Response to the Call for evidence on the upcoming Digital Omnibus

Middle Tech Europe welcomes the opportunity to respond to the Call for evidence on the upcoming Digital Omnibus. Regulatory coherence and simplification is particularly important for midsized companies, which often lack the extensive compliance teams of the largest competitors. This is why Middle Tech Europe is keen to actively contribute towards the common goal of streamlining the digital acquis and advocate for a proportionate and flexible regulatory approach to the digital sector.

With this response, MTE is providing input on key areas where our members see potential to reduce bureaucratic burden: Artificial Intelligence, Cookies, the Digital Services Act and its interactions with other pieces of legislation, Incident reporting and Future tech policy-making.

Artificial Intelligence

We strongly support the AI Act's core objectives and obligations, as it provides a harmonized framework for the safe and responsible development and use of AI across the EU. We welcome those targeted simplification measures that reduce administrative burdens for businesses, without compromising the Act's intent or effectiveness. It is vital for middle-sized companies that any in-scope services they deploy in the EU are regulated in their member state of establishment, consistent with the country of origin principle. Clear and actionable guidance must be prioritized to aid company compliance so that compliance can be planned and resourced effectively and efficiently.

In order to ensure a simplified regime that is workable and scalable for middle-sized providers:

- Member state authorities must publish all guidance in draft form and hold an open and public consultation, with particular focus on ensuring guidance is proportionate and fair for companies of all sizes.
- If guidance is to be developed at EU level – under the auspices of the EU AI Board – an accountability structure must be put in place to ensure member state authorities consult with their national stakeholders and have a fully informed view to input to AI Board deliberations. This should complement consultation by the AI Board itself to ensure the process to develop EU guidance does not unfairly favor very large companies that can resource this engagement.

- All guidance must include a reasonable implementation period, with regulators' support to inform compliance where needed, and guidance must always precede any enforcement action.
- Member state authorities and the AI Board must publish an annual strategy and work program so that providers understand priorities and planned workstreams, and what to expect and when.

Downstream providers and deployers must have timely access to the technical documentation and information from upstream suppliers required to assess risks, fulfil their compliance obligations under the AI Act and other EU frameworks, and enable their responsible and transparent use of AI to the benefit of EU consumers and business customers. The simplification process should therefore support, rather than weaken, the operation of the GPAI Code of Practice and empower the AI Office (AIO) to proactively monitor the flow of information from model providers to downstream players. The AIO should also monitor for any unintended consequences inconsistent with the simplification goals, such as conduct that increases downstream firms' liability, creates new compliance gaps, or makes their regulatory compliance unnecessarily complex or risky.

Companies must be equipped to comply with the AI Act, and timely harmonized standards for that are essential. If standards for high-risk AI systems are delayed, temporary postponement of related obligations throughout the AI supply chain should be considered to ensure compliance remains feasible.

Clarifying how the AI Act interacts with the Digital Services Act (DSA), the General Data Protection Regulation (GDPR), and other frameworks is also critical to avoid legal uncertainty and duplication. Where full legislative alignment between the relevant legislative acts is not feasible to prevent overlaps, unified practical guidance should be developed jointly by the regulators concerned, in a timely manner and in line with the suggested process outlined above, to ensure effective compliance. Good examples of such guidance is the European Data Protection Board opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, as well as the upcoming guidelines on the interplay between the AI Act and the GDPR, currently being prepared jointly by the EDPB and the AI Office. Furthermore, guidance must avoid imposing unreasonable obligations on downstream firms that would be in tension with the simplification objective and be unworkable because of imbalances in market power. For example, obligations to verify that an upstream model provider has complied with particular EU rules or to make disclosures to users requiring inputs withheld by an

upstream provider would significantly increase regulatory complexity and risk for downstream AI applications. Crucially, such outcomes would also disincentivize adoption of AI across the economy and conflict with the objectives of the EU's recently published *Apply AI Strategy*.

Cookies

MTE agrees that some data legislation has become outdated and that fragmentation has made the legal framework unpredictable and incoherent. This situation is particularly impactful on middle-sized firms for whom regulatory instability and unpredictability is a significant driver of cost and risk which can chill investment decisions. We therefore strongly support the idea of addressing cookie consent fatigue, by reviewing and separating uses that are more likely to be invasive to an individual's privacy from those that have become essential to operating a digital service today and pose low risk to EU consumers.

Crucially, some MTE members rely wholly or mainly on advertising revenue to provide their services and compete in the EU. Regulators' view that all advertising-related cookie uses require consent regardless of risk - paired with the requirement to offer users an "accept all/reject all" button on the first layer - significantly limits available ad revenue where users 'reject all' cookies. For example, low risk cookies are required to measure audiences and verify ad delivery, which are essential to accurately price ad inventory, invoice advertisers and receive ad revenue. Low risk cookies are also essential to address ad fraud and cap ad frequency to avoid bombarding consumers with the same ads.

The current framework has become insufficiently flexible and adversely affects decision-making about future product development and investment, and undermines what has allowed the internet to grow into a place where every individual could gain access to a broad array of services and knowledge, free of charge. A simplified, more balanced and predictable approach to cookie consent, based on risk and a refreshed understanding of what is essential to support commercial operations, should be a priority for the simplification program.

As mentioned, in addition to advertising cookies, analytical and service-essential cookies (including SDKs, APIs or similar technologies) are essential to maintain, improve, and secure digital services. For instance, they enable the detection of technical errors, the measurement of feature performance or safety metrics, the optimization of user experience, fraud detection, and software updates without involving intrusive tracking or personalization and should not be treated the same way as social media tracking pixels. They are typically

controlled by the online service itself and present minimal privacy risks. Yet, divergent interpretations among Member States on whether consent is required create legal uncertainty and unnecessary compliance costs. Requiring consent for such low-risk uses is disproportionate and contributes to consent fatigue. A harmonized and proportionate approach should recognize alternative legal bases for this category of cookies, such as legitimate interest or performance of a contract, under appropriate safeguards. Reviewing and separating uses would remove unnecessary regulatory barriers to providers' operations in the EU and ensure that they do not have to disable essential technologies for users who 'reject all' cookies.

To address these issues, the Commission should consider revising the list of cookie uses that do not require consent to include new low-risk uses and explore embedding Article 5(3) in to the GDPR to enable legal bases other than consent. Permitted exemptions should extend to controllers' essential technology partners (e.g.: consent management platforms) to avoid unfairly affecting middle-sized firms that are not vertically integrated and must partner with third parties to provide core services to them.

Regarding addressing user fatigue where consent will continue to be required, we recommend only including in banners those cookies which users have to consent to and permitting bundling of certain cookies which are inherently linked to the same purpose. We also counsel against centralized cookie controls – e.g. through browsers – which would disintermediate the relationship between providers and their customers, complicate rather than simplify compliance burdens and risk creating new gatekeepers.

Digital Services Act

The DSA has several overlapping requirements with other pieces of legislation, imposing significant and redundant compliance burdens on online platforms and certain other in-scope intermediaries. Its transparency reporting rules duplicate that of other frameworks – including the Platform-to-Business Regulation (P2B), Media Freedom Act (MFA), Regulation on addressing the dissemination of terrorist content online (TERREG) and the derogation to the ePrivacy Directive enabling Child Sexual Abuse Material (CSAM) detection – with each one requiring bespoke and prescriptive templates making repurposing difficult. Risk assessment requirements for VLOPs will likely overlap with the proposed CSAM Regulation once adopted, while Article 28 guidelines extend these requirements to all online platforms accessible to minors. The DSA's recommender system transparency obligations also overlap with the P2B, the Consumer Rights Directive (CRD) and the Unfair Commercial Practices Directive (UCPD) – each with slightly different requirements, making

it harder to comply. Additional overlaps in the DSA include internal complaint-handling mechanisms that mirror P2B obligations, overlap and inconsistency around rules governing dark patterns, and for video-sharing platforms, protection of minors obligations that duplicate Audiovisual Media Services Directive (AVMSD) requirements. The DSA's data-sharing provisions with authorities also overlap with Data Act requirements.

MTE therefore recommends that the Digital Omnibus consider ways to streamline transparency reporting across the digital acquis in order to make compliance more efficient and less costly for middle-sized firms. In particular, this should consider whether some reporting obligations are now redundant and could be repealed, as well as identify opportunities to recognize a single report as compliant with multiple frameworks, including the DSA. We also advocate for a more proportionate approach to lower-risk services, including VLOPs under the DSA. For example, when platforms consistently demonstrate low-risk profiles and strong compliance records, the current VLOP-specific obligations become disproportionately burdensome and resource-intensive. Ideally, we would support introducing a rebuttal mechanism for VLOP designation in the DSA, similar to Article 3.5 of the Digital Markets Act, allowing platforms to request reconsideration of their status based on positive audit outcomes, risk assessments, and proven effective mitigation measures. As a minimum, we propose that lower-risk VLOPs with proven compliance track records should be permitted to submit streamlined risk assessments and audit reports at reduced frequencies, allowing them to focus resources on meaningful safety improvements rather than administrative processes.

Finally, we note that the administrative burden resulting from overlapping requirements is compounded by laws from third-party jurisdictions that impose similar obligations as the EU, e.g. the UK and Australia. As such, coordination amongst different legal regimes and avoiding inconsistencies wherever possible helps providers in scope of multiple regimes to better protect their users and be more efficient and compliant. To this end, we urge the Commission to discuss possible alignment with the Global Online Safety Regulators Network on certain regulatory products that lend themselves to standardization – and which represent a significant compliance burden for midsized companies – such as risk assessments and transparency reports. It ought to be possible for a service to complete a thorough report for one jurisdiction and for that product to be recognized by another like-minded jurisdiction – a "compliance passport" of sorts.

Incident reporting

MTE welcomes recognition that incident reporting obligations are duplicated across a number of EU cybersecurity and data frameworks, including the GDPR, ePrivacy Directive and the NIS2 Directive. Under these frameworks, some of our members risk having to submit multiple incident reports to multiple regulators for the same incident, within short time periods (typically 24 hours) and sometimes in multiple member states (e.g.: if a service is a Number Independent Interpersonal Communications Service) and in different EU languages. We therefore strongly support the development of a single reporting system which eliminates duplication and unnecessary cost by allowing providers to submit a single incident report to meet their obligations under all applicable frameworks and creating a centralized system that ensures the reports are shared with the relevant member state authorities. In addition, the Digital Omnibus should consider raising the threshold for reporting to ensure regulators focus on the highest risk incidents that require their engagement, and also remove obligations on downstream firms to report incidents that occur on the systems of their upstream suppliers and for which they have no operational or legal responsibility.

Future policy-making and regulation

MTE welcomes the emphasis on ensuring that new policy and regulatory proposals create optimal conditions for legal certainty and reliability, and that new regulatory proposals are not made without simplifying existing rules and proactively avoiding duplication. In this regard, the Digital Omnibus should prioritize:

- Refreshing the EU's better regulation principles to strengthen the commitment to proportionate, targeted and evidence-led policy-making, and add new tests including scalability and affordability to ensure rules are fair for middle-sized and smaller firms and do not serve as barriers to their market entry and investment;
- Embedding a culture of open and broad consultation at EU and member state level, with structures to manage pro-active engagement with key stakeholder groups, including middle-sized providers;
- Requiring an impact assessment *before* all policy and legislative proposals are published, and include a competitiveness test;
- Introducing common statutory duties for member state regulators and EU-level bodies to have regard to the impact of regulation on competition, innovation and growth, and requiring them to explain how their decisions have taken these duties into consideration;
- Building inter-institutional solidarity and support with the co-legislators to ensure new policy and legislation remains consistent with the EU's better regulation principles throughout the legislative process and delivers on its original objectives;

co-legislators also have a responsibility to ensure that implementation deadlines are reasonable and achievable for organizations operating in the EU and member state authorities.

MTE also commends this consultation for acknowledging the cumulative effect of EU digital regulation on businesses in Europe. As noted above, this is a significant issue for middle-sized firms that are facing significant increases in regulatory burdens now that frameworks adopted under the previous mandate are being implemented at member state level (including EMFA, NIS2, the eEvidence package). These will add significant new legal and operational costs for our members and require engagement with multiple existing and new regulators. We ask that the Commission consider broadening the simplification process to pre-empt implementation problems in other areas of regulation rather than wait for the Digital Fitness Check which risks coming too late for our members.

Closing comments

The Commission's simplification agenda is a crucial step for enabling innovation, growth, and competitiveness across Europe's digital sector, allowing middle-sized companies to focus resources on building better services rather than navigating overly complex compliance requirements. The path to effective and proportionate digital regulation requires ongoing dialogue between policymakers, regulators and the diverse range of companies that shape Europe's internet ecosystem. Middle Tech Europe is committed to being a constructive partner in this process.