Middle Tech Europe response to the draft guidelines under Article 28 DSA

Additional contribution

MTE welcomes the opportunity to provide feedback on the Commission's draft guidelines under Article 28 of the DSA. We are happy to be able to provide the perspective of a diverse range of mid-sized companies seeking to ensure that the regulatory approach is consistently proportionate, adaptable and relevant to all the online players in scope and ensures a level playing field.

Risk review

We welcome the guidelines' risk-based approach that underpins the DSA, recognizing that different platforms pose varying levels of risks to minors. However, we think this approach could be strengthened and integrated even further in the guidelines, specifically:

- **On the risk assessment:** The fact that the guidelines do not create a new burdensome reporting requirement (i.e. they don't oblige providers to submit a detailed, highly-documented risk review based on a prescriptive template) is welcome, as focusing on actual safety investments should take priority and not be hindered by over-burdensome documentation and reporting obligations. That being said, we believe that a recognition of equivalent compliance efforts - notably in the context of the UK's Online Safety Act - would contribute towards the Commission's overarching goal of simplification and streamlining for businesses. As such, should our member companies' respective DSA regulators inquire on whether a risk review for children has been performed in one form or another, it would be helpful if their OSA children's risk assessment could be presented as evidence of diligence in this area.
- **On the concept of platforms' accessibility to minors:** We believe that the risk-based approach should also be extended to the very concept of a platform's accessibility to minors, as even the simple fact of being accessible does not carry the same risks from platform to platform.
- **On the specific measures recommended in the guidelines:** We note that some of the measures in the guidelines are excessively service-specific. As such, we appreciate that the list of measures is non-exhaustive but would welcome further reassurances in the text that these measures do not constitute an exhaustive list of ways to fulfil the Article 28 requirements. On a related note, some of the recommendations not only go much further than the obligations set out in the DSA (care should be taken not to impose measures exceeding the DSA's scope, at risk of legal overreach), but they also

seem like they would be disproportionately burdensome for midsized platforms. Examples include:

- One of the proposed measures on recommender systems underlines that platforms should not "rely on the on-going collection of behavioral data that captures all or most of the minor's activities on the platform". This could be challenging to implement if it requires new and separate non-behavioral recommendation models.
- The user empowerment measures include this potentially very burdensome suggestion: Platforms should "explain why each specific piece of content was recommended to [a minor], including information about the parameters used and the user signals collected for that specific recommendation."
- Some of the "default settings" measures may also be too restrictive or burdensome, such as:
  - Restricting third parties from taking screenshots or downloading content posted by minors.
  - Disabling push notifications during core sleep hours for minors.
  - Designing temporary vs. permanent defaults.
- The draft guidelines read that providers should carry out a review whenever they make any “significant changes to their online platform,” whereas the current Impact Risk Assessment requirement of DSA Art. 34(1) is to conduct a risk assessment only “prior to deploying functionalities that are likely to have a critical impact on risks.”
- The measure recommending "human review for content that substantially exceeds the average number of views" is not practical and would not necessarily have the desired result of increasing safety.
- Furthermore, while certain parental controls can be helpful elements of a risk mitigation strategy, they should be considered as options, not obligations. Requiring tools for guardians such as screen time controls, guardian oversight over minor account settings, and total visibility into minor communications/interactions with other accounts may be problematic, disproportionate, and potentially in violation of the rights of the minor. We advocate strongly for a pragmatic approach on the basis that minors can be kept safe without providing "active monitoring tools" for parents (e.g., with age assurance where access to mature content is concerned) and that they may have legitimate reasons for seeking information or community without parental knowledge – for example, in cases where they may be in an abusive home situation. Alternative measures could include the relevant services

providing a dedicated process and support channel where guardians can reach out, with reinforced mechanisms in place when a safety concern or inappropriate use involving a minor is raised.

- **On a potential impact assessment:** We also recommend the Commission conduct a competition impact assessment to evaluate how cumulative compliance obligations affect midsized services.

Age assurance

We welcome the fact that the draft guideline's risk-based approach also applies to the recommendations on age assurance. Indeed services not directed at children - or that pose lower risks - should not be held to the same standards as high-risk services.

However, we are concerned that the recommendations on age assurance are unclear and overly prescriptive in places - especially the call for mandatory age verification for some services like dating apps. This risks favoring mandatory identity checks over other valid methods like age estimation, without consideration for the specific risk profiles identified by the platform.

Moreover, we believe that some key age assurance strategies and solutions are overlooked or discarded in the draft guidelines. As such we would like to draw the Commission's attention to the following:

- The guidelines do not acknowledge multilayered and authenticity-focused strategies, such as targeted account verification (voluntary or forced where appropriate; manual or automated where appropriate, etc.), detection of suspicious signals that could trigger further safety actions or monitoring, use of biometric technologies to verify accounts, etc. For example, 'Verified accounts' can strengthen user trust and help prevent fraud, grooming, and other deceptive behaviors to which minors are particularly vulnerable.
- Self-declaration, in conjunction with other risk mitigations providing an age-appropriate experience such as strong default settings, should be preserved as a form of appropriate age assurance. This would depend on the risk posed to minors and the risk mitigations put in place.
- We also encourage the Commission to clearly acknowledge that services should have the options to use a wide array of solutions from the entire value chain. This includes: upstream interventions (e.g. through app stores, device providers, or browsers), where large companies are better positioned and better resourced to implement horizontally effective, scalable, and privacy-preserving safeguards; the EU Digital Wallet; free,

open-source solutions; risk-based age assurance with voluntary age checking and gating; etc. Enabling parents to identify minors on shared devices could significantly reduce the burden on small & mid-sized platforms, especially for services that are not child directed.

Finally, we want to stress that while the guidelines reference privacy-preserving age assurance approaches, they do not sufficiently acknowledge that today's in-market solutions often rely on sensitive data like biometric scans or government-issued IDs. These practices are driven by the very goals the guidelines emphasize - accuracy & circumvention resistance - which makes it difficult to reconcile with foundational privacy principles like data minimization and proportionality. Child safety and privacy are often in tension, and in the absence of clear frameworks, platforms may be reluctant to deploy innovative safeguards, even with strong protections.

Online interface design and other tools

On online interface design, the guidelines recommend a measure to ensure that minors are not exposed to persuasive design features that are aimed predominantly at engagement, including the possibility to scroll indefinitely, automatic triggering of video content. We note that such features are part and parcel of contemporary web design and not inherently harmful. This creates a concerning situation where services not specifically targeting children (but that can be accessed by them) may nonetheless be required to identify which users are minors and provide them with an alternative version of the service stripped of these features. This approach seems to create tensions with the privacy principle and go beyond the scope of the DSA, anticipating potential future rules that are being considered in the context of the forthcoming Digital Fairness Act. We strongly caution against anticipating the DFA by embedding its forthcoming rules into today's DSA guidance. Each legislative instrument must be implemented on its own terms, ensuring legal clarity and respecting the intended legislative timelines.

Recommender systems and search features

On recommender systems and moderation, the guidelines recommend platforms put in place measures to reduce the risk that content is recommended that has been reported or flagged and whose lawfulness and adherence to the platforms' terms and conditions have not yet been verified. This could amount to a restriction of the visibility of content under Article 17(1) of the DSA, meaning that platforms would have to issue a statement of reasons to the content provider prior to the content's lawfulness or harmfulness having even been assessed and determined. This seems disproportionately burdensome, and the interaction with DSA Articles 16 and 17 should at the very least be clarified here.

Furthermore, some measures listed in the guidelines - such as providing minors with the opportunity to reset their recommended feeds completely and permanently, or providing prompts for the minor to search for new content after a certain amount of interaction with the recommender system - clearly go beyond the scope of the DSA, even its obligations for VLOPs. While those could serve as best practices, they should not be considered a standard in terms of the Commission's expectations for compliance. Furthermore, measures should be targeted to the risks they are intended to mitigate. For example, the proposal in the draft guidelines to provide a "reset" option on a provider's recommender systems may not provide any safety benefit for the vast majority of users, while likely being severely detrimental to their experience on the service.

The draft guidelines also discourage reliance on engagement-based signals for content delivery to minors, referring to "parameters and metrics related to accuracy, diversity, inclusivity and fairness [that] should also be considered." We would like to underline that to our members' knowledge, there are no qualitative or quantitative assessments for such metrics.

User reporting, feedback and complaints, and transparency

On user reporting, feedback and complaints, as well as transparency, the guidelines list numerous information, communication and warning measures, with a simultaneous expectation that this information be presented in a child-friendly, accessible format. Platforms should maintain the flexibility to design their services in a way that offers protective measures without compromising the overall user experience or creating information fatigue among minor users through excessive notifications and warnings.

Governance

While we are not opposed to guidelines that encourage platforms to hire dedicated human staff for safety, as this can help prioritize resourcing and justify internal investment in trust & safety, expectations must remain proportionate and scalable, particularly for mid-sized services. We would favor the Commission clarifying that the dedicated person or team should be required only when at least medium risks have been identified for minors.

Generally speaking, while some midsized platforms do have dedicated compliance teams, these are typically smaller than those found at large tech companies with extensive resources. Coupled with technical bandwidth limitations, this can make it difficult to implement every safeguard simultaneously. The guidelines' expectations - child-friendly designs, privacy-by-

default settings, and age-tailored safety controls - will require significant UI overhauls (e.g., optional comment disabling, content filters, autoplay toggles), imposing ongoing maintenance burdens.