIA and breach notification templates, but further alignment is needed for other key concepts and operational guidance. The EDPB is expected to be working on joint guidelines with the European Commission to clarify the relationship between the AI Act and GDPR, though the timeline remains uncertain. However, future success depends on ensuring that this consolidated guidance is truly timely, pragmatic, consistent, and grounded in real use cases, including practical templates and examples, rather than just theoretical principles.

MIDDLE LAYER OF THE ICEBERG

Structural issues

A persistent theme across all workshops was the profound sense of anxiety created by fragmented enforcement and inconsistent interpretations of digital regulations, particularly the GDPR. Many participants expressed deep concern that the lessons from the GDPR's challenging implementation and failures of its one-stop-shop (OSS) mechanism are not being learned, and that the EU AI Act's complex, multi-layered enforcement architecture is poised to replicate and even amplify these problems. This fragmentation undermines the core promise of a harmonized Digital Single Market, creating a confusing and unpredictable environment where a company's compliance obligations can change drastically simply by crossing a regional or even national border within the EU.

A The authority proliferation problem

Participants consistently highlighted the problem of having "too many enforcers" with respect in particular to GDPR, each with their own agendas and interpretations. This is especially acute in federalized Member States like Germany, which has 16 state-level data protection regulators, one for each of its federal states, plus a federal data protection commissioner (BfDI) for federal public sector bodies and telecommunications providers. The AI Act is seen as worsening this, with one participant noting, "There are way too many authorities that are responsible... that creates risk of regulatory uncertainty". This structure forces companies who are operating across the EU to navigate a complex web of different national and sectoral authorities, each with potentially different views and interpretations of key regulations.

The workshops revealed systematic discoordination in regulatory architecture:

- Market Surveillance Authority Confusion: Brussels participants noted that companies "don’t even have clarity on who is the Market Surveillance Authority," under the AI Act, reflecting fundamental institutional design failures.
- Cross-Border Coordination Breakdown: Unlike GDPR’s one-stop-shop mechanism, the AI Act creates complex multi-authority interfaces where "companies must engage with multiple national Market Surveillance Authorities for general compliance across and within different Member States."

The scope of regulatory fragmentation across digital governance exceeds many policymakers' awareness. As noted in the Draghi report, the EU has approximately 100 tech-focused laws and over 270 regulators across member states, and this number is increasing. Critically with respect to the enforcement of the AI Act, at this point it is still unclear what the role of the AI Office will be, and how it will coordinate with other regulatory authorities. This issue is especially acute when there is also a lack of clarity about who the Market Surveillance and Notifying Authorities are within some Member States, as some countries appear to have missed the deadline for

formally designating these “National Competent Authorities” (NCA), which passed on 2 August 2025. Spain and Poland have indicated that they will be establishing new AI regulatory bodies, adding to an already crowded field.

The practical impact emerges clearly in workshop discussions. Companies report basic uncertainty about "who to go to" when seeking guidance or reporting compliance issues. Some oversight authorities remain unestablished, leaving businesses without clear regulatory contacts. This administrative opacity prevents effective compliance among companies who are seeking to meet regulatory requirements.

B Differences in enforcement approach and priorities

At the workshop in Brussels, some participants raised "questions about political enforcement or enforcement that is not justified… by the rules," while others highlighted how enforcement varies dramatically "depending on the political will” of various DPAs as a clear example of how GDPR enforcement is not uniform.

Gold-plating (a term used to describe the process whereby the powers of an EU directive are extended when transposed into the national laws of a Member State) emerged as potentially being a systematic problem rather than isolated incidents. The Paris workshop specifically mentioned how "France and Germany gold-plated most of the legislation, which makes it very difficult for organizations to navigate the maze." This creates multiple compliance regimes within supposedly harmonized EU law, defeating single market objectives.

C Issues of GDPR Interpretation which are exacerbated in the age of LLMs

C1. Data subject rights

Further complications arise from the application of Data Subject Access Requests (DSARs); they present a specific operational and legal complexity, moving beyond traditional data protection concerns. Participants in Munich noted that DSARs are "misused" in practice, often serving purposes other than their intended function of providing data access. This misuse includes using DSARs to facilitate "litigation, to get to information," or simply "to just create a big pain point for the other side and move them towards compensation interests". This deployment of DSARs as a legal tactic substantially increases the complexity and cost to compliance efforts for companies, especially those managing large-scale AI systems. Furthermore, this administrative burden is exacerbated by the legal framework itself: the scope of what companies are actually obligated to provide in response to a DSAR is considered "extremely unclear".

C2. Right to rectification

The right to rectification presents an especially difficult case. Participants described it as “incredibly difficult and costly to implement” in the context of large language models and other complex AI architectures. One participant cited OpenAI’s position, accepted by the French Data Protection Authority (CNIL). However, this is currently "the only position in Europe," and there is a critical need for an official position at the European level to address this conflict between technical feasibility and data rights, that users should “shift from a rectification to a larger filter [for outputs or results],” since retraining massive models to correct individual data points is technically infeasible. This example illustrates a broader conflict between data rights and technical feasibility, leaving companies to navigate inconsistent national interpretations within the EU.

D Capacity and knowledge gaps around AI

At the workshop in Brussels, some participants raised "questions about political enforcement or enforcement that is not justified… by the rules," while others highlighted how enforcement varies dramatically "depending on the political will” of various DPAs as a clear example of how GDPR enforcement is not uniform.

Gold-plating (a term used to describe the process whereby the powers of an EU directive are extended when transposed into the national laws of a Member State) emerged as potentially being a systematic problem rather than isolated incidents. The Paris workshop specifically mentioned how "France and Germany gold-plated most of the legislation, which makes it very difficult for organizations to navigate the maze." This creates multiple compliance regimes within supposedly harmonized EU law, defeating single market objectives.

BOX 2

Omnibus Centralization Efforts and Persistent Gaps

While the Digital Omnibus focused predominantly on legal coherence (Layer 1) and certain GDPR/AI Act overlaps, the fundamental structural issues underpinning institutional fragmentation—including the "authority proliferation problem" and differences in national enforcement philosophies—remain unaddressed, necessitating deliberate reform action.

The Omnibus has taken some steps by attempting to streamline oversight with the AI Office, harmonizing DPIA and breach notification templates, and strengthening data subject rights abuse prevention. Yet, a comprehensive review of the enforcement model, further capacity-building, and robust cross-border coordination remain essential to ensure consistent, pragmatic regulation across the EU. More work will be needed to truly shift toward learning-oriented enforcement, with clear differentiation between genuine, unintentional errors and willful non-compliance.

BOTTOM LAYER OF THE ICEBERG

Cultural issues

A An innovation-averse, anti-competitive mindset across agencies and institutions

Beyond the sheer volume and complexity of digital laws, companies face a deeper challenge: a regulatory culture that acts as a “hidden tax on innovation.” As one participant in Copenhagen observed, this environment “infects velocity, infects innovation, and maybe even infects [long-term] culture” within companies—suggesting that anti-innovation norms are both a cause and a consequence of Europe’s current regulatory approach.

This challenge extends beyond overlapping statutes or unclear provisions. It reflects a broader mindset of fear and risk aversion that prioritizes control over progress. Participants described how this culture creates an adversarial relationship between regulators and industry, stifles growth, and positions the EU as a place where innovation is managed rather than encouraged.

Many contrasted this with the United States and China, where world-leading large language models (LLMs) have emerged while the EU lags behind. One participant noted, “In Europe, the first question is often, what are the rules, boundaries, and limitations I need to establish first… before we can even discuss what this technology (AI) can be used for?” By contrast, competitors ask, “Can I build this? Can I go on and do these kinds of things?” This difference, participants argued, reflects a cultural tendency to be “pro-regulation first, not innovation first.”

A participant in Paris further highlighted that this mindset is embedded in the legislative process itself—“drafted by lawyers for lawyers”—producing texts that are opaque and difficult for innovators to navigate.

Across all six workshops, participants described a pervasive regulatory culture marked by limited resourcing and literacy, punitive enforcement, a lack of trust between regulators and businesses, and a disconnect between policymaking and market realities. This culture not only slows compliance but fundamentally reshapes how companies approach innovation in Europe, constraining adoption and scalability.

B Lack of consideration for societal and economic benefits

Many participants described a regulatory and legal culture that prioritizes the protection of individual, non-collective rights over economic and social benefits broadly. This suggests a cultural perception that regulators currently lack an explicit responsibility to foster innovation which can benefit the majority.

There was a strong feeling that regulators approach technology with a negative bias, focusing immediately on risks to individuals and small groups rather than engaging in a balanced cost-benefit analysis which takes a more holistic, cross-society approach. Participants advocated for more stakeholder involvement and a move toward "use cases" to define real risks based on evidence, suggesting the current approach could be better informed by the everyday uses and benefits of technology to citizens of the EU.

C Punitive "zero-risk" enforcement culture erodes trust

Highlighting the erosion of trust between regulators and European companies, one participant shared an example of receiving a warning letter merely for utilising AI in a way and within a sector (Recruitment) which would likely be categorized as "high-risk" under the EU AIA, despite "not doing anything wrong," prompting the question: "Are we building trust for [sic] the public, or are we trying to scare them?"

This lack of trust extends to regulatory sandboxes, which are intended to provide safe environments for experimentation and collaboration. In practice, companies reported perceiving them as potential risk vectors, rather than opportunities. Several participants expressed fear that participation might place them "on the regulator's radar" (as a company trying some unconventional, though not necessarily non-compliant things), deterring engagement and undermining the sandbox's purpose as a cooperative testing space.

Across workshops, companies described a dynamic in which they are presumed non-compliant and must continuously demonstrate their conformity. A participant in Munich characterized this as a "reverse burden of proof," noting that "you have to [constantly] prove you're compliant, so that's really not helpful." This sentiment reflects a broader perception of opacity and unpredictability in enforcement. As another participant in The Hague observed, "it's very easy to get a fine, but it's very hard to get clarity, which feels very unfair."

Some participants reported that even after substantial investment in compliance documentation, authorities can retrospectively question company interpretations of ambiguous rules, effectively shifting all responsibility onto the organization to justify past decisions. This dynamic was seen as reinforcing defensiveness rather than collaboration.

The combination of a risk-averse culture, broken trust, and a reversed burden of proof has led many companies to view the regulatory environment as punitive rather than supportive. Authorities are perceived less as partners in navigating emerging technologies and more as entities “waiting to find fault”, focused primarily on compliance verification rather than collaborative problem-solving.

Many participants identified this zero-risk culture as a core structural challenge within the EU’s digital regulatory system—an institutional mindset that discourages experimentation, learning, and proportionate risk-taking. Without addressing this underlying cultural dynamic, participants cautioned that technical or procedural reforms alone will be insufficient to restore trust or strengthen Europe’s global competitiveness in innovation.

BOX 3

Omnibus Omissions and the Persistence of the Cultural Gap

The most profound and persistent barrier identified in the Open Loop workshops is the deeply embedded risk-averse, zero-tolerance enforcement culture that characterizes much of Europe’s digital regulatory environment. While the Digital Omnibus package introduces important technical and administrative simplifications, it deliberately avoids amending the fundamental objectives and mindset of the digital rulebook. As a result, the Omnibus misses the opportunity to address the deeper cultural and institutional gaps that continue to stifle innovation.

The majority of participants consistently called for a transformation toward a learning-oriented regulatory model, emphasizing the need for explicit innovation mandates for regulators—such as Data Protection Authorities and the AI Office—to ensure a balanced approach between protection and economic progress. Participants also advocated for the establishment of permanent stakeholder forums to enable continuous, structured dialogue between industry and authorities, and for the creation of “real” cross-border regulatory sandboxes that provide legal certainty and a presumption of conformity for participants. These mechanisms are seen as essential to foster trust, enable experimentation, and support adaptive, evidence-based regulation. Addressing these omissions is critical if Europe is to move beyond incremental fixes and achieve a genuine paradigm shift toward digital competitiveness and regulatory trust.

Conclusion

Insights from the Open Loop Workshop Series highlight an urgent need for systemic simplification of the EU's digital regulatory framework, particularly at the intersection of the AI Act and data protection laws. Europe's current system—marked by complexity, fragmentation, and risk aversion—is seen as undermining competitiveness while failing to deliver proportionate protection for citizens and businesses.

Participants called for pragmatic, coherent, and concise frameworks that reduce duplication and regulatory burdens across the Single Market. They urged the European Commission, Data Protection Authorities, and the AI Office to coordinate more closely and engage meaningfully with stakeholders to avoid further fragmentation.

The European Commission's Omnibus Simplification process was identified as a critical opportunity to act. Participants agreed that incremental fixes are insufficient: the challenges are structural but solvable, provided there is political will. Industry stakeholders expressed strong readiness to partner in designing and implementing reforms.

Recent initiatives by the European Commission demonstrate growing awareness of these implementation challenges. The launch of the AI Office Help Desk in late 2025 and the Single Information Platform, represents important first steps toward providing businesses with clearer guidance and more streamlined regulatory interfaces. These efforts signal a welcome shift toward more practical, business-facing support mechanisms. However, as workshop participants consistently emphasized, such measures—while valuable—address only a fraction of the systemic challenges identified in this report. The Help Desk, for example, can assist with navigating existing requirements but cannot resolve the underlying legal conflicts, definitional ambiguities, or institutional fragmentation that create confusion in the first place.

What is needed is not merely better navigation of a complex system, but fundamental simplification and harmonization of the system itself. The EU Commission's Omnibus Simplification Package provides the necessary vehicle for such comprehensive reform, and industry stakeholders stand ready to contribute their expertise to ensure these efforts deliver meaningful, lasting change.

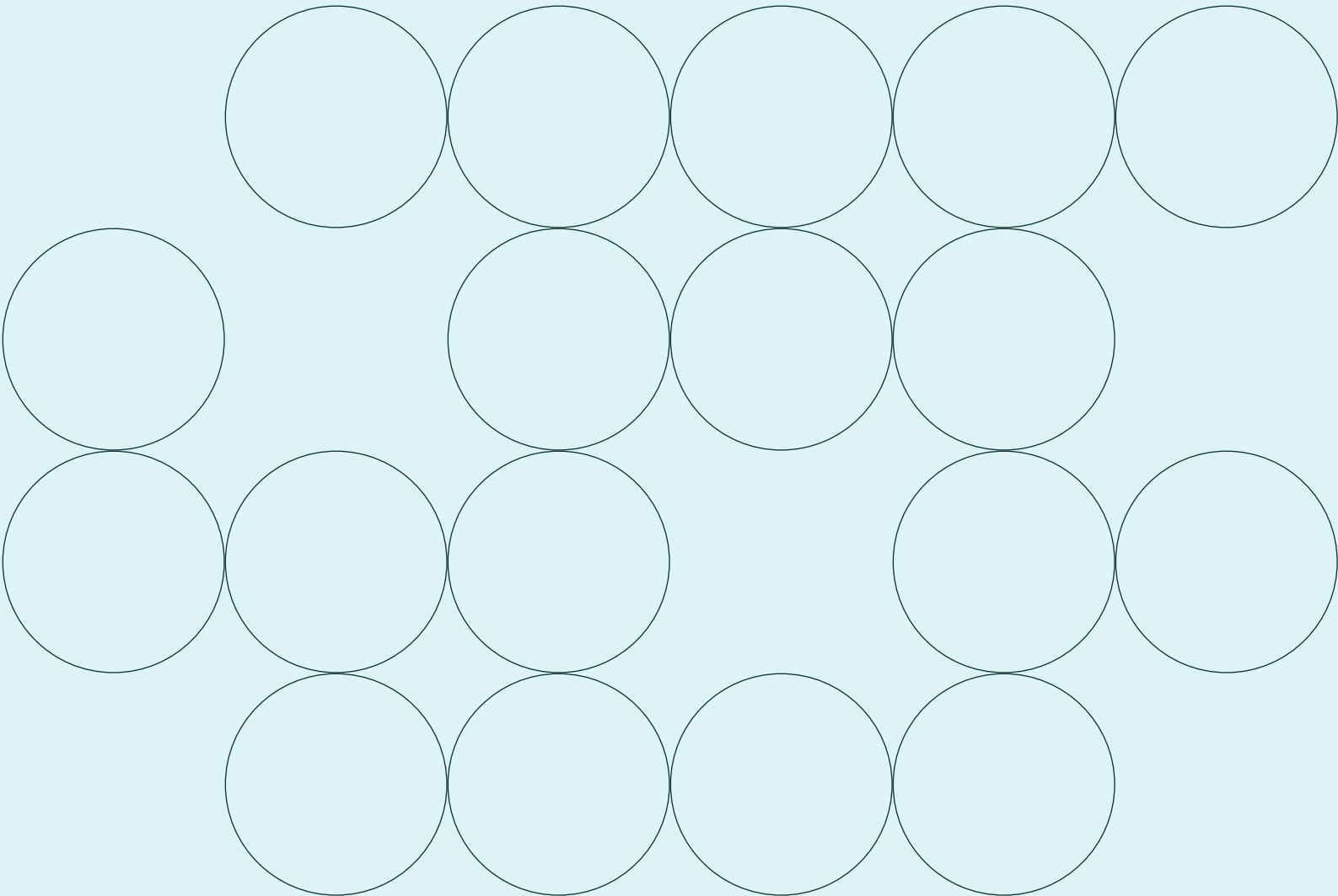
The final Digital Omnibus package represents meaningful progress on several fronts, including ideas for centralized enforcement, harmonized DPIA and breach notification processes, and expanded support for SMEs significant gaps remain. The next phase of European digital policy requires a deliberate and balanced focus on three core objectives: achieving deeper legal harmonization, delivering clear and consolidated implementation guidance, and cultivating a regulatory ecosystem that actively enables innovation and long-term competitiveness.

The workshops revealed broad consensus for radical institutional and cultural change—moving from a compliance-driven to a learning-oriented regulatory model. Short-term measures such as implementation pauses, clearer provisions, and functional regulatory sandboxes could provide some immediate relief, but lasting progress requires deep institutional reform to rebuild trust and align regulation with technological realities.

Participants' vision of a European Digital Social Contract encapsulates this broader ambition: a governance model that balances innovation and protection through evidence-based, adaptive regulation. Europe now faces a strategic choice—continue on a path of escalating compliance costs and declining competitiveness, or embrace comprehensive reform that makes European values work in practice by enabling innovation and safeguarding rights simultaneously.

Simplifying the EU's Digital Rulebook

Annex



Annex I

The insights in this report are gathered from six workshops which took place in:

The geographic distribution of workshops across Brussels, Copenhagen, Munich, Paris, The Hague, and Warsaw supported representation of diverse member state perspectives on digital regulatory implementation challenges and solutions. All workshops took place under Chatham House Rule and provided an open and interactive space for participants from the private sector to share their views on the EU simplification agenda. Each workshop convened approximately 30 people and lasted for two hours. The discussion was organized through a mix of facilitated and structured breakout group discussions and reporting plenaries. Participants were invited to explore key questions through the lenses of ensuring policy effectiveness, policy coherence, policy clarity, policy adaptation and feasibility. Key areas of discussion included:

1. **What in current key privacy and AI related frameworks could potentially present implementation challenges that influence the development of the EU ecosystem?**

2. **How might we simplify and better align EU AI and privacy related frameworks to address the challenges identified and ensure regulatory clarity and coherence?**

3. **From a governance perspective, what measures would enable regulators (e.g., AI Office, DPAs) to better support AI and digital innovation?**

Limitations

By integrating perspectives from workshops verbally shared, as well as in the form of live Mentimeter surveys, this study aims to reduce biases and enhance insight depth. Although not universally representative, the findings offer meaningful trends and insights from participating organizations, with future research well-positioned to expand and update these observations as regulatory files evolve. Data and perspectives were collected from stakeholders between June 2025 and September 2025 during the workshops, capturing a specific moment in time. As AI practices and regulatory responses shift, some findings may change in relevance.

Disclaimer

The synthesis and recommendations contained in this report represent synthesis of stakeholder input and independent policy analysis. They do not necessarily reflect the official positions of any participating organizations, host institutions, or government entities. The authors take full responsibility for any analytical errors or omissions in synthesizing the extensive stakeholder input received through the consultation process. The goal has been to provide an accurate representation of stakeholder perspectives while developing actionable policy recommendations for EU decision-makers.

Annex II

Examples of Definitional and Interpretational Challenges as Identified by Workshops Participants.

Legal Framework	Issue/ Provision	Identified Issue of Clarity, Ambiguity, or Definition	Workshop Participant Quote
EU AI Act	Definition of "AI System" (Article 3)	The fundamental definition of what constitutes an AI system is unclear. This creates confusion even for technical personnel who may not know if a specific piece of software falls under the Act's scope, especially if it only contains a minor AI component. This also creates issues for global interoperability, as the EU's definition may differ from those used elsewhere.	"The technical personnel does not know if a particular software is an AI system or not… A piece of software may only encompass an AI component which is significant for the output and sometimes not".
EU AI Act	High-Risk AI Classification (Article 6 & Annexes)	The criteria for classifying an AI system as "high-risk" are ambiguous and subject to different interpretations even within the same company. Participants found the legal text (Article 6 and its annexes) tricky to navigate due to exceptions and exceptions to the exceptions. There was also a strong sentiment that the classification should be based on real, tangible risks to individuals rather than abstract or overly broad categories.	"Uncertainty in the definition, some supposed to be clarified by the commission. They did some of that, some of that they clarified, and it still is not very clear" . "Very challenging to categorize different processing, especially when the company would like to be compliant from the AI Act to be sure that they are doing it in right way"
EU AI Act	Roles in the AI Value Chain (Articles 16, 23, 25-27 - Provider, deployer, distributor roles) Article 28 (Substantial modification)	There is significant confusion for organizations in identifying their specific roles (e.g., provider, deployer, importer, distributor) and the corresponding responsibilities. A key ambiguity is the lack of a definition for "substantial modification," which is the trigger for a deployer taking on the obligations of a provider. This creates an "identity crisis" for actors in the value chain.	"Big uncertainty and complexity with a view to how value chain roles and obligations interact in a way that creates huge confusion and overhead for companies to navigate" "Issues as to the deployer's obligation, higher system... there might be different obligation applicable depending on who is using AI system, if it's a lawyer, if it's a judge, it's an arbitrator" "Value chain roles don't align. Can be provider under AI Act but controller or processor under GDPR. The determination method differs. Creates confusion about responsibilities."
EU AI Act	Outdated or Non-Future-Proof Provisions Article 3 (GPAI definition)	Certain provisions and definitions are already becoming obsolete due to the rapid pace of technological advancement. For example, the definition of a general-purpose AI model and the use of technical thresholds (such as computing power measured in FLOPs) can quickly become outdated, challenging the Act's long-term viability.	"How can lawmakers define measurement capabilities when even R&D labs find it difficult to predict how to measure AI in 6 to 12 months, how on earth can the legislators actually tell that?"

ANNEX II

Legal Framework	Issue/ Provision	Identified Issue of Clarity, Ambiguity, or Definition	Workshop Participant Quote
EU AI Act	AI Literacy (Art. 4)	The concept of "AI literacy" is considered extremely vague and poorly defined. Participants felt it was "bolted on" to the Act without a clear underlying concept, making it difficult for companies to understand how to implement the requirement and for regulators to enforce it. Experts themselves have multiple opinions on what AI literacy truly means.	"It's mandatory to have an AI literacy course in your organization, but it's not mandatory that it has been followed or something like that. It's totally unclear what's happening there" "There is no real enforcement risk, because how [do you] enforce something that is so abstract as AI literacy?"
EU AI Act	Cybersecurity Requirements	The AI Act's provisions on cybersecurity are considered too brief and vague, leaving companies without clear guidance on how to implement the necessary technical and organizational measures to protect AI systems from cyberattacks. There is also a lack of clear terminology with other acts such as the Data Act, and Digital Operational Resilience Act (DORA) for cybersecurity. Furthermore, the AI Act does not adequately "reflect ISO standards" which are widely used by European companies for implementing controls.	"References to technical documentation without further guidance, for example, related to NIS directive existing cybersecurity or ISO norms"
EU AI Act	Transparency Requirements	Unclear scope and implementation of transparency obligations.	"Transparency requirement as regards AI Act and the question that provides segue between complexity and the recommendation about which authorities is responsible for what"
EU AI Act	Missing One-Stop-Shop for AI Act GDPR Art. 56: Lead Supervisory Authority mechanism (partially functional) AI Act: NO one-stop-shop mechanism	The AI Act has no coordination mechanism for regulators, and no obvious hierarchy among them. Companies must engage multiple MSAs across/within Member States plus AI Office for GPAI plus sectoral authorities. **No lead authority coordination.**	"We don't have a one stop shop mechanism in the AI Act... question is... do we need... one [stop] shop authority?"
AI ACT & GDPR INTERFACE	Data Reuse for AI Training & Development AI Act Art. 10 (Training data), GDPR Art. 6 (Legal basis), Art. 5(1)(b) (Purpose limitation), Art. 5(1)(c) (Data minimization	AI development hindered by unclear rules on data reuse. Companies are uncertain which GDPR legal basis applies. Risk-averse approach prevents beneficial AI innovation. Purpose limitation prevents use of existing datasets.	"What are the rules about reusing data for developing or improving AI? We need clear guidance, whether they're personal or non-personal data, what legal basis can we rely on, for instance, of the intimate [legitimate] interest in the GDPR or not?"

ANNEX II

Legal Framework	Issue/ Provision	Identified Issue of Clarity, Ambiguity, or Definition	Workshop Participant Quote
GDPR	Personal Data & Bias Testing	The AI Act creates misalignment with the GDPR. For bias testing, the Act imposes a higher legal threshold for processing special category data ("strikingly necessary") than the GDPR ("necessary"). Furthermore, the requirement to delete data after testing is impractical, as bias testing is a continuous exercise. There is also a broader need to clarify the very boundary of what is considered personal data. There is also a somewhat confusion with “Personal Data Boundaries” including exemptions in the GDPR, where a type of data, such as technical data, data related to processes, or even professional B2B email addresses should not be subject to the GDPR.	"The threshold for processing special category data for bias testing under AI Act high-risk systems is higher than in GDPR. Asking for 'strictly necessary' rather than just 'necessary'" "There was one voice about the bias, it's not defined term, and it's very important and it's basically used in references in the Act and it should be interpreted from European perspective from fundamental rights"
GDPR	Legal Basis for Model Training	Problems regarding establishing the proper legal basis for both AI training, but also for using data for the development of AI systems.	"Problems regarding establishing proper legal basis for both AI training, but also for using data for the development of AI systems"
GDPR	Data Subject Rights (e.g., Right to Rectification)	It is technically complex and costly to comply with data subject rights, such as the right to rectification, for large generative models. It is unclear how to balance these rights with technical feasibility, and participants noted the need for a unified European position on the matter.	"DSARs are misused... typically used for litigation, to get information, or to create a big pain point for the other side"
GDPR	Legitimate Interests Assessment	Unclear documentation and balancing requirements.	"What is a balancing of interest, what do you have to document? What do you have to balance?"
GDPR	One-Stop-Shop Inefficacy	OSS doesn't function as intended. Concerned Supervisory Authorities (CSAs) interfere. No real consistency despite mechanisms. "Lead" authority undermined. One-stop-shop in name only. Prolonged decision processes. Inconsistent outcomes. Companies face 27+ interpretations. Enforcement “lottery” persists	"Maybe there's not too many, but... they [need to] coordinate in [a proper] way... mechanisms... for consistency"
GDPR	Anonymization Standards	Inconsistent interpretation across Member States.	"Different interpretation of key concepts pertaining to personal data (e.g. anonymization)"

ANNEX II

Legal Framework	Issue/ Provision	Identified Issue of Clarity, Ambiguity, or Definition	Workshop Participant Quote
ePrivacy Directive	Cookie Consent Interpretation	Absolutist interpretations creating a consent-only regime.	"Absolutist interpretations... created a de facto consent only regime"
ePrivacy Directive	Legal Basis Conflicts	Conflicts with GDPR consent requirements. Therefore it would be simpler to merge the GDPR and ePrivacy Directive.	"Outdated provisions... conflict with legal basis for example in GDPR"
ePrivacy Directive	Consent Fatigue	Excessive consent requirements reducing protection effectiveness.	"Consent fatigue" as result of "outdated provisions"
Cross-Framework	Risk Assessment in Both the EU AI Act and GDPR	The two regulations have different approaches to risk assessment and classification. A company might find that under the AI Act, their system is not high-risk, but a Data Protection Authority (DPA) could still consider the associated data processing to be high-risk under GDPR, creating a confusing and contradictory situation for businesses.	"Multiple risk assessments, conflicting definitions across GDPR/AI Act, inconsistent reporting requirements"
Cross-Framework	Interplay with Other Regulations	A major source of confusion is the overlap and lack of alignment between the AI Act and other regulations like the GDPR, Data Act, Cyber Resilience Act, and sector-specific rules. Definitions and concepts are not aligned across these different legal frameworks, creating a complex and sometimes contradictory compliance maze for companies.	"Different understanding on definitions of AI and things like this that would need to be simplified" "Interplay with sectoral legislation, specifically as regards highly regulated sectors like financial sector, which coincides with many reporting obligations"
Cross-Framework	Multiple Risk Assessments	Duplicative and conflicting assessment requirements.	"Multiple risk assessments, conflicting definitions across GDPR/AI Act, inconsistent reporting requirements"
Cross-Framework	Reporting Obligations	Multiple, overlapping reporting requirements to different authorities.	"Multiple reporting obligations across different regulations with different deadlines, various points in the year, through various means and to various authorities"

Annex III Participation

The chart below presents a consolidated overview of participation throughout the workshop series. The main stakeholder group consulted was the private sector for practical experiences and insights on implementation challenges. However, depending on location and interest, think tanks, academia, international organizations, public entities, and not-for-profits were invited to solicit a broader range of views.

- **Private sector** 64.3%
- **Non-profit** 8.7%
- **Law firm** 7.6%
- **Public entity** 4.8%
- **Int. organization** 4.3%
- **Academia** 4.2%
- **Trades** 2.2%
- **Think-tank** 1.8%
- **Consultancy** 0.7%
- **Entrepreneur** 0.7%
- **Self-employment** 0.7%

COPENHAGEN, MAY 27, 2025

Private sector 72% **Non-profit** 8% **Int. organization** 8% **Trades** 8% **Academia** 4%

Danske Bank, Nordic Council of Ministers , KPMG, KasparAI , Hopp & Partners , Proem AI , Frankly, Accenture , PUFIN-ID , Danish Industry , Novo Nordisk, Cognizant Technology Solutions Corporation, Nvidia, Aalborg University / CAISA, Danish Entrepreneurs, CCAO, Netcompany

BRUSSELS, JUNE 12, 2025

Private sector 68.4% **Non-profit** 21.1% **Public entity** 5.3% **Trades** 5.3%

European Banking Federation, Covington & Burling LLP, Computer & Communications Industry Association (CCIA) , King & Spalding , European Banking Federation , EDPS , Ingram Technologies, Pour Demain , Mastercard Europe , Volvo Cars , Flint Global for Uber, ITI, Leidar , OpenAI , Credo AI

MUNICH, JUNE 12, 2025

Private sector 68.4% **Law firm** 18.2% **Think-tank** 4.5% **Consultancy** 4.5%
Entrepreneur 4.5% **Self-employed** 4.5%

Allianz, A&O, Lawyer Schurmann Rosenthal Dreyer, Fresenius, Freshfields, Zeiss, Accenture, DataGuard, zooplus, BMW, Noerr, DHL, Allane Mobility Group, Tum- AI, Tech Innovators Inc., BNP Paribas, Aleph Alpha, Youmaday, ON Semiconductor, Trail GmbH, Global Solutions Group, Digital Transformation Corp., Slalom

PARIS, SEPTEMBER 11, 2025

Private sector 68.7% **Non-profit** 12.5% **Int. organization** 12.5% **Public entity** 6.3%

Jus Mundi, EIT Manufacturing, Milliman, Adobe, Talos Network, Opella Healthcare Group, DGE - Digital Economy Department - Ministry of Economy, L'Oréal, Criteo, Globethics, International Chamber of Commerce France, OECD, LINKLATERS LLP, EY, Franklin

WARSAW, SEPTEMBER 17, 2025

Private sector 42.1% **Law firm** 26.3% **Public entity** 12.5% **Academia** 10.5% **Think-tank** 5.7%

Inpost, Agora, Ministry of State Assets, Allegro, InPost, Bird & Bird Koremba, Dziedzic i Wspólnicy sp.k., UODO, Institute of Law Studies, Polish Academy of Sciences, University of Łódź, AI Chamber, Addleshaw Goddard, Edenred Polska sp. z o.o., Bird & Bird, Agora S.A., Lubasz i Wspólnicy, Allegro, NASK- PIB, PGE Polska Grupa Energetyczna S.A., Dentons, Cardinal Stefan Wyszynski University in Warsaw

THE HAGUE, SEPTEMBER 29, 2025

Private sector 63.6% **Non-profit** 9.5% **Academia** 9.5% **Int. organization** 4.5% **Public entity** 4.5%

KickstartAI, TNO, GNKS Consult BV, Weaviate, Prosus, ABN AMRO, WSP Global Inc., ICC NL, Rathenau Instituut, KPMG, KPMG Cyber & TechLaw, TomTom, DPO Consultancy, Mila - Quebec AI Institute, Danone, CIO Platform Nederland, FME, Deloitte, 8vance, Autoriteit Persoonsgegevens (Dutch DPA)