NOTE FOR THE ATTENTION OF VERONICA GAFFEY, CHAIR OF THE REGULATORY SCRUTINY BOARD

Subject: Preliminary responses to the RSB’s checklist on the Impact Assessment report for the Digital Services Act

Thank you very much for your constructive questions and comments in the checklist sent by the Regulatory Scrutiny Board. I am sharing with you ahead of the hearing replies to the main questions raised and my team will be happy to provide further details during the hearing. The checklist has been extremely helpful, and work on revising the Impact Assessment is already under way, to address the concerns you have raised.

1. What are the inter-linkages between this initiative and related legislation? Does this broader regulatory framework for digital services contain any overlaps or unclear delineations? If so, will they be addressed in the proposed initiative? How have non-legislative or self-regulatory measures worked so far? What will be their role in the future?

This is a very important question and we are clarifying, in the revised impact assessment report, the interlinkages and delineations with sector-specific regulation and the relations with non-binding and self-regulatory measures and more clearly pointing to the gaps identified. In 2016, the first Commission Communication on online platforms set an issues-driven approach, with targeted regulatory interventions and self-regulatory measures. The Recommendation of 2018 is the only horizontal measure adopted in this period aiming at bridging some of the gaps and ensuring some level of harmonisation.

Legislative instruments

---

1 We are providing further explanations and more detailed analysis on these points e.g. in the context section, in the relevant driver for regulatory gaps, as well as the coherence analysis of the impact assessment report. We are also developing the presentation in Annex 7, which initially presented the relevant existing and proposed instruments and how they interact today with the E-Commerce Directive.


3 Recommendation (C(2018) 1177 final) on further measures to effectively tackle illegal content online
In the last years, in response to various sector specific challenges, legislation has been adopted or proposed at EU level: e.g. Copyright Directive, revised Audiovisual Media Services Directive, proposal for a regulation on terrorist content online, regulation on explosive precursors, market surveillance regulation.

There are important gaps identified in the sector-specific approach. None of these instruments provides fully-fledged rules on the procedural obligations related to illegal content and they only include basic rules on transparency and accountability of service providers and limited oversight mechanisms. In terms of scope, they are limited from two perspectives. First, these interventions address a small subset of issues (e.g. copyright infringements, terrorist content, child sexual abuse material or illegal hate speech, some illegal products). Second, they only cover the dissemination of such content on certain types of services (e.g. sub-set of online platforms for copyright infringements, only video-sharing platforms and only as regards audiovisual terrorist content or hate speech in the AVMSD).

All three options in the draft impact assessment report provide for a horizontal legal framework, which addresses these gaps. They complement but do not need to amend sector-specific legislation. The Digital Services Act should replicate the way the E-Commerce Directive interplays with other, sector-specific acts addressing digital services, including as regards supervisory competences of sector specific regulators (further explained in section 3 of the note). It is intended to be a horizontal instrument, with more targeted provisions only where necessary.

We are also explaining in the revised draft report specific points of complementarity between the implementation of different instruments and the DSA provisions – e.g. more detailed requirements for the notification system, as well as the transparency and redress obligations set out in the AVMSD; how the instrument complements the Copyright Directive and the consumer protection acquis through the harmonised notice-and-action mechanism.

Non-legislative and self-regulatory measures

The Recommendation of 2018 fleshed out procedural requirements that the sectorial legislation had not fully addressed. It included horizontal procedures for notice and action mechanisms, safeguards for users’ rights and transparency. The uptake of the Recommendation was mostly limited to the measures included in the self-regulatory efforts supported by the Commission, such as the Safety Pledge against unsafe products, the Memorandum of Understanding against counterfeit goods, the Code of Conduct against illegal hate speech, or the EU Internet Forum with regard to terrorist content. However, the Recommendation has not had a harmonising effect: Member States proposed legislation with diverging measures in the national legal drafts analysed so far. Most of the provisions of the Recommendation will be made binding in all options considered in the impact assessment.

The self-regulatory initiatives supported by the Commission have led to some positive results, yet reveal inherent limitations. Given the voluntary nature of these initiatives, only a selected number of providers take part in them, measures cannot be enforced and reported results and data cannot be verified. We are further clarifying this assessment in

---

4 For example, the ‘know your business customer’ obligations are mainly related to sale of products or services, rather than dissemination of content, but they are ill-suited in a strictly sector-specific intervention, as they address concerns related to any type of illegal goods, not just e.g. counterfeit products, or unsafe products, toys or medical devices.
the report\(^5\), and including up-front the continuation of existing and potentially new self-regulatory initiatives in all three options, not just in the baseline. Option 3 already includes participation in such cross-industry cooperation coupled with mandatory transparency on the measures taken as part of a re-enforced co-regulatory design for very large platforms in particular.

2. **What are the main political trade-offs and risks relating to the options? How was the initial threshold for a ‘very large platform’ set? Who would be covered? To what extent are third country digital services covered, and why?**

*Political trade-offs and risks*

In revising the report, we are adding further clarity to the architecture of the options and specific measures included in each of the options.

**The first option** is essentially based on the horizontal option assessed in 2018\(^6\). The due diligence obligations were widely supported in the feedback to the inception impact assessment and in the submissions to the public consultation. This option addresses the most prominent elements in the current legal fragmentation and codifies the 2018 Recommendation. We are revising the presentation and assessment, making it clear that all options also include the continuation of self-regulatory efforts.

As regards political risks and trade-offs, while the option is aligned with the core principles fleshed out in the European Parliament’s (EP) own initiative reports, it only covers to certain extent, through the self-regulatory efforts, the other issues identified by the EP as additional areas of concern (e.g. related to the amplification of content or online advertising). It is possible that the EP’s and Council’s intentions to legislate go beyond the soft approach of the first option, and, alternatively, that Member States regulate these issues independently.

**The second option** follows a similar regulatory approach, but covers more elements through hard law as regards user-facing transparency on recommender systems and advertising. It also includes modifications of the liability regime for intermediaries set in the E-Commerce Directive to remove disincentives for voluntary measures against illegal content\(^7\).

Similar to option 1, the main political risks relate to a potential legal fragmentation where some Member States would want to go further through legislative means. This option covers more of the EP’s additional measures.

\(^5\) In particular in driver 2.3.4 presenting the current regulatory gap, in the description of the baseline, options, and throughout the analysis of impacts. We are also revising Annex 10 for a more complete and analytical description of the self-regulatory initiatives in place

\(^6\) Assessed in a draft impact assessment presented to the Regulatory Scrutiny Board, but an intervention on terrorist content was prioritised at the time for the urgency to propose targeted measures specifically on terrorist content at European level.

\(^7\) In the logical structure of the options, the provisions on liability included in option 3 could also be combined with option 2. For the sake of simplicity, we chose this presentation to ensure that genuinely different options on the liability regime are assessed, within the boundaries set for the retained options. The preferred option could have been, hypothetically, a hybrid of the components considered for the different options, but the comparison of the options did not point in this direction. We are making adjustments in the analysis of impacts to explain to what extent the alternatives would change the overall assessment on the options.
The third option additionally provides for a supervised risk-management framework (similar to the regulatory approach in the financial sector) that addresses specifically very large platforms posing high societal risks. This option manages the levels of ambition in the EP reports and positions of some Member States focusing on the specific harms brought by a subset of prominent platforms, and is the least likely to be followed by further legal fragmentation.

The choice of the retained options (and some of the discarded options) also stems from managing a series of other political risks:

- **Weakening the single market for digital services:** this is a high risk in the current and evolving baseline. The intervention manages this by addressing the legal fragmentation and by preserving the ‘country of origin’ principle in the supervision of digital services. The measures will likely lead to the repeal of several national laws. In this regard the balance of measures is important: if the bar is set too low, this will in turn lead to further fragmentation and fail on the single market general objective of the intervention; if set too high, the obligations will be prohibitive for small companies and undermine the innovation objective. Along these parameters, the options explore proportionate rules common to all platforms, or an asymmetric approach for very large platforms. In managing uncertainties, we are further revising the approach to include in all options an exemption for small and micro-enterprises.

- **Changing the balance of rights and interests:** through modifications to the liability regime and the prohibitions on general monitoring in the E-Commerce Directive. These legal provisions have significant impacts on the protection of fundamental rights and freedoms, including freedom of expression, freedom to conduct a business as well as public policy objectives in ensuring online safety. The options consider clarifications to the liability regime, but do not depart from its core principles.\(^8\)

- **Automatic filters:** the Courts have found that legal obligations to monitor and filter all content on a platform are incompatible with the EU Charter on fundamental rights. This is also a highly contentious issue among stakeholders, in particular civil society, as well as for the EP. None of the options requires the use of such technologies. Option 3 proposes to regulate the voluntary use of such technology, as part of its transparency and accountability framework.

- **International dynamic:** all three options extend the scope of the due diligence obligations to service providers established outside of the EU. They take a proportionate approach, excluding very small, incidental players. From an international trade perspective, the provisions are in line with the non-discrimination provisions in the GATS, as they follow objective and non-discriminatory criteria, regardless of the location of the headquarters or the country where the company historically originated. This is also the case in establishing whether, in option 3, service providers fall into the category of ‘very large online platforms’.

**Very large platforms and third-country platforms**

We are clarifying in the revised report the methodological and policy considerations for establishing the threshold used to identify very large platforms. The threshold seeks to capture those service providers that are, *de facto*, public spaces for information exchanges and economic transactions and, consequently, present the highest societal

---

\(^8\) These issues are analysed in greater detail in Annex 9, together with a longer list of discarded options.
risks. At the same time, in setting the operational threshold, we also considered the importance of the legal certainty for companies, establishing a workable proxy for the risk-centric approach, without imposing disproportionate risk assessments on every service provider. The most easily applicable metric, comparable across service providers, is the user base in the EU. The threshold is set at the equivalent of a coverage of 10% of the EU population (around 45 mil.) as unique monthly users. We benchmarked the methodology and estimates against other regulatory approaches in this space and considered alternative proxies as alternative or cumulative criteria, such as turnover or market capitalisation.

The due diligence obligations address in themselves a series of concerns related to sellers from third countries, notably through the ‘know your business customer’ obligations. This does not, however, address the issue of third-country online platforms targeting the EU single market. This is important not least in light of the emergence of new services from China and elsewhere, with rapid increase in their user base in the Union. All three options extend the due diligence obligations to service providers established outside the EU to ensure the safety of Europeans as well as the protection of their fundamental rights online. Such extension is also important to ensure a level playing field for EU-based services. Past a de minimis presence in the Union, linked to a minimum number of users from the EU as we are explaining in the revised impact assessment, service providers will be required to appoint a legal representative in a Member State.

3. How would the supervisory framework function under the different options? How would it link to other (existing or planned) supervision structures in the digital area? Could an alternative structure be considered for the EU Board?

This is a key point in the policy design and we are revising and further explaining the architecture in the revised impact assessment report. The supervisory components of the options are intended to proportionately address the cooperation and due diligence obligations in each of the options. Briefly summarised, the approach for each option is:

Under the first option, the supervision rests on the current rules, with additional improvements in the day-to-day information sharing and requests set by Member States through an upgrade to the current IT system. Member States have maximum flexibility to designate one or several authorities competent for supervising the obligations in the act. The country of origin would continue to be responsible for the supervision of services established on their territory, and any derogations would follow the mechanism of the E-Commerce Directive. The interface with sector-specific regulators such as the media regulators or the consumer protection authorities would remain based on the framework set by the E-Commerce Directive and the discretion of Member States to organise internal coherence.

In the second option, Member States would appoint one authority as the Digital Services Coordinator, primarily responsible for supervising compliance with all due diligence obligations for services established in their Member State, for coordinating, as

---

9 E.g. NetzDG (DE) – special obligations on online platforms with more than two million registered users; ACCC Digital Platforms Inquiry (AU) – special recommendations for platforms with more than one million monthly active users; Online Harms White Paper and Furman Report (UK) – significance of the largest platforms.

10 We have reviewed the presentation of the options, with greater detail on the supervisory components and are following-through the changes in the analysis of impacts and comparison of administrative costs.
necessary, with the sector specific regulators within their Member State, and for ensuring the interface for the cooperation with other Digital Services Coordinators at EU level. This is also supported by an enhanced IT platform. It should primarily address the concerns raised by national authorities in the public consultation related to the need for enhanced alignment and coherence across authorities within a Member State. It would also address the need for better supervision of the more complex areas of algorithmic systems covered in the due diligence obligations under this option through potential synergies and exchanges across authorities. The interface with other sector-specific regulators would be enhanced, but remain at national-level.

**In the third option**, an EU Board, including the participation of the national Digital Services Coordinators, enhances the governance system, particularly necessary for ensuring the supervised risk management approach for regulating the due diligence of very large platforms. The Digital Service Coordinator of the home country of a very large platform supervises the audits, risk assessments and risk mitigation measures of the very large platforms; they ensure that the EU Board is appropriately informed of the issues detected, measures and sanctions. Other Member States can raise their issues within the Board and require the home country to take measures, and the Body can offer technical support for investigations. Eventually, the Body can request the Commission to take measures.

This system ensures in particular that systemic problems brought by those platforms with an EU-wide impact are appropriately addressed through EU supervision, with sufficient expertise and appropriate competencies. This system ensures that those (often small) Member States\textsuperscript{11} in charge of supervising very large platforms receive appropriate assistance from other Member States. This includes e.g. technical assistance for complex investigations related to algorithmic systems or language-specific issues. This system also gives concrete resolutions to those host Member States where the effects of content moderation decisions are felt: they can flag and assist the competent Digital Service Coordinator in identifying and addressing risks or compliance concerns for a specific service affecting their own citizens.

Based on these further specifications of the mechanism, we are revising the impact assessment report to consider two operational sub-options for the set-up of the EU Board: a decentralised agency with own resources and incorporating its secretariat, and an EU body similar in its structure to the European Data Protection Board (but with different competencies, as explained above), and the secretariat absorbed by the Commission. We are explaining the resource implications for both options, as well as potential trade-offs of efficiency and effectiveness in each of these sub-options. The report will provide a solid base for informed political decision in this regard.

We have considered and discarded also alternative structures for the EU body, and are providing further details in the revised impact assessment report and annexes. The longer list of considered architectures includes:

- **An expert group including Digital Services Coordinators**, managed by the Commission: this would at most ensure information sharing among authorities, but would not provide for the appropriate mechanisms for triggering the requests to home state Digital Services Coordinators, nor the joint and specific expertise and

\textsuperscript{11} Recurrent resource and information issue flagged by some Member States in the targeted consultation and position papers.
competencies for assessing the risk brought by very large platforms and triggering actions. The expert group would not be empowered to issue guidelines. At most, it could prepare reports, informing the Commission and, in turn, the Commission would issue guidelines. However, the Commission does not follow the necessary independence requirements in light of the considerations and consequences for freedom of expression online the operative guidelines entail.

- **Assigning the competences to an existing body.** We have shortlisted and assessed: the BEREC Office, ENISA, the Cybersecurity Competence Centre, EDPB, EDPS, Europol. We did not identify appropriate synergies with these structures. We made the assessment primarily in light of independence considerations and/or technical capability considerations and scope of services and concerns covered: they are either focused on more limited types of services and supervision of very specific regulatory provisions\(^\text{12}\) – or sector-specific provisions applicable to a wider set of services, sometimes non-digital\(^\text{13}\).

4. **On what basis does the assessment conclude in favour of the preferred option? How does it account for stakeholder views? What would be the additional costs imposed on very large platforms under Option 3?**

Option 3 is selected as preferred option on the basis of our assessment of the economic and social impacts identified, and the comparison of its effectiveness, efficiency, coherence and proportionality. Option 3 is also broadly supported by stakeholders’ views, including positions from the European Parliament and Member States.

The revised report will provide additional qualitative and quantitative evidence underpinning this assessment, notably through a more granular presentation of stakeholders’ and evidence made available in the meantime on costs and economic impacts.

Overall, the core distinction between the third option and the other options stems from the asymmetric approach targeting very large platforms and the corresponding governance system for enforcement. The risks such platforms pose can and do have a disproportionately more impactful negative effect than, for instance a small, regional social network or a marketplace selling niche products. Consequently, the binding, targeted intervention is also expected to produce significantly better results in ensuring safety online: tackling illegal content, goods or services.

The asymmetric obligations are only imposed on very large platforms which are, based on the current data, also the largest companies with important turnover. Consequently, while the targeted measures are more restrictive than for other companies, they are proportionate to the ability of the companies to comply. As such, they are not expected to have significantly (and overall) more negative impact on the freedom to conduct a business than the second option, but include additional restrictions on a subset of service providers. We are clarifying the distinctions between effects on very large players and other companies, to make sure the presentation clearly shows these arguments. We have also estimated the fixed costs from the additional obligations imposed on very large

---

\(^{12}\) e.g. BEREC Office supporting BEREC and national regulatory authorities in enforcing framework addressed to electronic communications networks/services operators, which a very restricted subset of digital services

\(^{13}\) e.g. ENISA’s focus on cybersecurity, EDPB’s strict focus on data protection, but wider set of services as ‘data controllers’
platforms compared to other smaller platforms (i.e. risk assessments, audits, transparency of ad archives and reporting), based on benchmarks of the compliance costs with the risk mitigation obligations in the financial sector.

Besides the qualitative refinement of the analysis, we can supplement the presentation in the revised impact assessment in some areas. The analysis of economic impacts can be further substantiated with evidence from a new study executed for the European Parliament\textsuperscript{14} that estimates a €76 billion increase in EU gross domestic product (GDP) over the 2020-2030 period for a package of measures broadly equivalent to the preferred option. We have been working with the Joint Research Centre to benchmark the estimates for each of the options along a similar methodology for a macro-level model.

Stakeholders’ views will be more extensively reflected\textsuperscript{15} in the design and assessment of the options through further edits in the report. Some highlights are summarised herebelow:

- There is a broad alignment of stakeholders in support of the components of the due diligence obligations and the regulatory approach in preserving the core principles of the E-Commerce Directive.
- The necessity for risk management and the usefulness of an independent audit system, as in Option 3 are widely supported in the public consultation (around 70% of respondents), including start-ups and publishers, with reservations from online platforms. More than half of the Member States explicitly raised the issue of such measures in a targeted manner and the own initiative reports.
- Brand owners and other right holders are requesting further proactive measures for the detection of illegal content, but these were analysed as part of the discarded options in Annexes 9 and 11. Instead, to address the reappearance of illegal content, all options rely on case law, codifying these standards in options 2 and 3 with regard to court orders.
- With regard to algorithmic transparency, measures included in option 2 and, to a larger extent, in Option 3, civil society organisations, academics and small businesses stress the importance of enhanced oversight, while online platforms support further transparency, they flag the need for limitations for trade secrets purposes. The options account for a balanced approach in this regard.
- Concerning the liability regime, there is broad alignment on the approach, with some variations of the approach raised by consumer protection associations regarding liability of marketplaces, which are not reflected in the options, but assessed in Annex 9.
- The area where stakeholders’ views have developed most clearly over the past year concerns the governance structure: in the public consultation on the DSA package (2020), 80% of respondents called for enhanced cooperation across Member States’ authorities, and 66% also called for a EU-level body, as in option 3. Several Member States are aligned with these views, and the European Parliament’s reports are also calling for robust measures in this sense.


\textsuperscript{15} Based on the latest open public consultation, targeted consultations, feedback to the inception impact assessment, position papers received, meetings, and workshops, benchmarked with similar consultation conducted over the past years and summarised in Annex 2
c.c.: Members of the Regulatory Scrutiny Board, RSB secretariat

Annex: Annotated checklist outlining the ongoing work by DG CONNECT in revising the impact assessment report.