Response to the Call for evidence on the Digital Fitness Check

Middle Tech Europe (MTE) is a growing alliance whose members currently include Automattic, Dailymotion, Discord, Dropbox, Grindr, Patreon, Pinterest, Reddit, WeWard, Yahoo, and Yubo. Our members operate a wide variety of services, ranging from video-sharing and e-commerce to e-mail, forums, communication, media, online dating and hosting services – representing the often missing "middle-voice" in tech policy discussions.

MTE welcomes the opportunity to provide input on key areas where our members see avoidable overlaps across EU legislation and potential to reduce reporting and bureaucratic burden. Overlapping requirements are particularly burdensome for companies with limited resources, which often lack the extensive compliance teams of the largest competitors. As a coalition, we advocate for a proportionate and flexible regulatory approach to the digital sector and are therefore keen to contribute towards the common goal of simplification and streamlining of obligations.

We have highlighted below the key areas where we see existing overlapping requirements stemming from various pieces of legislation that could be streamlined to reduce burden, and where we also provide recommendations, namely: transparency reporting requirements; risk assessments; recommender systems transparency; internal complaint-handling systems and out-of-court dispute settlement bodies; dark patterns; requirements for video-sharing platforms; B2G data sharing; and international alignment.

Impact of the EU digital acquis

One of the key positive impacts of the digital rulebook has been its contribution to a degree of harmonization, legal clarity and certainty, facilitating companies' (especially less-resourced, mid-sized companies) scaling, growth and innovation capabilities across the EU. However, despite this progress, the current regulatory landscape remains characterized by significant fragmentation, overlaps, and duplications.

The application of digital EU legislation has resulted in increased compliance costs and regulatory fragmentation, particularly for mid-sized tech companies operating across multiple Member States. While many digital rules are adopted at the EU level, companies often face overlapping and cumulative obligations across different EU laws, combined with divergent national implementation, interpretation, and enforcement. In some cases, businesses are also subject to oversight by multiple authorities under different regulatory frameworks, each with its own procedures, expectations, and timelines. This creates additional complexity and legal uncertainty for companies operating across borders,

disproportionately affecting middle tech companies, which are cross border by design but lack the compliance scale of the largest players.

Overall, regulatory fragmentation, including overlaps between EU laws and the involvement of multiple regulators, acts as a barrier to cross-border activity, weakens the functioning of the Single Market, and diverts resources away from innovation and consumer facing investment, contrary to the objectives of the EU digital policy. For some categories of service, they also face layers of domestic regulation and a patchwork of different regulations across multiple Member States in addition to EU-level regulation. Taken together, these factors make compliance unnecessarily complex and costly, and inevitably slow down market entry and the launch of new products and features to EU consumers. This cost and complexity disproportionately impact smaller and middle sized providers trying to grow and scale in the EU.

Overlaps between EU digital acquis and sector-specific legislation

Overlaps between the DSA (including the guidelines on the protection of minors under Article 28) and the Audiovisual Media Services Directive (AVMSD), particularly obligations relative to the protection of minors as they apply to video-sharing platforms, which have to comply with both pieces of legislation, have been increasingly identified as an issue to tackle in upcoming initiatives.

The DSA includes a wide range of obligations for online platforms, including requirements such as putting in place a notice and action mechanism as well as specific measures on the protection of minors. Platforms notably have to put in place proportionate measures to ensure a high level of privacy, safety and security of minors on their service, and are prohibited from presenting advertisements based on profiling when they are aware that the user is a minor. Additionally, the guidelines on the protection of minors under Article 28 introduces new requirements on age verification, age-appropriate designs, recommender systems, user agency and parental controls for platforms accessible to minors. Very Large Online Platforms (VLOPs) are also required to assess the protection of minors as part of their assessment of systemic risks, and must take appropriate targeted measures including age verification and parental control tools to protect the rights of the child.

The AVMSD requires video-sharing platform providers to establish mechanisms for users of the platform to report or flag content which may impair the development of minors, contains incitement to violence or hatred or content whose dissemination constitutes an activity which is a criminal offence (i.e. public provocation to commit a terrorist offence, offences concerning child pornography and offences concerning racism and xenophobia). They must also protect minors from programs that may impair their physical, mental or moral development. Measures to that end include, as appropriate, establishing and

operating age verification and parental control systems with respect to content which may impair the development of minors.

Therefore, the duties in the DSA and the AVMSD in relation to protection of minors are, in practice, functionally equivalent. Certainly in compliance and enforcement terms, there is significant overlap. This overlap isn't merely incidental; it creates entirely separate yet parallel compliance streams, as the DSA and AVMSD are typically overseen by different regulators in each Member State. This produces divergent approaches to regulatory supervision, similar-but-different compliance undertakings, and the risk of multiple, concurrent investigations into the same underlying issues.

In addition, there are areas of digital regulation - such as NIICSs - which are not yet aligned with single market principles, in particular the country of origin principle. This principle is particularly important for middle tech firms so that they can unify and streamline their compliance in their Member State of establishment and avoid fragmentation, unnecessary cost and effort across multiple EU markets as they grow and scale. The regulation of NIICSs continues to apply on a country of consumption basis under the EECC and NIS2, exposing providers to 27 different regulators and additional layers of domestic regulation which current rules allow Member States to introduce, in tension with the Single Market principles. Neither the Digital Omnibus nor the Digital Networks Act (DNA) address this issue and the absence of streamlining and simplification consistent with the country of origin principles will bear heavily on middle tech firms and affect their ability to grow.

Overlaps between EU and national laws

As noted above, Member States have layered additional domestic rules on NIICSs in tension with the Single Market principles. Many of these are redundant since NIICSs are now fully in scope of the NIS2, the EU's consumer protection acquis and the eEvidence and EIO frameworks. There is also an opportunity to review certain Member State consumer protection regulations in the context of the DFA. For example, German domestic law requires providers to implement a one click cancellation which is open to impersonation and is in tension with EU-level regulation requiring providers to protect personal data and ensure user security.

Dark patterns

Dark patterns are currently tackled inconsistently throughout the EU legislative framework - notably in Article 25 Digital Services Act (DSA), Article 6(1) Unfair Commercial Practices Directive (UCPD), Article 5(1) AI Act and the General Data Protection Regulation (GDPR). While this framework provides ample rules, the lack of consistency and harmonization across intersecting areas of regulation - including the absence of a common definition of "dark pattern" - creates some operational and legal uncertainty for certain providers. The

term “dark pattern” may be currently used as a catch-all concept, encompassing a wide variety of user interface practices, some of which may have significantly different purposes, contexts, and impacts on users.

We believe that this existing lack of consistency could be addressed through non-binding guidance on the basis of the definition already provided in Article 25(1) of the DSA, clarifying that it applies only to practices for which there is evidence of negative effects on users.

Overlapping requirements in EU law: Transparency reporting requirements

There is an increasing number of EU regulations that require transparency reporting. While we recognise the importance of transparency for specific public interest purposes, reports are time consuming and costly to produce. The Digital Services Act (DSA), Platform-to-Business Regulation (P2B), Media Freedom Act (MFA) and Regulation on addressing the dissemination of terrorist content online (TERREG) all impose the publication of transparency reports which must include specific elements - many of which overlap. Beyond the significant and redundant burden that this creates for providers, part of the issue is that the DSA imposes very prescriptive, specific templates for reporting by all in-scope providers (i.e.: online platforms and intermediaries) - thus making it even harder to repurpose the reports. Against this background, we note that the obligations set out in the P2B Regulation have to a large extent been superseded by the adoption of the Digital Services Act and Digital Markets Act and MTE agrees with the Commission’s conclusion that online intermediaries will benefit from increased clarity of legal provisions if it were repealed. We welcome the proposal in the Digital Omnibus to do so.

DSA

The DSA requires online platforms to publish annual reports, for which they will have to use highly detailed and prescriptive templates provided by the Commission. The reports must include information on the complaints received through internal complaint-handling systems, the disputes submitted to the out-of-court dispute settlement bodies, the notices submitted, the content moderation engaged in at the provider’s initiative, etc. VLOPs have additional requirements, notably to publish their report twice a year and to include additional elements such as the qualifications and linguistic expertise of the persons moderating content, etc.

P2B Regulation

The P2B Regulation requires concerned platforms to publish information on the functioning and effectiveness of the internal complaint-handling system for business users, including the total number of complaints lodged, main types of complaints, average time period

needed to process complaints and aggregated information regarding the outcome of complaints; and to verify and update this information at least annually.

MFA

VLOPs are required to make publicly available on an annual basis detailed information on: the number of instances in which it imposed any restriction or suspension on the grounds that the content provided by a media service provider that has submitted a declaration is incompatible with its terms and conditions, the grounds for imposing such restrictions or suspensions, the number of dialogues with media service providers, the number of instances in which it rejected declarations submitted by a media service provider, and the number of instances in which it invalidated a declaration submitted by a media service provider.

TERREG

TERREG requires hosting service providers that have taken action to address the dissemination of terrorist content or have been required to take action in a given calendar year to make publicly available a transparency report on those actions for that year. The report has to be published before 1 March of the following year, and include information such as the measures the provider has taken in relation to the identification and removal of terrorist content, the number of items of terrorist content removed, etc.

Overlapping requirements in EU law: Risk assessments

One area where many overlaps are existent is in relation to the risk assessments. Several pieces of legislation - namely the DSA and its guidelines on Article 28, as well as the Regulation laying down rules to prevent and combat child sexual abuse, or CSAM - require online platforms to perform a risk assessment of their services. This is already a time-consuming and resource-intensive exercise, made all the more burdensome when duplicated and adjusted to fulfil different requirements.

The DSA specifically requires VLOPs to conduct risk assessments to identify, analyze and assess any systemic risks stemming from the design or functioning of their service and its related system. Furthermore, Article 28 of the DSA notes that all in scope services (i.e. online platforms accessible to minors) are required via the guidelines to conduct a child specific impact assessment structured around risks to minors from content, conduct, contact and consumers as well as cross-cutting risks. In addition, while the proposal for CSAM Regulation is still in the process of being amended, when adopted it will likely require platforms to perform self-assessments to identify risks linked to the solicitation and abuse of children on the service. Platforms and other providers in scope of multiple obligations requiring risk assessments should be able to comply with all applicable obligations via a single assessment report to save unnecessary cost and effort, and diversion of resources

away from compliance and commercial activities.

Overlapping requirements in EU law: Recommender systems transparency

Another overlap across the legislation is apparent concerning the transparency obligations of recommender systems. The overlap can be found across the DSA, the P2B Regulation as well as two pieces of horizontal consumer protection laws - the Consumer Rights Directive (CRD) and the Unfair Commercial Practices Directive (UCPD). These frameworks all require platforms to be transparent about the parameters they use in their recommender systems, but the slightly different requirements in each text makes the overlap burdensome and the laws harder to comply with.

DSA

The DSA requires platforms to set out in their terms & conditions the main parameters used in the recommender system as well as any options for the recipient to modify or influence those main parameters. The main parameters shall include at least: the criteria which are most significant in determining the information suggested to the recipient; and the reasons for the relative importance of those parameters. Where several options are available for recommender systems that determine the relative order of information presented to recipients, there is an obligation to make directly and easily accessible from the specific section of the online platform's online interface where the information is being prioritized a functionality allowing the recipient of the service to select and to modify at any time their preferred option. On top of this, VLOPs are also required to provide at least one option for each of the recommender systems which is not based on profiling.

P2B Regulation

The text includes an obligation to set out in the terms & conditions the main parameters determining ranking and the reasons for the relative importance of those main parameters as opposed to other parameters. Where the main parameters include the possibility to influence ranking against any direct or indirect remuneration paid by business users, there is an obligation to set out a description of those possibilities and the effect of such remuneration on ranking in the terms & conditions. We welcome the Commission's proposal to repeal this Regulation.

CRD and UCPD

Both laws include an obligation for online services providing consumers with the possibility to search for products offered by different traders or by consumers to provide general information, made available in a specific section of the online interface that is directly and easily accessible from the page where the query results are presented, on the main parameters determining the ranking of products presented to the consumer as a result of the search query and the relative importance of those parameters, as opposed to other

parameters.

Overlapping requirements in EU law: B2G data sharing

Both the DSA and the Data Act require platforms to share information with national authorities under determined circumstances. Once again, these overlapping obligations make the work of internal compliance teams harder and therefore put a strain on the already limited resources of most service providers.

DSA

Under the DSA, platforms are required to share information about users at the request of a national judicial or administrative authority for the purposes of determining compliance by the users with applicable Union or national rules. A crisis response mechanism (applicable to VLOPs only) is also foreseen: where a crisis occurs (where extraordinary circumstances lead to a serious public security or public health threat), the Commission may require a VLOP to analyze the impact of their activities on the crisis in question and identify and apply specific, effective and proportionate measures to be put in place for a temporary period.

Data Act

The Data Act foresees that where a public sector body demonstrates an exceptional need to use certain data to carry out its statutory duties in the public interest, data holders which hold those data shall make them available upon a duly reasoned request.

Overlapping requirements in EU law: Internal complaint handling and out-of-court dispute settlement

Several pieces of legislation require services to provide internal complaint handling systems and/or to identify and engage in good faith with external mediators with a view to reaching an agreement on the settlement of disputes with users. These include the DSA and the P2B Regulation, alongside the revised Alternative Dispute Resolution framework, which provides further instructions on the resolution of disputes themselves. There is scope to clarify the process for handling consumer complaints across multiple frameworks, including the GDPR and the consumer protection acquis. This would support a fair and predictable process, give businesses an opportunity to resolve complaints before an investigation, and help regulators focus resources on the most egregious consumer harms. All applicable frameworks should require consumers to complain in the first instance to the provider and only submit complaints to a regulator where they are unresolved.

DSA

The DSA requires platforms to provide users access to an effective internal complaint-handling system, which enables the complaints to be lodged against the

decisions taken upon the receipt of a notice, or certain decisions taken by the provider on the ground of illegality or incompatibility with the terms & conditions.
Under the DSA, users are also entitled to select any certified out-of-court dispute settlement body in order to resolve disputes relating to decisions taken under the internal complaint-handling mechanism. Platforms have to ensure that information about this possibility is easily accessible in their online interface in a clear and user-friendly manner, and both parties have to engage in good faith with the selected certified body.

P2B Regulation

Concerned platforms are required to: provide an internal system for handling the complaints of business users; duly consider complaints; and process them swiftly and effectively. They also have an obligation to provide in their terms & conditions relevant information relating to the access and functioning of the system, and update this information at least annually. The text also specifies what the complaints can concern.

Under the P2B Regulation, concerned platforms also have to identify in their terms & conditions two or more mediators with which providers are willing to engage to attempt to reach an agreement with business users on the settlement of disputes arising in relation to the provision of online intermediation service, including complaints that could not be resolved through the internal complaint handling system. They are also required to engage in good faith.

Overlaps between laws of EU and third-party jurisdictions

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.

Governance models

The Fitness Check should consider drawing on the experience of countries which have introduced robust models of transparency and accountability for domestic regulators and common statutory duties. For example, all UK regulators have common duties to have regard for their effect on innovation, competition and growth and are required to report

annually on how they fulfil these duties. They also have requirements to be transparent so that businesses know what is coming when, and regulators' programmes of work and indicative timelines are clear and predictable. Enforcement priorities are also published. Public and sectoral consultation is also the norm.

Providers have faced a number of challenges with the implementation and oversight of new EU regulations which have been introduced at pace and in large volumes over the last few years. Specific challenges include regulators' lack of readiness, the absence of actionable and workable guidance at the point when new regulation enters into force and the use of enforcement powers before guidance is in place and/or companies have had a meaningful and reasonable period to comply. The Fitness Check should therefore consider a new model whereby EU regulations do not apply or become enforceable before guidance is in place and in-scope providers have had sufficient time to comply. Regulators should draw on good practice to converge on a shared model of transparency and accountability based on an annual programme of work and a risk-based enforcement strategy, developed in consultation with stakeholders and published. Regulators should have common duties to have regard to their impact on innovation, competition and growth and be required to report on how they fulfil these duties.

Similarly, EU-level bodies should have clear transparency and accountability frameworks, also based on annual work programmes, aligned with risk and commercial as well as consumer protection priorities. Regulators' work should be informed by a detailed understanding of the economic and commercial environment in which businesses operate in the EU so that this shapes guidance and ensures it is actionable and workable in practice. This understanding should be built via proactive engagement and consultation with in-scope businesses and relevant stakeholder groups. The approach should be fair and proportionate for companies of all sizes, with particular attention to the needs of new and growing businesses such as MTE members.

Compliance tools

MTE supports the exploration of novel means to aid company compliance with EU regulations. Third party compliance vendors, industry schemes and independent certifications or standards should all be explored as part of the Fitness Check. These are already envisaged in the GDPR via processes for DPAs to recognise industry codes and certification schemes, however the process to obtain approval is complex and outcomes uncertain, which can disincentivise industry investment in them. In other cases, the legal framework does not support them at all.

While MTE welcomes the Commission's intention to explore tools that could simplify compliance, reduce administrative burdens and associated costs, as well as incentivize the

digitalisation of information, such initiatives must remain flexible and technology-neutral. MTE emphasizes that it is essential to avoid mandating a single, prescriptive solution. Companies should retain the freedom to choose the compliance approach that best fits their business model and operational realities, ensuring that innovation, adaptability, and operational efficiency are not constrained. While so-called "one-click compliance" tools may offer significant value, especially for smaller players, they require time and effort to create and be formally recognised and there needs to be a clear path for approval and a reasonable amount of certainty in order to justify investment.

MTE recommendations

There is an opportunity in the Digital Fitness Check to 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 because of overlapping obligations or whether they are redundant for certain categories of services. For example, a vast number of intermediaries have to submit transparency reports under the DSA but there is no evidence that this data is useful to regulators. The Digital Fitness Check should therefore consider whether some obligations could be repealed, as well as identify opportunities to recognize a single report as compliant with multiple frameworks, including the DSA and the ePrivacy derogation (and future CSAM Regulation). 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.

Looking ahead, MTE believes that there is a significant risk that the proposed DFA could introduce further layers of regulation in areas already extensively covered by the current digital policy framework. We're concerned that the DFA's evidence base, largely derived from the 2023 Digital Fairness Fitness Check, may not fully account for the substantive impact of more recent landmark legislations such as the DSA and the AI Act. Introducing additional prescriptive requirements or duplicating numerous DSA-style obligations across all online actors risks creating major divergent legal interpretations and significantly increasing compliance costs without a clear enforcement deficit being established. To uphold the principles of Better Regulation and simplification, the priority should remain on

ensuring that the existing digital rulebook is applied before layering a further landmark piece of legislation onto a complex regulatory system.

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.