Skriftliga synpunkter om förslag till förordning om inre marknad för digitala tjänster (DSA)

Tack för möjligheten att inkomma med skriftliga synpunkter om förslag till förordning om inre marknad för digitala tjänster (DSA). Google stöder fullt ut kommissionens och den svenska regeringens ambition att främja ett ansvarsfullt internet. Det är därför viktigt att förordningen är tydlig, främjar innovation och respekterar grundläggande rättigheter.

Denna skriftliga inlaga består av:

1. Kommentar på de punkter som framkom på sakrådet 18/2-2021
2. Analys av förslaget i sin helhet på engelska

Fokus i båda fallen är på hur kommissionens uttalade målsättning att främja innovation och respektera grundläggande rättigheter kan tillvaratas.

1. Sammanfattning av frågor från regeringens EU-sakråd

När du använder Googles tjänster i Sverige följs svensk lag samt respektive tjänsts användarvillkor. Vi vill ge våra användare och kunder en så bra upplevelse som möjligt och uppdaterar kontinuerligt våra tjänster, regelverk och processer för att främja detta. När innehåll bryter mot lagen eller våra användarvillkor tas innehåll ner i enlighet med den process som finns i villkoren.

Syftet med förslaget, det vill säga att främja ett ansvarsfullt internet där mellanhänder vidtar nödvändiga åtgärder gällande olagligt innehåll, utan att inskränka grundläggande rättigheter bör fortsatt vara i fokus. Utöver yttrandefriheten bör även näringsfriheten beaktas och att t.ex. undanta innehåll som publiceras av en viss typ av aktör (t.ex publicister) är inte förenligt med förslagets syfte och avtalsrätt. En så kallad must carry- skyldighet skulle begränsa hur privata företag kan säkerställa att användarvillkor följs och att olagligt innehåll hanteras på det sätt som föreskrivs i förslaget.

- Till exempel alla som interagerar med YouTube måste följa våra riktlinjer för communityn. Vi ger alla användare omfattande information om vad detta innebär.
- Det laddas upp över 500 h video per minut på YouTube och det är bara en bråkdel (1 procent) av detta som är olagligt eller innehåller material som bryter mot våra riktlinjer.
- Det tas på stort allvar och YouTube förlitar sig på en kombination av människor och teknik för att flagga olämpligt innehåll och se till att riktlinjer och användarvillkor följs.
    - Vi tar bort innehåll som bryter mot lagen och våra policyer så snabbt som möjligt.

    - Vi lyfter fram betrodda källor när människor letar efter information t.ex. som nu under corona.
    - Vi minskar spridningen av innehåll som befinner sig i gråzonen av som inte är olagligt eller oförenligt med våra policies men som tangerar.
    - Vi i ställer höga krav på vilka kanaler som kan tjäna pengar på YouTube. Detta ska vara ett privilegium och inte en rättighet.
- Process i tre steg för vad som sker om vi upptäcker att innehåll inte följer våra riktlinjer för communityn. Allvarliga överträdelser kan leda till andra konsekvenser. Alla kreatörer har möjlighet att överklaga bedömningar.
- När en video blir flaggad granskas den och videons sammanhang av YouTubes team för att avgöra om videon ska begränsas, tas bort eller ligga kvar. Videon bedöms också utifrån om syftet med den är utbildande, dokumentär, vetenskaplig eller konstnärlig.
- Vi investerar årligen 1 miljard dollar i detta arbete och utvecklar kontinuerligt både maskininlärning-baserade system för att känna igen olagligt innehåll och har ett stort antal personer anställda som granskar sådant innehåll.

2. Google's perspectives on the EU Digital Services Act

The Commission's draft EU Digital Services Act (DSA) regulation lays out responsibilities and accountability mechanisms for intermediary service providers. The text has three main portions: the liability regime, due diligence obligations, and regulatory oversight.

This non-paper evaluates the text against the Commission's objectives of providing legal clarity, respect for fundamental rights, harmonisation across the Single Market, and clear responsibilities for different types of intermediaries and authorities. It highlights the provisions that will help achieve these objectives, and identifies provisions that may fall short of them. It also considers how due diligence obligations can best serve users, by enabling services to build the most innovative and efficient tools to advance online safety.

The aim of the non-paper is to help bring about a DSA that promotes a responsible internet, through a regulatory framework that provides clarity, promotes innovation, and respects fundamental rights.

Cornerstone principles of the EU Single Market

The Commission rightly maintains the core principles of the e-Commerce Directive, including its conditional intermediary liability regime, the prohibition on mandating general monitoring, and the country-of-origin principle. These principles enabled the growth of the digital economy in Europe and expanded access to information. As the Commission writes in the Explanatory Memorandum, the DSA "maintains the liability rules for providers of intermediary

services set out in the e-Commerce Directive – *by now established as a foundation of the digital economy and instrumental to the protection of fundamental rights online*."

The Commission also helpfully clarified some aspects of the liability rules "to eliminate existing disincentives towards voluntary own-investigations undertaken by providers of intermediary services to ensure their users' safety and to clarify their role from the perspective of consumers in certain circumstances." This will provide services of all sizes with greater legal certainty, so they can undertake voluntary measures and develop innovative tools aimed at protecting users.

Maintaining cornerstone principles of the e-Commerce Directive, and improving them by, for example, adding protections for voluntary efforts to moderate content and creating mechanisms to support cross-border cooperation, will foster innovation and protect fundamental rights. It will also help ensure harmonisation across the Union.

Clarifications that could aid legal certainty

Small changes in the text would help ensure fidelity to the Commission's intent and provide services with legal certainty to meet their obligations. These include:

- Definition of illegal content (Article 2(g)): The Commission has explicitly stated that the DSA does not purport to define what illegal content is. This remains a matter for applicable national and EU law. Accordingly, there is a need to tighten the definition of illegal content by removing the text around "reference to an [illegal] activity," which could lead to excessive takedowns (e.g., would a video showing a car breaking the speed limit in Munich also qualify as illegal content?).

- Definition of marketplaces, or "online platforms that allow consumers to conclude distance contracts with traders" (Articles 5(3) and 22): These provisions are aimed at online marketplaces and, therefore, apply to online platforms that allow the consumer to conclude a distance contract with the trader *on the online platform*. The Commission's intent is evident in Article 5(3) which states that the concern is around online platforms presenting information or enabling transactions "*in a way that would lead an average and reasonably well-informed consumer to believe that the information, or the product or service that is the object of the transaction, is provided either by the online platform itself or by a recipient of the service who is acting under its authority or control.*" Online platforms that redirect the consumer to conclude a distance contract with the trader *on the third-party trader's site* should accordingly be explicitly carved out from the scope of application of Articles 5(3) and 22.

- Voluntary own-initiative investigations (Article 6): The Commission rightly introduced a clause providing that online intermediaries are not ineligible for the conditional liability exemptions *solely* because they carry out voluntary own-initiative investigations. To

meet the objective of promoting user safety, it is important to clarify that this provision *also* covers voluntary own-initiative investigations to detect content that violates a service's Terms and Conditions.

- Notice formalities giving rise to knowledge (Article 14(3)): The inclusion of notice formalities will help standardise and substantiate requests to remove illegal content. It is important to tighten the language in Article 14(3) to ensure that a notification that meets the requirements under Article 14(2) does not necessarily give rise to knowledge. As currently drafted, the DSA creates a risk of over-removal, which might negatively impact fundamental rights. For example, if a user argues that a piece of content is defamatory without providing other necessary context, the hosting service should not be incentivised to remove the content in order to avoid potential liability for it.

- Clearer distinctions for Cloud services: Cloud services should be explicitly classified as "basic hosting" services, to avoid the risk that they may be inadvertently subjected to the due diligence obligations for "online platforms." The main purpose of cloud services is not to disseminate information to the public, but rather to allow users to store personal content and share it within closed circles. For business-to-business cloud services, customers of cloud service providers -- and not cloud service providers themselves -- have ownership and control over the content they put on the cloud. Content moderation in the cloud can be impossible, as cloud service providers cannot always see and remove individual pieces of content, due to technical capabilities or privacy and contractual reasons. The DSA should take this complexity into account and should not subject cloud services to the most stringent due diligence obligations applicable to user generated content hosting platforms or social-media type of services.

- Clarity around fines (Articles 42 and 59): The DSA should make clear that fines may only be imposed for systemic violations of due diligence obligations.

Closing the backdoors to regulating lawful content

Backdoors in the risk management clauses may undermine EU fundamental rights

As currently drafted, the DSA might lead to regulation via the backdoor of illegal and lawful content alike. The DSA should neither allow regulators to define risks for businesses (Article 26), nor impose risk mitigation solutions on them (Recitals 59, 68 and Article 35).

- Regulators have wide powers to issue rules on illegal *and lawful content* in ways that have serious implications for fundamental rights, including restriction of free expression. For example, their powers extend to *lawful* content that may have a

"negative effect on... civic discourse," through Codes of Conduct that may become mandatory in practice for very large online platforms (pursuant to Recital 68).

- This runs counter to the Commission's stated intention to protect lawful content. In the Explanatory Memorandum, the Commission notes that lawful-but-harmful content "should not be subject to removal obligations, as this is a delicate area with severe implications for the protection of freedom of expression," yey these provisions risk exactly that result. They could also harm innovation and the fundamental right to conduct a business, if the regulators mandate the technical requirements for how platforms manage content.

- The DSA should remove these provisions that would lead to regulation of lawful conduct through the backdoor, and not through EU democratic processes.

Facilitating meaningful user redress

The text should aid efficiency, hinder bad actors, and protect the freedom to conduct a business

Provisions around out-of-court dispute settlement (Article 18), publication of statements of reasons (Article 15(4)) and limits on automation in complaint-handling (Article 17(5)) could open up avenues for abuse and weaken content moderation systems.

A. Out-of-court dispute settlement (Article 18)

Users should have the ability to appeal content decisions. However, the DSA provision on out-of-court mechanisms could lead to several unintended consequences:

- Enabling bad actors: Article 18 opens up avenues for abuse and does not scale to the millions of decisions online platforms make. Bad actors could use alternative dispute resolution (ADR) to arbitrate every content removal across EU Member States at a company's expense. Platforms remove billions of pieces of content from bad actors trying to spam, trick, or defraud users. Enabling bad actors to access ADR could slow down the process for legitimate seekers of redress. Surely this is not meeting the intent of meaningful user redress.
- National authorities' removal orders: Under the current DSA text, content uploaders may arguably also challenge services removals made pursuant to national authorities' removal orders (under Article 8), including where those orders may be confidential and appear as the online platforms' own decision. This may not have been intended, and underscores the implications of ADR provisions that have not been fully thought through.
- Fragmentation and confusion: The use of ADR by content uploaders to review any content moderation decision is highly likely to result in contradicting decisions by

different ADR bodies in different Member States as regards the same issues or policies. Given the scale of content moderation that online platforms engage in, trying to make sense of a patchwork of often contrasting (but nonetheless binding) decisions by different bodies across the EU risks paralysing online platforms' content moderation systems.

B. Publication of statement of reasons (Article 15)

We are concerned that the provisions in Article 15 lack clear value for users and regulators, and could risk user privacy, lead to abuse by bad actors, and interfere with law enforcement investigations.

- Publication: Making all statements of reasons available to the public (under Article 15(4)) would lead to undue burdens for hosting services, without clear value for users or regulators. Platforms would need to examine every single statement of reasons to remove personal data. Meanwhile, individual users will already be in a position to understand why certain action was taken over content they uploaded through individual statements of reasons addressed to them. Similarly, public authorities may request access to statements of reasons through their investigation powers under the DSA. Publication would also effectively provide a roadmap for bad-faith actors to game the services' content moderation systems.
- Level of detail: In addition, we are concerned by the granular level of detail we are required to include in statements of reasons. We note that there is a fair amount of tension between (i) treating notices in a timely manner (under Article 14) and, more generally, removing harmful content promptly, and (ii) drafting statements of reasons for content removals to share with content uploaders "at the latest at the time of the removal or disabling of access" (under Article 15). In addition, it may undermine efforts to use technology for detection and removal of scaled abuse, e.g. for spam. We urge policymakers to adopt a more flexible approach so that the provision does not apply where a detailed statement of reasons may not be appropriate, e.g. for spam and other scaled abuse, and for removals of child sexual abuse material to avoid interfering with potential law enforcement action.

C. Limits on automation in complaint-handling (Article 17(5))

The text in Article 17(5) is too rigid in requiring that no decision on appeal should be taken solely on the basis of automated means. This is not reasonable given the scale at which content moderation takes place, including around the billions of spam or bad ads content. The DSA should not undermine platforms' ability to detect and remove scaled abuse. Also, as occurred during the COVID pandemic, there are situations in which this may become simply infeasible.

A more appropriate outcome would be a risk-based approach to appeals, using a combination of human review and automation. For more egregious or nuanced cases online platforms may indeed need to more heavily rely on expert human review.

Safeguarding transparency and data access

Transparency can be insightful without being overly rigid, risking privacy, or enabling bad actors

There is no one-size-fits-all approach that makes sense across services, and meaningful transparency cannot come at the expense of user privacy or enabling bad actors. Safeguards should be added in the DSA to ensure transparency and data access obligations are reasonable, flexible, and proportionate.

- Transparency reporting obligations (Articles 13, 23, and 33): The transparency reporting obligations imposed on intermediaries are extremely broad. Policymakers should carefully consider the objective that each requirement seeks to achieve and define its scope in a proportionate manner, taking due account of what level of transparency is meaningful for users and feasible for intermediaries. For example:
    - Providing information on any content moderation that intermediaries engage in (under Article 13) is likely to (i) result in information overload that is difficult to make sense of, (ii) provide a roadmap for bad-faith actors to game content moderation systems, and (iii) involve a significant amount of engineering effort and associated costs, potentially crippling SMEs. Article 13(1)(c) should, at a minimum, be limited to content that is removed or disabled by the intermediary. Finally, the requirement in Article 13(1)(d) to report average turnaround time should be removed, as it may be an ineffective metric and could encourage platforms to make hasty decisions rather than work expeditiously but carefully to review content.
    - The requirement to provide information on the average monthly active recipients of the service in each Member State every six months (under Article 23(2)) imposes a disproportionate burden on online platforms. The 45 million user threshold to qualify as a very large online platform applies across the EU, irrespective of Member State. It is therefore unclear why this metric is required.
    - Transparency reporting templates (provided as a possibility under Article 23(4)) are too rigid to take account differences between services. They may become a reporting “straightjacket” that distorts the content moderation efforts different online platforms engage in. Online platforms should be provided with adequate flexibility to report on their efforts.

- It is not clear why users would need to have access to risk assessment reports, risk mitigation measures, audit reports, or audit implementation reports under Article 33(2). Obliging very large online platforms to engage in a confidential information redaction process prior to annual public disclosures would be disproportionate, given the level of detail included in those reports is unlikely to be of interest to the average user. In addition, making information on risk exposure and existing vulnerabilities public has the potential to be exploited by nefarious actors. These reports should rather be made accessible to regulators only as a means to ensure accountability of very large online platforms.

- National authorities' data gathering powers (Article 9): Article 9 does not contain the necessary safeguards for authorities to access user data. It creates legal uncertainty, as its requirements are inconsistent with, and push past the guardrails of, the draft e-Evidence Regulation. We believe Article 9 should match the standards and principles of the e-Evidence Regulation, including the need for harmonised legal frameworks for cross-border law enforcement requests within the EU, and strong procedural and substantive safeguards.

- Proactive notifications to authorities (Article 21): As written, the requirement under Article 21 for a service to notify authorities where it "becomes aware of any information giving rise to a suspicion that a serious criminal offence involving a threat to the life or safety of persons has taken place" would improperly shift the function of law enforcement investigation from government to private actors. We believe this Article should be aligned with the language used and safeguards included in the draft Terrorist Content Online Regulation. This would ensure the DSA reflects Europe's strong tradition of protecting privacy as a fundamental right.

- Access to data by researchers (Article 31): Researchers need to be able to access data to scrutinise or investigate issues of societal concern. However, as Article 31 is currently drafted, there are virtually no safeguards around what data may be requested, how such data may be accessed, and what may be done with the data. Suggested safeguards include:

    - Defining "reasoned request" to set parameters around what information can be requested and shared with vetted researchers, in line with the GDPR data minimisation principle.

    - Allowing online platforms to take additional measures to protect the privacy of data subjects (e.g. through pseudonymisation), where appropriate.

    - Allowing online platforms to object to methods of data transmission that they do not consider sufficiently secure, and to set limits on what can be done with

the data and clarify that the data should not be further shared/disclosed, in line with the GDPR purpose-limitation principle.

- Commission access to databases and algorithms (Article 57): Article 57 lacks safeguards, which are of heightened importance given that the provision relates to highly commercially sensitive information. Providing explanations over databases and algorithms in response to information requests by the Commission would be more proportionate than granting direct access. In addition, such information requests should only be directed to online platforms on the basis of a non-compliance investigation and under strict confidentiality safeguards.

Providing meaningful insights to oversight bodies

The auditing framework should support robust independent assessments

It is important for independent experts to be able to verify the risk assessments and risk mitigation measures of very large online platforms (VLOPs). An audit regime under the DSA should support robust analysis by auditors and provide meaningful insights to oversight bodies into how VLOPs are seeking to comply with DSA obligations. The audit regime as currently proposed may not achieve these aims.

The following suggestions would improve the auditing framework:

- The frequency and scope of routine audits (Article 28(1)):
    - To allow sufficient time for auditing activities, the frequency of routine audits under Article 28(1) should be at least every two years.
    - In line with the recommendations of this non-paper concerning Codes of Conduct and Crisis Protocols, the DSA should exclude these frameworks from the scope of audits under Article 28(1). In any event, the provisions on Codes of Conduct (Article 35) and on Crisis Protocols (Article 37) already envisage that there will be reporting on the measures taken under those frameworks; such reporting will allow assessments that are tailored and more appropriate to the measures at issue than the broader auditing framework.
    - In certain circumstances it will be beneficial to have the remediation plans of VLOPs independently audited (Article 50(3)). Where this does occur, and the relevant assessments and measures taken by VLOPs are deemed adequate, these aspects should be excluded from the scope of the next routine audit under Article 28(1).
- Triggers for ad hoc, voluntary audits (Article 50(3)): Given the range of obligations for VLOPs under Section 4 of Chapter 3, the DSA should clarify the circumstances in which

the Digital Services Coordinator (DSC) of establishment may request an ad-hoc audit of the action plan under Article 50(3). The DSC should only be able to trigger a request when there is evidence that VLOPs have diverged from baseline compliance standards.

- The timeframe for action plans: A period of one month is insufficient to develop an audit implementation report (Article 28(4)) or remediation plan (Article 50(2)). The DSA should adopt an objectives-based approach, where remediation timelines are based on the scope, severity and complexity of the auditor's recommendations or the decision of a DSC of establishment. A mechanism should be added whereby VLOPs would have a minimum of 45 days to acknowledge the recommendations, scope the work, and communicate a timeline for an action plan. Such an approach would support proportionate process rules, linking the response time to the scope, severity, and complexity of the recommendations.

- Adopting a risk-based approach to audit findings (Article 28(3)): To support the development of action plans and remediation, the DSA should adopt a risk-based approach to audit findings. For example, rather than 'positive, positive with comments, or negative' assessments (as is currently proposed in Article 28(3)), the risk-based tiers could be:

    - No/limited control gaps/findings, with observations
    - Medium control gaps/findings - 6 month remediation timeline
    - High control gaps/findings - 6 month remediation timeline
    - Critical control gaps/findings - 3 month remediation timeline