Response to the EDPB on the draft Guidelines 03/2025 on the interplay between the DSA and the GDPR

31 October 2025

Google welcomes the opportunity to provide feedback to the European Data Protection Board (**EDPB**) on its *Guidelines 3/2025 on the interplay between the DSA and the GDPR*, as adopted on 11 September 2025 (the **Guidelines**). Our response contains general observations on the Guidelines together with a number of specific points of interpretation that we would be grateful for the EDPB to consider.

Introductory remarks

Google's mission is to organise the world's information and make it universally accessible and useful. This objective is based on Google's founding goal of using technology to benefit the lives of our users, and to make the internet more transparent and helpful for all. Google's services are therefore designed to allow and encourage users to seek, engage, and share information safely and respectfully.

Google has long been aligned with the broad goals of the Digital Services Act (**DSA**),[1] including to address illegal and harmful activities, and to create a fair and open online platform environment. Google has devoted significant resources into tailoring our services to comply with the DSA[2] and has invested consistently in research, policies, and practices to offer age-appropriate ways for our users to participate in the online world. Such methods recognise the value of creativity and free expression, whilst seeking to protect and balance other fundamental rights, including but not limited to data protection.

The EDPB's acknowledgement of the interplay between the DSA and GDPR is welcomed. We think close coordination between data protection and online safety regimes is possible but requires an effort to ensure consistency and a clear definition of competences. Google therefore supports the EDPB's recent commitment to providing timely, clear, consistent, and practical guidance, and to proactively engage with other regulators to support a

[1] As summarised by the European Commission: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en.
[2] Google, Complying with the Digital Services Act, 24 August 2023: blog.google/around-the-globe/google-europe/complying-with-the-digital-services-act/.

cross-regulatory landscape (as outlined in the Helsinki Statement)[3]. This is especially important in relation to the intersection between data protection and digital regulation (including DSA obligations), which requires careful and consistent inter-regulatory cooperation.

However, notwithstanding the Helsinki Statement, the Guidelines do not appear to have been produced in cooperation with the European Board for Digital Services (**EBDS**) and, in their present form, contain impractical recommendations that indicate a misunderstanding as to how DSA obligations can be discharged (in particular, the level of human involvement in content moderation and the impact of a content moderation decision).

Google therefore urges the EDPB, prior to final adoption, to discuss the Guidelines in cooperation with the EBDS. This is to ensure that the Guidelines are based on a holistic and balanced interpretation of both the GDPR and DSA, and recognise - and seek to clarify - potential overlap proportionately and practically. This is necessary to avoid unnecessary regulatory fragmentation.

Key observations

Our response contains general observations on the Guidelines, grouped by the corresponding sections in the Guidelines.[4] We summarise our key observations for ease of reference below:

- **Unreasonably expansive interpretation of automated decision making with a legal or similarly significant effect:** The Guidelines risk creating significant ambiguity in relation to the application of Article 22(1) GDPR, in particular what constitutes a legal or similarly significant effect.

  For example, the EDPB indicates that the removal of illegal content, the suspension or removal of account privileges, the mere presentation of content on a recommender system, and the mere presentation of a specific advert could - in certain circumstances - produce legal effects concerning or similarly significantly affect the individual (if based on a solely automated decision). The rationale is unclear and Google encourages the EDPB to ensure the threshold for what is deemed a legal or similarly significant effect remains appropriate and proportionate.

  An unreasonably broad interpretation could apply Article 22 GDPR inadvertently to activities beyond the legislative intention of GDPR and data subject expectations. This could also frustrate core objectives of the DSA, including to protect consumers from harm online. For example, the DSA envisages (and expressly authorises) *automated*

[3] EDPB, The Helsinki Statement on enhanced clarity, support and engagement: A fundamental rights approach to innovation and competitiveness, adopted on 2 July 2025, www.edpb.europa.eu/system/files/2025-07/edpb-statement-20250702-enhanced-clarity-support-engagement_en_0.pdf.

[4] References to "Paragraphs" are to Paragraphs in the Guidelines.

content moderation - recognising that a degree of automation is essential to ensure reasonable, proportionate, and effective risk mitigation measures. Expanding Article 22 GDPR to any automated content moderation activities is disproportionate and counterproductive.

- **Unclear basis for expectations:** The basis for certain statements in the Guidelines appears unclear. For example, the EDPB indicates that the right to the protection of personal data takes precedence over other fundamental rights (which is not the case), and the Guidelines appear to read in obligations that are not in fact present in the DSA or GDPR. For example, the Guidelines indicate limitations on requesting further information from notifiers, retaining information on user's settings, or retaining the age or age range of a child following age estimation, irrespective of purpose of processing.

- **Expansive interpretation of deceptive design patterns:** The EDPB's examples of deceptive design patterns lack contextualisation. There is a risk that the Guidelines inadvertently seek to designate common and legitimate interface features (that are requested and expected by users) as inherently deceptive without a case-by-case assessment. Google encourages the EDPB to ensure it takes a user-centric approach that ensures objective assessment and consideration of real life evidence (noting that the Digital Fairness Act is subject to consultation).

- **Clarity on regulatory cooperation and separation of enforcement competencies:** The Guidelines recognise the lack of an explicit duty of consultation and cooperation between competent authorities in relation to the interplay between GDPR and DSA (and need for "adequate mechanisms" to ensure inter-regulator consistency). However, the Guidelines do not appear to have been developed in cooperation with the EBDS (in contrast to the EDPB's joint guidelines on the DMA and GDPR with the European Commission). The Guidelines also do not outline how the EDPB intends to ensure coherent interpretation and inter-regulatory cooperation in practice, and avoid the risk to the principle *ne bis in idem*. Further clarity is also necessary on how enforcement competencies under the DSA and GDPR will be maintained, not least to avoid duplication of proceedings and to ensure procedural safeguards (as set out under EU law) are respected.

- **Regulatory uncertainty on content moderation:** The Guidelines do not appear to recognise the practical implications of DSA obligations on providers of intermediary services; in particular, obligations concerning content that is harmful but not illegal. For example, content that may not be allowed on a service per its terms and conditions under Article 14 DSA, or that may give rise to the risks mentioned in Article 34 DSA for VLOPs and VLOSEs.

The EDPB's exclusive focus on *illegal* content in the Guidelines risks undermining core objectives of the DSA and appears contrary to existing European Commission guidance on the DSA.[5] It also raises considerable uncertainty; for example, how organisations can seek to identify and address content that is legal but which could have an adverse impact on users (particularly children),[6] the service, and the online environment. We encourage the EDPB to avoid adopting an overly restrictive and impractical approach that does not recognise the practical implications of obligations on service providers or the broader importance of content moderation.

The relationship between the DSA and GDPR

1. Fundamental rights must be balanced proportionally

Google welcomes the EDPB's recognition that a coherent interpretation and application of the DSA and GDPR is important, and that such interpretation and application must consider fundamental rights. The need for consistency in interpretation applies to both providers subject to the DSA *and* competent authorities. Google therefore encourages the EDPB to ensure that the final Guidelines recognise the relevance of other fundamental rights (beyond privacy and data protection), and acknowledge the importance of balancing all fundamental rights.

Data protection is not an absolute right

Fundamental rights outlined in the Charter of Fundamental Rights of the European Union (the **Charter**) include the freedom of expression and information, freedom of thought, and freedom to conduct a business - as well as privacy and data protection. However, the EDPB appears (in Paragraph 11) to elevate the status of the right to the protection of personal data above other fundamental rights, noting its "*singular importance*", without a basis in EU law.[7]

---

[5] The European Commission's *Guidelines for VLOPs and VLOSEs on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) DSA* (C/2024/2537), references the need to address "legal but harmful" forms of content, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024XC03014&qid=1714466886277.

[6] The European Commission's *Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) DSA* (C/2025/6826) explicitly refers to expectations and obligations under the DSA in relation to harmful but legal content, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C_202505519.

For example, the European Commission notes the importance of moderation to "*reduce minors' exposure to content and behaviour that is harmful to their privacy, safety and security, including illegal content or content that may impair their physical or mental development…*" (emphasis added). The European Commission also states that it considers platforms accessible to minors should establish moderation policies to identify and limit exposure to "harmful" content.

[7] The basis of this statement appears to be the Opinion of the Advocate General Szpunar delivered on 11 May 2023 in Case C-33/22 Österreichische Datenschutzbehörde. However, this element of the opinion was not included or referenced in the final judgment.

However, Recital 4 of the GDPR makes clear that the GDPR respects all fundamental rights, and that the right to the protection of personal data (which is not absolute) should be balanced against other fundamental rights in accordance with the principle of proportionality.[8] The CJEU also notes, in Case C-507/17, that "*...the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality...*" (emphasis added).[9]

Data protection must be balanced with other fundamental rights

However, the Guidance does not acknowledge the relevance of other fundamental rights, including those that the DSA seeks to protect. Google encourages the EDPB to recognise how such fundamental rights interact and how they can be balanced proportionately and appropriately. For example, European Courts, including the CJEU in *Tietosuojavaltuutettu* (interpreting Directive 95/46/EC),[10] have confirmed that in order to take account of the importance of the right to freedom of expression in a democratic society, it is necessary to interpret notions relating to that freedom broadly, and that account must be taken of the evolution and proliferation of methods of communication and the dissemination of information.

The Recitals of the DSA also recognise the importance of freedom of expression, and clearly emphasise the need to balance all rights, in particular the freedom to conduct a business, and consumer protection. For example:

> "*Responsible and diligent behaviour by providers of intermediary services is essential for a safe, predictable and trustworthy online environment and for allowing Union citizens and other persons to exercise their fundamental rights guaranteed in the Charter of Fundamental Rights of the European Union (the 'Charter'), in particular the freedom of expression and of information, the freedom to conduct a business, the right to non-discrimination and the attainment of a high level of consumer protection*" (Recital 3, emphasis added).

---

[8] GDPR, Recital 4, "*...The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This Regulation respects all fundamental rights and observes the freedoms and principles recognised in the Charter as enshrined in the Treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity.*"

[9] CJEU, Case C-507/17, paragraph 60, https://curia.europa.eu/juris/document/document.jsf?docid=218105&doclang=EN.

[10] CJEU, Case C-73/07, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62007CJ0073.

"This Regulation respects the fundamental rights recognised by the Charter and the fundamental rights constituting general principles of Union law. Accordingly, this Regulation should be interpreted and applied in accordance with those fundamental rights, including the freedom of expression and of information, as well as the freedom and pluralism of the media. When exercising the powers set out in this Regulation, all public authorities involved should achieve, in situations where the relevant fundamental rights conflict, a fair balance between the rights concerned, in accordance with the principle of proportionality" (Recital 153, emphasis added).

"*When designing, applying and enforcing those restrictions, providers of intermediary services should act in a non-arbitrary and non-discriminatory manner and take into account the rights and legitimate interests of the recipients of the service, including fundamental rights as enshrined in the Charter. For example, providers of very large online platforms should in particular pay due regard to freedom of expression and of information, including media freedom and pluralism"* (Recital 47, emphasis added).

Voluntary own-initiative investigations and legal compliance in relation to illegal content (Article 7)

2. Processing personal data is necessary to develop and deploy content moderation tools

The EDPB recognises (Paragraph 14) that the development of content moderation[11] techniques can involve machine learning techniques that require "*large amounts of data to train on to predict whether a piece of content constitutes illegal content*". However, the EDPB subsequently notes that the training of such models and their deployment "should not involve any processing" of personal data "insofar as possible".

Google would welcome further clarity on this apparent contradiction. The EDPB separately recognises (in its 2024 Opinion) that data minimisation does not *prevent* the processing of personal data, and there are legitimate purposes of using personal data in the development and deployment of AI models. For example, to avoid the risks of potential biases and errors.[12]

[11] The term **content moderation** in this response refers to both automated and non-automated own-initiatives to detect, identify, and address illegal and harmful content or to take the necessary measures to ensure compliance with EU law.

[12] EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models Adopted on 17 December 2024, www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf, Paragraph 64.

This is recognised by EU supervisory authorities, such as the CNIL, which confirms that the data minimisation principle "*does not prevent the use of large training datasets*".[13]

Google therefore encourages the EDPB to acknowledge in the final Guidelines that it is likely necessary in practice to process personal data (that is adequate and relevant) in order to develop and deploy effective content moderation tools.[14] For example, such processing is necessary not just for the purposes of ensuring user safety and complying with obligations under the DSA (such as to implement effective safeguards), but also to discharge requirements under the AI Act and GDPR (such as in relation to accuracy and bias mitigation).

3. Legal basis: detecting illegal content represents a societal legitimate interest

Google welcomes the EDPB's recognition that there is a legitimate interest in detecting and addressing illegal content on intermediary services to protect the recipients of that service (Paragraph 18), and that legitimate interests (Article 6(1)(f) GDPR) is an available legal basis.

The Guidelines note that this interest is legitimate "in particular" where content can be disseminated to the public via an "online platform". Google encourages the EDPB to recognise that such interest remains legitimate, irrespective of medium or platform, for all intermediary service providers, and that such interest extends to content that is contrary to providers' terms of service (which the provider deems harmful for users, but which is not necessarily illegal).

Detecting, identifying, and removing illegal and harmful content (not just on online platforms) demonstrates a clear positive impact, not just to the service users but also broader interests, including to the wider community. This recognition of the broader societal interest would demonstrate consistency with the Article 29 Working Party position that "*[s]ome interests may be compelling and beneficial to society at large*".[15]

The Guidelines therefore provide the EDPB with a constructive opportunity to recognise the societal benefits of content moderation (including automated content moderation) and to acknowledge that such benefits can be considered as part of a legitimate interests

---

[13] CNIL, AI and GDPR: the CNIL publishes new recommendations to support responsible innovation, 7 February 2025, www.cnil.fr/en/ai-and-gdpr-cnil-publishes-new-recommendations-support-responsible-innovation.

[14] Article 5(1)(c) GDPR (the "data minimisation" principle) requires the processing of personal data to be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*".

[15] Article 29 Data Protection Working Party, WP217, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC Adopted on 9 April 2014, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf , page 24.

assessment.[16] This would continue to protect the rights and freedoms of individuals (as such interest would be subject to the necessity and balancing conditions, in the context of the legitimate interests assessment), and give confidence to organisations seeking to conduct appropriate and proportionate content moderation.

4. **Legal basis: transparency must be proportionate**

The EDPB states (Paragraph 18) - in commentary on legitimate interest - that intermediary service providers acting as controllers should take "all necessary steps"[17] to inform data subjects about the concrete measures envisaged by the controller to "*detect, identify and remove (or disable access) to illegal conten*t".

The Guidelines would benefit from a clear statement by the EDPB that intermediary service providers (acting as controllers) do not need to undermine the effectiveness of the underlying content moderation technique in order to discharge their respective transparency requirements.

It would be contrary to public policy and the aims and obligations under the DSA to expose information in relation to the organisational and technical functionality of content moderation processes. This would significantly undermine the efficacy of such processes, which are essential to avoid bad actors from exploiting information in relation to content moderation (given the risk of serious, sophisticated, and repeat offenders).

5. **Legal basis: content moderation can be necessary to protect the vital interests of individuals and to enforce terms entered into by the user**

The EDPB does not consider the application of other legal bases under Article 6 GDPR in the context of content moderation. However, there are circumstances where other legal bases could also apply to content moderation. Google encourages the EDPB to recognise such legal bases and their relevance to content moderation.

---

[16] We encourage the EDPB to consider our comments on the application of legitimate interest in Google's 2024 consultation submission on the EDPB's draft guidelines 1/2024 on processing based on Article 6(1)(f) GDPR, https://www.edpb.europa.eu/sites/default/files/webform/public_consultation_reply/google-response-to-edpb-consultation-on-legitimate-interests-guidelines-20-november-2024.pdf.

[17] Google notes that the requirement to provide the data subject with information on the legitimate interests pursued by the controller (under Article 13(1)(d) and Article 14(2)(b) GDPR) does not require the controller to take "all necessary steps". The Guidelines reference the Judgment of the Court of Justice of 4 July 2023 *Meta Platforms and others*, C-252/21, paragraph 26. However, this paragraph does not concern legitimate interests, and does not impose a requirement to take "all necessary steps".

For example, the detection and combating of Child Sexual Abuse Material (**CSAM**) online in some contexts may be necessary in order to protect the vital interests of a data subject or another natural person. Article 6(1)(d) GDPR may therefore be an available legal basis in such circumstances.

Similarly, where the application of content moderation tools is a necessary part of enforcing terms of service (entered into by the user), the processing is necessary for the performance of a contract to which the data subject (the user) is party. Article 6(1)(b) GDPR may therefore be an available legal basis in such circumstances.

6. **Legal basis: legal obligation threshold must remain consistent**

Though the EDPB recognises legal obligation as a potential lawful basis, the Guidelines appear to impose additional requirements for intermediary service providers (without clear rationale) to rely upon the legal basis for the purposes of content moderation. For example, the EDPB notes (Paragraph 21) that the relevant law underpinning the legal obligation "*must indicate in what circumstances and under which conditions a measure providing for the processing of personal data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary*".

However, the basis of this statement (Judgment of the Court of Justice of 21 June 2022, *Ligue des droits humains*, C-817/19) does not in fact relate to compliance under GDPR - and does not apply this criteria to establishing a legal obligation under Article 6(1)(c) GDPR. Instead, the referenced judgment concerns whether (and how) a *Member State* can justify a limitation to the rights guaranteed in Articles 7 and 8 of the Charter when transposing EU Directives (such as Directive (EU) 2016/681) into national law. The relevance of the judgment to the Guidelines is therefore unclear.

Similarly, the threshold articulated by the EDPB for legal obligation (which refers to processing *required* by law) does not reflect the test under Article 6(1)(c) GDPR, as clarified by Recital 41 GDPR. As per Recital 41 GDPR, legal obligation does not necessarily require a legislative act, and does not require a specific obligation imposing the specific processing activity. The processing must simply be reasonable and proportionate to achieve compliance with a clear and precise legal basis, the application of which is foreseeable to persons subject to it.

Google therefore encourages the EDPB to ensure that the Guidelines do not unintentionally raise the threshold or criteria for relying upon legal obligation under Article 6(1)(c) GDPR, especially for the purposes of content moderation carried out pursuant to the DSA.

7. **Legal basis: legal obligation remains applicable to own-volition content moderation**

The Guidelines also indicate that, because controllers are "*not legally required to carry out processing for these purposes*", legal obligation (Article 6(1)(c) GDPR) is not an available legal basis for own-volition content moderation activities. Google would welcome further exposition on this statement, especially considering our comments immediately above.

The threshold for legal obligation under Article 6(1)(c) GDPR is *not* whether the processing is "required" at law, but whether the processing is "necessary" for compliance with a legal obligation to which the controller is subject. The EDPB has also previously confirmed that legal obligation could provide an alternative lawful basis for the processing of data for fraud prevention purposes.[18] This previous confirmation (in relation to fraud prevention) did not specify that such fraud prevention had to be *legally required* or exclude voluntary efforts to prevent fraud.

Content moderation is necessary to discharge the DSA's core purposes and is expressly authorised by the DSA. For example, Article 35 DSA requires VLOPs and VLOSEs to put in place reasonable, proportionate, and effective mitigation measures to address the specific systemic risks identified. Such measures explicitly include content moderation processes (as per Article 35(1)(c) and Recitals 84 and 87 DSA).

Article 7 DSA also notes that conducting voluntary own-initiative investigations does not prevent intermediary service providers benefiting from the liability exemptions contained in Articles 4, 5, and 6 DSA, including when carrying out voluntary investigations to take "*necessary measures to comply with the requirements of Union law and national law in compliance with Union law, including the requirements set out in this Regulation.*" The EDPB's indication that legal obligation (Article 6(1)(c) GDPR) would not apply to voluntary content moderation, even if such processing was to demonstrate compliance with the DSA (or other legal requirements under EU or Member State law), is therefore unclear.

Legal obligation must remain an available legal basis for content moderation activities, even if own-volition, especially if conducted to demonstrate broader compliance with DSA principles and obligations.

8. **Legal basis: providers cannot be prevented from complying with valid legal requests**

[18] EDPB, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf - paragraph 50.

The DSA recognises that intermediary service providers may receive orders from relevant national judicial or administrative authorities (issued under different legal regimes), for example, to act against a specific item of illegal content or to provide information about specific service recipients.

In relation to such orders, Articles 9 and 10 of the DSA require intermediary service providers to provide certain information without undue delay to such national judicial or administrative authorities. In particular, to confirm what action has been taken and when.

However, neither Article 9 nor Article 10 of the DSA imposes an obligation on the intermediary service provider to review, verify, or challenge the order transmitted to the provider. Instead, in each case, the DSA obliges the *Member State* (not the provider) to "ensure" that relevant orders meet certain conditions. Recital 31 of the DSA also confirms that the DSA does not - itself - provide the legal basis for the issuing of orders by such authorities (i.e. the requirements of Article 9(2) and Article 10(2) DSA do not affect whether or not the relevant order is binding on the provider).

Notwithstanding the above, the EDPB indicates in the Guidelines (Paragraph 21) that an intermediary service provider can only rely upon legal obligation (as a legal basis under Article 6 GDPR), when complying with such an order if it verifies that the competent authority has issued the order in accordance with Articles 9 or 10 DSA.

There is no basis for this threshold. This would apply an additional and impractical obligation on relevant providers that is not present in the wider policy objectives of DSA and GDPR. Where a competent national judicial or administrative authority has issued an order for the provider to take action or provide information - in accordance with the applicable legal regime - it is reasonable and proportionate for the provider to rely upon legal obligation as its legal basis. It would be contrary to the public interest to seek to limit and therefore prevent intermediary service providers from responding to such orders (often in highly time sensitive circumstances) which are executed in good faith by providers.

9. Special condition: detecting illegal content represents a societal legitimate interest

As society becomes increasingly comfortable discussing sensitive matters (such as relating to health, sexuality, race, religion and politics) online, there is a possibility that the moderation of content can include the processing of special category data under Article 9 GDPR. Google encourages the EDPB to recognise that if activities undertaken by providers pursuant to the DSA (such as content moderation) involve the processing of special category data, providers

can rely on the substantial public interest condition (as per Article 9(2)(g) GDPR), subject to suitable and specific measures to safeguard data subjects' fundamental rights.

The EDPB also notes the requirements of Article 22(4) GDPR (Paragraphs 33 and 73). However the Guidelines do not contain commentary on whether providers can rely on either Article 9(2)(a) or (g) GDPR in relation to automated decision making subject to Article 22 GDPR. Considering the circumstances of content moderation, and the practical challenges in seeking explicit consent for content moderation, the Guidelines would benefit from clearly acknowledging that content moderation represents a substantial public interest and is (through the DSA) subject to suitable measures to safeguard data subjects' rights and freedoms.

10. Special condition: expansive application of Article 9 risks reducing appropriate safeguards

The EDPB (Paragraph 72) indicates an expansive interpretation of Article 9(1) GDPR. In particular, the Guidelines suggest that Article 9(2) GDPR applies irrespective if the controller is intentionally processing special category personal data (i.e. regardless as to the purpose of processing) or whether the controller is aware that they are processing such personal data.

This risks an impractical and counterintuitive approach - in particular in relation to content moderation, and the effective and safe delivery of advertising - whereby the EDPB seeks to apply Article 9 beyond its statutory scope. It also ignores the fact that certain categories of special category data are dependent on the purpose of processing. For example, biometric data is only special category data under Article 9 GDPR *if the controller processes that personal data for the purpose of uniquely identifying an individual*.

Content that is subject to moderation can contain various categories of personal data, many of which are entirely irrelevant to the moderation decision. For example, content that infringes copyright but which incidentally contains political speech relating to an individual. It would be disproportionate and hinder efforts to protect users online and comply with DSA obligations (including to remove illegal and harmful content), if Article 9 GDPR was applied to personal data that was entirely incidental to a content moderation decision. For example, it would be unreasonable and impractical to expect a provider to seek the explicit consent (under Article 9(2)(a) GDPR) of the user who posted such content in order to moderate that content.

11. Removal of illegal content: overly broad interpretation of legal or similarly significant effect

The Guidelines appear to assert (Paragraph 22) that the removal of illegal content could affect recipients (whose content is removed) so significantly that Article 22 GDPR is triggered (if the

decision was based solely on automated processing). Google would welcome further clarity on this position. In particular, exposition on the EDPB's rationale on how and why the removal of illegal content (or allegedly illegal content) could have a *legal* effect or a *similarly significant* effect on an individual.

The EDPB's approach appears inconsistent with the DSA's own express authorisation of automated content moderation tools. For example, the DSA defines "content moderation" to explicitly capture both automated and non-automated activities. It would frustrate the purposes of the DSA to assert that any application of such automated content moderation activities (as authorised by the DSA) could automatically constitute a legal or similarly significant effect.

As per the Article 29 Working Party Guidelines on automated individual decision making,[19] the wording of Article 22 "*makes clear that only serious impactful effects will be covered"*. By way of example, the Article 29 Working Party explicitly references decisions affecting legal rights, such as to vote in an election or take legal action, the refusal of admission to a country or denial of citizenship, or an impact on an entitlement to a social benefit granted by law such as housing benefit. The removal of content on an online platform is highly unlikely to ever significantly affect the recipient in such a manner.

It is also currently unclear whether the EDPB's position - i.e. the indication that the mere removal of illegal content could constitute a legal or similarly significant effect - applies only to the removal of content that was allegedly (*but not in fact*) illegal, or also to content that was both allegedly *and factually* illegal. It would be particularly problematic if the Guidelines sought to restrict the removal of content that was factually illegal or harmful.

Google, like many platforms, makes significant use of online safety tools. Such tools frequently involve human reviewers (e.g. in relation to CSAM). However, the scale of online activity - considering the volume, the number of users, and 24 hour nature - means it would be highly challenging, and could impact the efficacy of safety mechanisms, to implement adequate online safety measures without reliance on solely automated tools. The sheer scale of content posted and user activity across our services means that automated tools are essential in our efforts to ensure a safe online environment: human review in all cases is neither possible nor desirable - automated content moderation tools are an appropriate, proportionate and effective safeguard for online safety.

It is therefore important to avoid an overly broad interpretation of "legal or similarly significant effects", to ensure that Article 22(1) GDPR is not triggered for relatively minor consequences,

[19] Article 29 Data Protection Working Party, WP251rev.01, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

such as the removal of posting privileges, which in each case are subject to appeal pursuant to the DSA. This would also align and ensure consistency with Recital 71 of the GDPR, which refers to the refusal of credit and e-recruiting practices. It would not be proportionate to compare these examples with the removal of online content.

Google therefore encourages the EDPB to acknowledge that, *in the vast majority of instances,* the removal of (illegal or harmful, or allegedly illegal or harmful) content would not meet the threshold for a legal or similarly significant effect, and that very few content moderation decisions would trigger Article 22 GDPR.

12. Removal of illegal content under the DSA should benefit from Article 22(2) GDPR

The EDPB notes (Paragraph 22) that an exemption under Article 22(2) GDPR is necessary if Article 22(1) GDPR applies. However, the Guidelines do not provide guidance on such exemptions.

As outlined above, we consider that content moderation decisions that are based solely on automated processing of personal data are generally highly unlikely to meet the threshold for a legal or similarly significant effect. However, if such decisions were to trigger Article 22(1) GDPR in practice, the final Guidelines should recognise that the exemptions in Article 22(2)(a) or Article 22(2)(b) GDPR likely apply in the context of content moderation pursuant to the DSA.[20]

For example, in relation to Article 22(2)(b) GDPR, Recital 71 GDPR recognises that the exemption applies where a decision is expressly authorised (not necessarily required) by EU or Member State law - "*including for fraud and tax-evasion monitoring and prevention purposes*". Taking measures to address *illegal* content (which could include fraudulent material) by intermediary service providers is therefore directly analogous. For example, as per the definition of "content moderation" (Article 3(t) DSA) and the recognition that content moderation will use automated means (Article 15(1)(e) DSA), the DSA explicitly envisages, authorises, and expects that automated content moderation will be used by providers to discharge their obligations under the DSA. The DSA also provides suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, including via the requirement to provide transparency and an appeal right over a content moderation decision.

In relation to Article 22(2)(a) GDPR, intermediary service providers typically prohibit the creation and dissemination of illegal and harmful content on their services in their terms and conditions and respective agreements with the user. As a result, the removal of illegal or harmful content - generated by the user in breach of their contract with the provider - in

[20] This would apply in the very rare occasions where a decision to remove illegal content, following a solely automated decision, produces a legal or similarly significant effect on an individual.

accordance with the DSA is necessary to perform that contract. It is in the public interest for intermediary service providers to benefit from the exemptions under Article 22(2)(a) GDPR to exercise their rights to manage their service.

13. Content moderation does not intrinsically constitute high-risk processing

The Guidelines (Paragraph 24) indicate that content moderation activities pursuant to Article 7 DSA (irrespective of the nature or relevant context of such activities in practice) are "likely" to fulfil criteria necessitating a DPIA. However, content moderation activities do not generally pose a high risk to the rights or freedoms of data subjects, and - as with any processing activity - the relevance and likelihood of risks change depending on the specific activity.

Google therefore encourages the EDPB to acknowledge in the final Guidelines that whether a DPIA is necessary for content moderation processes will *in fact* depend on the relevant circumstances and require a contextual assessment to assess whether the processing is "*likely to result in a high risk to the rights and freedoms of natural persons*" (as per Article 35 GDPR).

For example, removing products or descriptions of product information posted by businesses and merchants on shopping platforms (where such content does not comply with applicable terms, including if the content infringes copyright). This is necessary to maintain the integrity of the platform, protect users from harm, and ensure that content reflects applicable terms and user expectations. The identification and removal of such content is highly unlikely to pose a high risk to the rights or freedoms of individuals.

Processing of personal data in notice and action mechanisms and in internal complaint-handling systems (Articles 16, 17, 20, and 23 DSA)

14. Providers are required to request the identity of the notifier, and the notice may require their identity

The EDPB recognises (Paragraph 30) that a provider may deem it necessary to identify the notifier, including to request additional data. This is particularly relevant in relation to allegations (such as defamation and equivalent claims), where generally only the affected individual can challenge the content.

However, the EDPB subsequently notes that providers should not make the submission of a notice contingent on the notifier providing their identity. The basis of this statement under the DSA is unclear, given that Article 16(2)(c) DSA specifically requires providers to ask for the name and contact information of the individual or entity submitting the notice. Other than in instances where the information relates to a relevant offence referred to under Directive

2011/93/EU (i.e. as per Article 16(2)(c) DSA), no restriction against requiring this information exists in Article 16(2) DSA.

Indeed, Recital 53 of the DSA confirms that, except for such offences under Directive 2011/92/EU, *"those [notice] mechanisms should ask the individual or the entity submitting a notice to disclose its identity in order to avoid misuse"* (emphasis added).

Google encourages the EDPB to recognise that it can be reasonable and proportionate for a provider to insist on the identity of the notifier for the purposes of a submission, especially considering the potential for misuse (as explicitly recognised by Recital 53 of the DSA). For example, this is necessary to identify the relevant rights holder, and to ensure the notice and action system is not abused to cause detriment to others, including undermining their fundamental rights.

15. DSA requires notices to be adequately substantiated

The EDPB also appears (in Paragraph 30) to apply an additional restriction that is not present in the DSA, namely that a provider "*should generally not ask for notifiers' additional personal data [other] than those referred to in Article 16(2) DSA*". Google encourages the EDPB to recognise that a provider may in fact need to consider and request information that is not included in Article 16(2) DSA, where necessary (subject to data minimisation and purpose limitation principles).

Article 16(2) DSA does not limit or restrict a provider from only asking specific questions or requesting specific data. On the contrary, the Article emphasises the importance of ensuring that the notice is "sufficiently precise and adequately substantiated". The provider is therefore permitted under the DSA to request further information which it considers necessary. Google encourages the EDPB to recognise such circumstances to avoid unintentionally limiting providers from discharging their DSA obligations (which remain subject to purpose limitation and data minimisation obligations under GDPR).

16. DSA and GDPR permit automated decision making

Paragraph 41 of the Guidelines indicates that the EDPB expects controllers should avoid conducting automated decisions when building safeguards against misuse of online platforms in the context of Article 23 DSA. This is irrespective of the effect on the individual, or whether Article 22(1) GDPR is in fact engaged:

> "*In this regard* [envisaging safeguards against the misuse of online platforms]*, the EDPB welcomes the safeguards the DSA already identifies, as they will allow avoiding the*

adoption of automated decisions in such cases..." (Paragraph 41, Guidelines, emphasis added).

However, no such recommendation or prohibition exists under GDPR or DSA. Article 23(1) DSA does not prohibit or prevent the application of tools that allow for "automated decisions" as a measure to protect against misuse of online platforms. The issuing of a prior warning and reasonable suspension can be conducted via automated tools, including on a case-by-case basis. Similarly, Article 23 DSA does not prohibit or prevent the use of solely automated decision making (with or without legal or similarly significant effect).

The EDPB therefore risks conflating any automated decision with an automated decision that triggers Article 22(1) GDPR, or indicating that any automated decisions (irrespective of impact) should be avoided. This does not reflect the reality of online safeguards in practice, appears to read in a restriction that is not in fact present in the DSA, and frustrates the implementation of "appropriate, proportionate and effective" safeguards to protect users (as per Recital 63 DSA).

Google encourages the EDPB to recognise that the term "case-by-case basis" in Article 23(3) DSA does not require human involvement (either in practice or under the DSA), and automated decision making can (and in many cases, must) be conducted to discharge, and to reflect the criteria outlined in, Article 23(3) DSA. In many circumstances, considering the potential harm to users and the scale and frequency of misuse, such decision making *must* be automated in order to be appropriate, proportionate, and effective, and for providers to discharge their obligations under the DSA.

17. Account suspension does not indicate a significant effect

The EDPB states (Paragraph 42) that it is "likely" that the decision of an online platform provider to suspend the activities of persons it considers to be "*engaged in abusive behaviour may significantly affect their rights*". The rationale for this statement is unclear, or how such action would in fact affect the data subject's rights, especially without a case-by-case assessment.

The Guidelines would benefit from a greater recognition of proportionality. For example, an acknowledgement that it is important to balance rights and freedoms proportionally to consider whether any actual harm is justified considering the relevant circumstances (for example, whether a temporary suspension of posting rights is justified).

Similarly, as per our comments above in relation to illegal or harmful content moderation, Google encourages the EDPB to ensure that the threshold for a "significant" effect - especially considering Article 22(1) GDPR - is not expanded or set too low. This would create significant practical burdens and be contrary to the spirit of the GDPR (and Article 29 Working Party Guidelines).

Deceptive design patterns (Article 25 DSA)

18. Examples of deceptive design patterns must be proportionate and contextualised

Google supports efforts to assess deceptive patterns and to create sustainable frameworks with which to evaluate their influence. In particular, such frameworks should appropriately consider whether a design feature benefits users, or has been requested or is expected by users.[21]

As a result, there is a risk that the Guidelines apply an overly expansive interpretation of a deceptive design practice without recognising the need for contextual assessment and without considering the benefits to or intentions of the user. An unclear and potentially expansive interpretation may harm innovation that benefits users of online services and exceed legislative intentions (noting that the Digital Fairness Act, which is anticipated to address deceptive pattern issues, remains subject to consultation).

For instance, the example contained in Paragraph 44 of the Guidelines is provided without context or consideration of the potential benefits to the individual. The rationale for designating this example as a deceptive design pattern is unclear; it is highly unlikely to hinder an individual's ability to make a conscious choice.

Similarly, Paragraph 47 identifies "*common examples of deceptive design patterns that [in the EDPB's opinion] may cause addictive behaviour*". These examples - many of which are common and popular features of many online experiences - are presented without commentary. For example, the Guidelines do not consider the specific context in which they are deployed, their impact on the user in reality, or recognise the benefit to or agency of the individual. Google therefore encourages the EDPB to avoid designating common and legitimate features as inherently deceptive (and by extension, unlawful) without a contextual case-by-case assessment.

It is also unclear to us on what foundation the EDPB has based its analysis on addictive behaviour. Behavioural addiction in an online environment is a highly complex topic that requires nuanced and scientific analysis; the EDPB's ability to designate a design pattern as causative to addiction is not explained and the complexity of the topic should be recognised. The EDPB also provides no indication as to the types of objective evidence that can be used as an indication of deceptive design leading to addictive behavior.

[21] Google, Unpacking deceptive design: A more user-centric framework for assessing and categorizing dark patterns, static.googleusercontent.com/media/publicpolicy.google/en//resources/unpacking_deceptive_designs.pdf.

Advertising transparency and prohibition of presenting advertisements based on profiling using special categories of data (Article 26 DSA)

19. Presenting an advert does not produce legal or similarly significant effects

The EDPB indicates (Paragraph 62) that the provisions in Article 26(1) DSA could constitute automated decision-making subject to Article 22 GDPR. The rationale for this is unclear. As per our comments above in relation to illegal or harmful content moderation, further clarity is needed on how and why the presentation of a specific advertisement could have a *legal* effect or a *similarly significant* effect on an individual.

The Article 29 Working Party Guidelines notes that the wording of Article 22 GDPR "*makes clear that only serious impactful effects will be covered"*[22] and, by example, identifies a decision that impacts an individual's right to vote in an election. The presentation of an advert (irrespective of specificity) is not in any way analogous to impacting a right to vote, and is highly unlikely to ever significantly affect the recipient in a legal or similarly significant manner.

The EDPB also provides examples (in Paragraph 62 of the Guidelines) of recommended criteria to assess whether an automated decision to present a specific advertisement triggers Article 22(1) GDPR. However, these examples fail to consider or assess the impact on the individual (i.e. whether the impact is in fact legal or similarly significant). There is therefore a risk that the EDPB is seeking to argue that the act of contextualising or personalising an advert itself constitutes profiling, and that such contextualisation or personalisation itself automatically produces legal effects concerning, or similarly significantly affects, the individual. This is not the case or the threshold in Article 22(1) GDPR.

Recommender systems (Articles 27 and 38 DSA)

20. Recommender systems benefit users; the general presumption cannot be that they create significant risks

Google encourages the EDPB to reflect on the real-world value and benefits of recommender systems, the different context in which they operate, and that the types of personal data used may vary considerably across platforms.

Recommender systems are in principle designed to enhance user experience and utility. They therefore act as a risk mitigation measure, enabling users to access high-quality information

[22] Article 29 Working party, WP251rev.01, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

that is appropriate to their search result and settings, preventing harmful and repetitive exposure, and empowering user controls and choices. As the Guidelines appear to acknowledge (Paragraph 81), recommender systems also allow users of online platforms with large catalogues of content to access and engage with the most responsive and relevant content.

It is therefore unclear on what basis the EDPB generally indicates that recommender systems present serious risks to data subjects, and that the presentation of specific content to online platform users (via a recommender system) could constitute a decision with legal or similarly significant effect (Paragraph 84).

As per the Article 29 Data Protection Working Party Guidelines, for data processing to significantly affect someone, the effects must be "*sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to significantly affect the circumstances, behaviour or choices of the individuals concerns; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals*" (emphasis added).

The mere presentation of content is unlikely to meet this threshold. There should be no presumption that a recommendation creates a legal, economic, or social effect on the user.

Similarly, further clarity would be welcomed on the statement that "behavioural analysis for prediction purposes" constitutes profiling. This does not account for the context or specific behaviour considered, and therefore risks applying an overly expansive interpretation of profiling contrary to GDPR. As per Recital 71 GDPR, profiling consists of automated processing evaluating personal aspects relating to a natural person, *where it produces legal or similarly significant effects*. The EDPB's current formulation could capture basic features such as contextualisation and recommended content to reflect language, region, font size, or other basic user settings, without considering the impact on the individual.

As a result, there is a danger that the Guidelines seek to lower the threshold for Article 22(1) GDPR in a manner that is impractical, disproportionate, and contrary to the spirit of the GDPR and DSA.

21. Equal presentation is not required by either DSA or GDPR

The EDPB states (Paragraph 87) that providers of VLOPs and VLOSEs should present both options (provided under Article 38 DSA) equally on first use of the service. Google would welcome the specific obligation under the DSA upon which this statement is made, as the legal basis is unclear and appears to expand the obligations without a clear rationale in either GDPR or DSA.

The Guidelines also note that providers should not "nudge" service recipients to use a particular option. Google encourages the EDPB to consider broader obligations on, and commitments by, service providers (such as VLOPs and VLOSEs), for example to inform users whether a particular option provides more targeted and relevant results. It is also essential that the Guidelines ensure appropriate consideration of all fundamental rights - including freedom to conduct a business. There is otherwise a risk that the EDPB appears to be preventing providers from noting the benefits of their services and features to users, which risks damaging the user experience and user-centric innovation.

22. Storage of user choices is necessary for accountability

Paragraph 88 of the Guidelines indicates that the EDPB believes the collection and processing of a user's choices (in relation to modifying system parameters, i.e. user settings) should only be processed for the "sole" purpose of complying with the DSA. The EDPB asserts that providers should not retain a history of previous user choices. The basis of this limitation (which ignores the purpose of processing by the provider) under either GDPR or DSA is unclear.

Google encourages the EDPB to recognise that it can be both necessary and appropriate to process and retain a user's previous choices. The DSA also does not prevent or restrict a provider from processing user settings. Such processing may in fact be necessary to demonstrate accountability under other legal regimes, other than the DSA - including the GDPR (if the user choice constitutes data protection consent). It would therefore be essential to retain user preferences to ensure that appropriate settings are applied to the user, and to demonstrate accountability to the user (or competent authority) as necessary.

There are clear benefits to users and society to recognise how, when, and why users interact with user settings and features to ensure effective, consistent, and improved user experiences. Such processing is in the user's interest and helps justify privacy-centric innovation. Preventing providers from considering how their users engage with their settings risks stifling privacy-conscious development.

Protection of minors (Article 28 DSA)

23. Certainty on age assurance helps encourage privacy-conscious innovation

Google welcomes the certainty provided by the EDPB (Paragraph 92) that providers can rely upon legal obligation under Article 6(1)(c) GDPR - on the basis of Articles 28(1) and (2) DSA - when discharging obligations to implement appropriate and proportionate measures to ensure the online protection of minors, including age assurance. Google supports the application of a

case-by-case assessment and the emphasis on proportionality and necessity that considers the specific context and risks posed.

Google threfore also encourages the EDPB to recognise the need to build, improve, assess, and develop such appropriate and proportionate measures. In particular, the Guidelines would benefit from an explicit recognition that processing related to the improvement, development and assessment of appropriate and proportionate measures (used to discharge Article 28(1) and (2) DSA) is a legitimate interest under Article 6(1)(f) GDPR. This would also recognise the necessity (and wider benefits) to the proportionate use of personal data collected in the context of age assurance for compatible purposes in relation to the improvement and assessment of such age assurance, and for ensuring an age-appropriate environment.

Google further encourages the EDPB to provide similar certainty on the processing of biometric data for the purposes of age assurance. Specifically, where the purpose of processing is not to uniquely identify the individual. For example, where the purpose is to simply estimate an age or age range, the biometric data does not constitute special category biometric data that is subject to Article 9 GDPR.[23] As envisaged by both the definition of biometric data under Article 4(14) GDPR, and the distinction in Article 9 GDPR, the GDPR intends biometric data to only become special category biometric data *if* used for the purpose of uniquely identifying someone.

24. Effective age assurance requires the processing of age and age ranges

The EDPB indicates (Paragraph 94) that providers of online platforms should not store the age or age range of child users of a service as a result of the age assurance process. Instead, the EDPB indicates that providers should merely record whether the recipient fulfills the relevant service conditions of the user. This is impractical and undermines the critical goal of protecting children.

Google encourages the EDPB to consider the ramifications of such a restrictive approach. For example, not only on user experience, but the service provider's ability to ensure age-appropriate settings and to discharge obligations under other legal regimes (where a specific age is required, and where accountability is necessary).

Google consistently invests in research, policies, and practices to offer age-appropriate ways for children to explore, learn, and participate in the online world as they grow. As part of our efforts, we support flexible and smart regulation that respects users' rights to privacy, to access and seek information, and freedom of expression, and which can adapt over time as

[23] This has been recognised by international data protection regulators, including the UK Information Commissioner's Office.

technology evolves.[24] It is vital that children are adequately and appropriately protected, without curtailing their opportunities for growth, self-expression, and digital development.

As part of these measures to ensure age appropriate experiences, it is important to apply the *right* settings for the *right* age range. This approach is supported by the European Commission's recent Guidelines on measures to ensure a high level of privacy, safety and security for minors online.[25] For example, younger children may need different settings to older teens, as appropriate. To achieve this effectively and in accordance with user expectations, it may be necessary and proportionate to have a record of the relevant age or age range (as obtained via age assurance).

This avoids the application of excessive age assurance (that would be unnecessarily disruptive to service use and involve repeated processing). Service providers can then prompt users to conduct further age assurance measures when appropriate and proportionate. For example, when the user (based on their relevant age or age range) exceeds the relevant age of consent, or likely transitions to a different age range where different settings are more appropriate.

We also urge the EDPB to recognise that it may be necessary for providers subject to the DSA to share information on users' ages with third-parties as a proportionate risk mitigant across the connected online ecosystem (for example, sharing signals that indicate membership of a specific age category between app stores and app developers). The EDPB should acknowledge the developing global standards concerning age signals and that the sharing of age information can be necessary to protect children from age-inappropriate content in accordance with GDPR principles (such as data minimisation and purpose limitation). It is critical that the Guidelines do not inadvertently restrict or discourage such safeguards.

---

[24] We have led the industry by building and supporting the expansion of products like YouTube Kids - released in 2015 and used by families to access diverse, high-quality, playful and educational content from around the world - and Family Link - a parental controls app that allows parents to manage their child's privacy settings, among other things. We have invested heavily in programs like: Designed for Families in the Play Store which helps ensure families have access to high-quality apps that protect children's privacy; Search privacy and safety controls, which help users control their online footprint and blur unwanted explicit content; and School Time, which gives parents control over how and when their teens use Android devices. We also provide resources and guidelines for creators and developers, including programs that provide guidance on how to create great content for families.

[25] European Commission, Guidelines on measures to ensure a high level of privacy, safety and security for minors online, pursuant to Article 28(4) of Regulation (EU) 2022/2065 (C/2025/5519), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202505519, "*Age-appropriate design: providers of online platforms accessible to minors should design their services to align with the developmental, cognitive and emotional needs of minors, while ensuring their safety, privacy, and security. Age-appropriate designs are suitable for children considering their rights and well-being as well as their diversity and specific age or stage of development and take account of the evolving capacities of children*"(emphasis added).

Restrictions on retaining the user's age or age range received via age assurance would unnecessarily limit providers' efforts to discharge their ongoing and continuous obligations under Article 28(1) DSA and to ensure a high level of privacy, safety, and security in a manner that is appropriate to their age or age range.

In its current form, the Guidance could therefore lead to the wrong incentive - in particular, to discourage providers from understanding their users' ages and, in response, disincentivizing the application of age-appropriate protections. This is directly opposed to the DSA's objectives, the growing global regulatory consensus, and users' expectations (and where those users are children, parents' expectations). Understanding and storing a child's age helps ensure an age-appropriate environment.

Governance and enforcement

25. Greater certainty is needed on regulatory engagement and cooperation

The EDPB appears to encourage the establishment of regulatory cooperation mechanisms to ensure appropriate consultation on DSA and GDPR (such as in the context of enforcement). In particular, the EDPB notes the need for greater cooperation between the EDPB and EBDS and between digital services coordinators (**DSCs**) and data protection supervisory authorities.

Google welcomes this recognition. Considering the DSA-GDPR overlap, effective cooperation and consultation mechanisms between relevant competent authorities (including the Commission) are essential for ensuring regulatory consistency and coherence in interpretation, and providing certainty for intermediary service providers.

Guidance

Google would therefore welcome clarity on whether (and the extent to which) the Guidelines were developed in cooperation with the EBDS. If not, Google urges the EDPB to discuss the Guidelines with the EBDS prior to adoption. This would reflect the commitments made by the EDPB in the Helsinki Statement to prepare joint guidelines with other regulators as appropriate to ensure regulator consistency, and to address legal and practical challenges in cross-regulatory cooperation.

Cooperation

The Guidelines also do not explain how the EDPB and EBDS would cooperate in practice and - notwithstanding the risks of duplication - the EDPB does not seek to propose or commit to formal cooperation mechanisms. There is therefore continued uncertainty in how competent authorities would exercise their respective powers in relation to DSA provisions that affect or involve the processing of personal data, or which relate to the discharge of GDPR obligations in

the context of DSA compliance. Google encourages the EDPB to tackle the lack of consistent or effective cooperation mechanisms to avoid duplication, for example, a commitment from the EDPB to engage and consult with the EBDS.

Regulatory competency

The EDPB recognises that neither GDPR nor DSA provides for specific rules on cooperation between respective competent authorities, and there is no explicit duty of consultation and cooperation on the EBDS or DSCs with data protection supervisory authorities under the DSA (including in the handling of enforcement). The Guidelines therefore indicate the potential for duplication of proceedings in relation to GDPR and DSA obligations, and inconsistencies and risks related to the principle of *ne bis in idem*.

However, the Guidelines do not seek to clarify regulatory competencies in relation to the interplay between the GDPR and DSA. Google encourages the EDPB to set out clearer procedural competencies to ensure that procedural safeguards set out in Union law are respected - such as in relation to data protection governance and enforcement under GDPR.