Prof. Dr. Alexander Peukert, Goethe University

Max-Horkheimer-Str. 2, PF EXC-12, D-60323 Frankfurt/Main

Univ.-Prof. Dr. Alexander Peukert

Chair for Civil Law, Commercial Law and Information Law

Faculty of Law, Institute for International and European Private Lawand Comparative Law

Tel: +49 (0)69 798 31477
a.peukert@jur.uni-frankfurt.de
http://www.jura.uni-frankfurt.de/peukert

Frankfurt/M., 22 February 2024

Response to the Public Consultation: Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes

On 8 February 2024, the European Commission launched a public consultation to seek views on Draft Digital Services Act (DSA) Guidelines (in the following: Draft Guidelines) concerning the integrity of electoral processes. I write as an EU citizen and professor of information law. This response has not been initiated, funded or otherwise influenced by any third party.

Response to Q1:

Yes, there are documents, reports and academic studies that I recommend as further input for the Guidelines.

Firstly, the Guidelines should factor in empirical research that is showing that the scale and impact of foreign information manipulation and interference (FIMI) and online disinformation are limited, and that alarmist narratives about the destructive effects of these phenomena are exaggerated and have a potentially negative impact on citizens' trust in the media and the democratic system:

- Andreas Jungherr and Adrian Rauchfleisch, 'Negative Downstream Effects of Alarmist Disinformation Discourse: Evidence from the United States' (2024) Political Behavior, https://doi.org/10.1007/s11109-024-09911-3
- Andrew Guess, Jonathan Nagler and Joshua A Tucker, 'Less Than You Think: Prevalence and Predictors of Fake News Dissemination on Facebook' (2019) 5 Science Advances 4586
- Andrew M Guess, Brendan Nyhan and Jason Reifler, 'Exposure to Untrustworthy Websites in the 2016 US Election' (2020) 4 Nature Human Behavior 472

- Brendan Nyhan, 'Facts and Myths about Misperceptions' (2020) 34 Journal of Economic Perspectives 220
- Chico Q Camargo and Felix M Simon, 'Mis- and Disinformation Studies Are Too Big to Fail: Six Suggestions for the Field's Future' (2022) 3 Harvard Kennedy School Misinformation Review 1
- Edda Humprecht, Frank Esser and Peter Van Aelst, 'Resilience to Online Disinformation: A Framework for Cross-National Comparative Research' (2020) 25 The International Journal of Press/Politics 493
- Emily Van Duyn and Jessica Collier, 'Priming and Fake News: The Effects of Elite Discourse on Evaluations of News Media' (2019) 22 Mass Communication and Society 29
- Felix M Simon and Chico Q Camargo, 'Autopsy of a Metaphor: The Origins, Use and Blind Spots of the "Infodemic"' (2023) 25 New Media & Society 2219
- Felix M Simon, Sacha Altay and Hugo Mercier, 'Misinformation Reloaded? Fears about the Impact of Generative AI on Misinformation Are Overblown' (2023) 4 Harvard Kennedy School Misinformation Review 1
- Jennifer Allen and others, 'Evaluating the Fake News Problem at the Scale of the Information Ecosystem' (2020) 6 Science Advances 3539
- Mathias Osmundsen and others, 'Partisan Polarization Is the Primary Psychological Motivation Behind "Fake News" Sharing on Twitter' (2021) 115 American Political Science Review 999
- Melanie Freeze and others, 'Fake Claims of Fake News: Political Misinformation, Warnings, and the Tainted Truth Effect' (2021) 43 Political Behavior 1433
- Sacha Altay, Anne-Sophie Hacquin and Hugo Mercier, 'Why Do so Few People Share Fake News? It Hurts Their Reputation' (2022) 24 New Media & Society 1303
- Sacha Altay, Manon Berriche and Alberto Acerbi, 'Misinformation on Misinformation: Conceptual and Methodological Challenges' (2023) 9 Social Media + Society 1

Secondly, the Guidelines should factor in evidence from the U.S. about efforts of U.S. public authorities to informally influence the moderation practices of social media companies concerning speech protected by the 1st amendment.

- Court documents in the pending case *Vivek H. Murthy, Surgeon General, et al. v. Missouri*, et al., Supreme Court of the United States, Docket no. 23-411
- Michael Shellenberger, 'The Censorship-Industrial Complex', 2023, https://judiciary.house.gov/sites/evo-subsites/republicans-judiciary.house.gov/files/evo-media-document/shellenberger-testimony.pdf

Response to Q2:

The Commission can further clarify the purpose and scope of the Guidelines to better address systemic risks for electoral processes in three ways: It should define core concepts (1), address the reasonableness and proportionality of specific mitigation measures (2) and improve the fundamental rights analysis (3).

1. Clarity

According to Art. 35(3) DSA, the Commission may issue guidelines on the application of paragraph one of this article "in relation to *specific* risks". Art. 35(1) DSA establishes an obligation to put in place mitigation measures "*tailored* to the *specific* risks identified pursuant to Article 34". The legal basis for the Guidelines thus demands that the best practices and recommendations are specifically tailored to the mitigation of one or several systemic risks. At first sight, the Draft Guidelines comply

with this specificity requirement by addressing only one of the systemic risks listed in Art. 34(1) DSA, namely "any actual or foreseeable negative effects on … electoral processes" (lit. c, 2nd alternative).

However, this limited scope and purpose of the Guidelines should be spelt out more clearly. To this end, paragraph 1 should not refer to the separate risk category for "civic discourse". Instead, it should be expressly stated that the Guidelines are not concerned with the other two systemic risks (for civic discourse and public security) mentioned in Art. 34(1)(c) DSA. The systemic risk of a "dissemination of illegal content" (Art. 34(1)(a) DSA) should be clearly distinguished too. Art. 34(1)(a) DSA covers any kind of illegal content, including information that is declared illegal because it threatens the integrity of elections. On the one hand, the Draft Guidelines do not address this "specific" risk. On the other hand, the Draft mentions "illegal hate speech" (para 3), "illegal content" (para 22) and the misuse of a generative AI system "for illegal … purposes" (para 27(f)). Either the scope of the Guidelines is expressly extended to cover election-related illegal content or the aforementioned references to illegal content have to be deleted. In the course of this clarification, it should also be stressed that Art. 34(1)(c) DSA and the Guidelines address risks associated with *per se lawful content*, i.e. information that is in conformity with the laws of the Union and of the Member States (see infra 3).

In addition, the Guidelines should positively define the object of protection of mitigation measures, i.e. "electoral processes". While guidelines based on Art. 35(3) DSA only address risk mitigation measures, these measures are nevertheless a response to a problem, namely a systemic risk pursuant to Art. 34 DSA. This is why the basic risk mitigation obligation under Art. 35(1) DSA expressly refers to "specific systemic risks identified pursuant to Article 34" DSA. There is thus a clear statutory link between the legal basis of the Guidelines and the closed list of systemic risks. Absent a clear definition of the "specific" systemic risk to be mitigated, the Guidelines cannot set out "tailored" measures. At the same time, a vague and broad wording of the Guidelines could provoke content moderation measures that go beyond risks for electoral processes. This danger is exacerbated by the incoherent wording of the Guidelines (cf. "specific risks linked to electoral processes" (para 3); "risks related to electoral processes" (para 8); measures "of application to electoral processes in general" (para 10); "systemic risks in electoral processes" (Q2); "in the context of electoral processes" (para 27(f)) and the striking lack of examples for election-related FIMI and disinformation incidents.

In order to clarify the scope of the Guidelines, the final text should refer to and incorporate the wording of Commission Recommendation (EU) 2023/2829 of 12 December 2023 on inclusive and resilient electoral processes in the Union and enhancing the European nature and efficient conduct of the elections to the European Parliament. The object of protection could be specified as the promotion of "free, fair and resilient elections in the Union" (recital 4 RECO 2023/2829). As examples of information that is critical for the integrity of elections, the Guidelines could refer to information on basic rules and practical arrangements related to the exercise of electoral rights (recital 12 RECO 2023/2829), information campaigns of Member States supporting the election participation of specific groups of society (recital 18 RECO 2023/2829), youth-friendly communication campaigns and election guides (recital 19 RECO 2023/2829), information about organisations linked to European and national political parties (recital 25 RECO 2023/2829), information about political advertising (recital 26 RECO 2023/2829), transparency requirements regarding donations from third countries (recital 46 RECO 2023/2829), information on the opening hours of polling stations (recital 54 RECO 2023/2829), information on citizenship rights and electoral procedures (recital 55 RECO 2023/2829) and rules and sanctions related to multiple voting (recital 59 RECO 2023/2829).

The Draft Guidelines are also insufficiently clear about their temporal applicability, which should be spelled out in a separate paragraph. Section 3.5 makes recommendations for the time "during" an electoral period, and Section 3.6 for the time "after" an electoral period. This structure implies that the bulk of the recommendations (Sections 3.1-3.4) concern an unspecified timeframe "before" an election (see also para 6(c): "before or after an electoral event", para 33: "efficient exchange of information before, during and after the election"). Paragraph 37 suggests that "measures are already in place and functioning one to six months before an electoral period, and continue at least one month after the elections, depending on the risk assessment for the particular election". As there is effectively a continuum of elections on the local, regional and federal level in the Member States, Sections 3.1-3.4 describe a structure of permanent mitigation measures, for example in the form of internal teams and relationships with private actors (para 10 and infra, response to Q3). Such a permanent structure lends itself to measures against content that is unrelated to "electoral processes". In a democracy, any content capable of contributing to a debate of public interest, any expression of a political nature, can reasonably be considered to be election-related, simply because public discourse is the only legitimate forum to win votes and eventually political power. However, with their focus on the specific risk to "electoral processes", the Guidelines are neither intended nor suitable for a permanent moderation of any kind of general interest speech. Accordingly, recommendations insufficiently related to "electoral processes" should be deleted. This concerns, in particular, the recommendation to promote the availability of "trustworthy information from pluralistic sources" also outside of "election times" (para 24) and the recommendation to develop and apply "inoculation measures that pre-emptively build psychological resistance to possible and expected disinformation narratives" (para 16(b)(ii)).

Another reason why the scope of application of the Draft Guidelines is unclear is that they do not define two of their core targets, namely "foreign information manipulation and interference (FIMI)" and "disinformation" (see, e.g., paras 5 and 13). This lack of definitions is problematic for three reasons. Firstly, the terminology of the Draft Guidelines is incompatible with other relevant EU documents. While the Draft treats FIMI and disinformation as two separate issues, other Commission documents and the Code of Practice on Disinformation work with a broad notion of disinformation that functions as an umbrella term also covering "foreign interference in the information space" (cf. Peukert, The Regulation of Disinformation in the EU – Overview and Open Questions (June 30, 2023), http://dx.doi.org/10.2139/ssrn.4496691). Secondly, the concepts of FIMI and disinformation are again insufficiently related to electoral processes (see, in particular, para 16(g): "FIMI and disinformation *around* the elections"). The EEAS Report on FIMI Threats (citied in fn. 5) defines FIMI as "a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes." The term disinformation is equally vague and is used for all sorts of false or misleading content. To remedy these flaws, the Guidelines should give concrete examples for foreign or local manipulations of electoral processes. Thirdly, the focus on FIMI and disinformation tends to neglect the fact that VLOP and VLOSE providers only need to mitigate systemic risks "stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services" (Art. 34(1) DSA). In other words, VLOP and VLOSE providers cannot be held responsible for the fact that foreign or EU actors provide harmful information in the first place (cf. Art. 3(k) DSA). They only have to ensure that their services do not facilitate the dissemination and findability of this third party information. This fundamental limitation of the DSA obligations should be made more explicit (cf. paragraphs 7 and 53).

In summary, the clarity of the Guidelines should be improved by defining, with examples, (1) the object of protection (electoral processes), (2) the systemic risks for electoral processes stemming

from the design, functioning or use of VLOP and VLOSE services, and (3) the measures recommended to mitigate these specific risks before, during and after an election.

2. Reasonableness and proportionality

VLOP and VLOSE providers have to put in place "reasonable, proportionate and effective" mitigation measures (Art. 35(1) DSA). The Draft Guidelines repeat these general requirements several times (paras 1, 7, 26 and 48). However, only one recommendation specifically calls for a consideration of the proportionality of a measure in light of the risk profile identified for the election in question (para 13 on the allocation of resources for an election integrity team). Apart from this example, the Draft Guidelines do not set out criteria on how to operationalise the proportionality principle in practice.

To improve the Guidelines in this respect, it is firstly necessary to define what constitutes a "systemic" risk to electoral processes. In contrast to other EU legal acts, the DSA does not operate with a risk hierarchy of acceptable, low, medium and serious/high risk, but with one single risk category, which has to be met in order to trigger risk mitigation duties. Applied to the context at hand, this means that a VLOP or VLOSE service has to pose a systemic risk for the integrity of electoral processes in the EU. If there is no systemic risk in the first place, no mitigation measures are justified. Chapter III Section 5 DSA aims to mitigate negative societal impacts (= societal risks) of VLOPs and VLOSEs. While the integrity of elections is, by its very nature, a societal concern, VLOPs and VLOSEs only pose a systemic risk to free and fair electoral processes if their services adversely affect such a process *as a whole*. Individual social media posts containing false information or an attempted FIMI campaign that does not go viral do not pose a systemic risk in this sense. In contrast to what the Draft Guidelines claim in paragraph 3 ("heightened risks to election integrity"), experience shows that most online manipulations remain below the threshold of systemic risk for electoral processes. The Commission report on the 2019 elections to the European Parliament (COM/2020/252 final) concluded that "no large-scale covert interference operation in the 2019 elections has been identified". The study cited in footnote 15 of the Draft Guidelines notes "that the phenomenon of echo chambers on social media may not be as widespread as was once believed" (p. 20). And the EEAS Report on FIMI Threats cited in footnote 5 observes that AI "is not (yet) the biggest threat" (p. 11) and advises against directly confronting any kind of manipulated information because doing so could inadvertently increase the damage (p. 17). The scientific literature on the phenomenon of disinformation/fake news also cautions against unfounded alarmism (see supra, response to Q1).

Consequently, the Guidelines should recommend escalating mitigation measures. The basic level of mitigation should be limited to the identification of systemic risks for electoral processes (Section 3.1) and the availability of transparency measures such as labels. Content moderation measures should only be applied once a FIMI/disinformation campaign has been identified that has the potential to negatively affect a concrete electoral process as a whole, because it can reasonably be expected to go viral in the relevant community. These content moderation measures should again be escalating in the sense that the intensity of the interference has to correspond to the spread and thus risk of a FIMI/disinformation campaign. Purely informational interventions such as prompts and notes should take precedence over more intrusive measures such as circuit breakers and demonetization. Removing content should always be a last resort.

3. Fundamental rights analysis

The need for a graduated response to FIMI/disinformation threats to election integrity also follows from Art. 35(3) 1st sentence DSA, which requires the Guidelines to have "due regard to the possible consequences of the measures on fundamental rights enshrined in the Charter of all parties

involved". In this respect, too, the Draft Guidelines fall short. The references to fundamental rights do not go much beyond a repetition of the statutory language (cf. paras 2, 21, 29).

To remedy this flaw, the Guidelines should firstly specify the fundamental rights of the relevant parties, i.e. VLOP and VLOSE providers, content providers and other recipients of VLOP/VLOSE services. Secondly, the Guidelines should clarify whether and in how far the Guidelines recommend measures against the dissemination of content that is not illegal in the sense of Art. 3(h), 34(1)(a) DSA because it is in conformity with the laws of the Union and the Member States. Indeed, the definitions of FIMI in the EEAS Report on FIMI Threats (footnote 5) and of disinformation in the Code of Conduct and other Commission documents (cf. Peukert, op. cit.) suggest that the bulk of election-related content targeted by the Guidelines is lawful. It should be noted that it is highly questionable whether the Commission is entitled to "strongly encourage" (para 53) VLOPs and VLOSEs to take action against lawful speech (cf. Peukert, op. cit.; see also infra, response to Question 12). Thirdly, the Draft Guidelines should recommend measures against the real risk that VLOPs and VLOSEs themselves manipulate electoral processes through biased ranking and other forms of preferential algorithmic treatment of their favoured contenders (see the study cited in footnote 15, p. 36). Transparency measures to ensure that content moderation decisions by VLOPs and VLOSEs do not affect equal chances of candidates (para 20) should be established. In addition, the last half sentence of paragraph 20 should be deleted. VLOP and VLOSE providers are not only barred from "disproportionately" favouring or promoting voices representing certain ("polarised" (?)) views. Any deliberate promotion of political parties, candidates or campaigns by VLOPs and VLOSEs violates the equal right of every citizen to vote and to stand as a candidate in elections (for the EU level cf. Art. 39 CFEU, Art. 10(3) TEU) and the equal right of political parties to contribute to the expression of the political will of the citizens (for the EU level cf. Art. 12(2) CFEU).

Response to Q3:

No, I disagree with the recommended best practices set out in Sections 3.1 and 3.2 because the Commission thereby "strongly encourages" the creation of a public-private *Kommunikationsüberwachungsbürokratie* (communications surveillance bureaucracy) that is not accountable to EU citizens and political parties and whose informal operations are not transparent.

Throughout Sections 3.1 and 3.2, the Draft Guidelines urge VLOPs and VLOSEs to continuously engage with "independent civil society organisations, researchers and fact-checkers" (para 12), unspecified "external experts" (para 13), "election related initiatives and campaigns" (para 16(b)) and "other relevant stakeholders" (para 18). Despite the important role of these private DSA actors, the Guidelines do not recommend any specific measure to make the multi-stakeholder cooperation transparent to the European public. Paragraph 20 is too vague and limited ("as far as possible") to accomplish this task. Paragraph 23 even undermines transparency by giving unspecified "civil society organisations" priority access to fundamental rights impact assessments of VLOPs and VLOSEs before the reports have to be made available to the public.

The secrecy of the cooperation between VLOP/VLOSE providers and private DSA actors runs contrary to the overall aim of the DSA to establish a safe, predictable and trusted online environment (Art. 1(1) DSA). The highly sensitive, election-related content moderation of VLOPs/VLOSEs will not be trusted by EU citizens if it is not known who is influencing these decisions. Private DSA actors who are involved in the election-related risk management of VLOPs/VLOSEs in relation to mostly *lawful* speech should at least be subject to the rules set out in Article 22 DSA for "trusted flaggers" notifying *illegal* content. Indeed, the moderation (and suppression) of lawful speech should be subject to stricter requirements and more transparency than the enforcement of existing content rules against illegal information. Consequently, the Guidelines should recommend

that VLOPs/VLOSEs may only cooperate with actors that meet the requirements of Art. 22(2) DSA. In addition, VLOPs and VLOSEs should make the names, contact details, corporate structure and funding sources of private cooperation partners publicly available in an up-to-date database (cf. Art. 22(5) DSA). The Guidelines should also call for a cessation of cooperation with actors who feed insufficiently precise, inaccurate or inadequately substantiated information into the election-related content moderation system (cf. Art. 22(6) DSA).

Art. 22(2) DSA does not explicitly require trusted flaggers to be independent of EU or national public authorities. Given the sensitivity of moderating lawful, election-related speech, the Guidelines should recommend that actors engaging with VLOPs/VLOSEs must be functionally independent of any public body, including the European Commission (cf. Art. 30(1) Audiovisual Media Services Directive 2010/13, as amended; see Schultz, Errichtung einer Europäischen Medienbehörde, Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2024, 53). Such independence not only implies that VLOP/VLOSE cooperation partners are legally distinct from any government, but also that their operations are not significantly dependent on public funding. As a rule, private DSA actors should not receive more than one third of their annual funding from public sources. At present, many formally private DSA actors do not fall into this category, but depend entirely or predominantly on public funding. This concerns, for example, the European Digital Media Observatory (EDMO) or the European Partnership for Democracy (cf. para 15).

Another requirement that "trusted flaggers" of illegal content have to meet is that they are established in a Member State (cf. Art. 22(2) DSA). Again, the Draft Guidelines do not recommend that VLOP and VLOSE providers only cooperate with private actors established in the EU. On the contrary, many of the organisations referred to in the Draft Guidelines are based in third countries, mainly in the U.S. This concerns, for example, "Accountable Tech" (fn. 13), the "Integrity Institute" (fn. 14) and the most important source raters (cf. para 16(c)(v) and Peukert, Who Decides What Counts as Disinformation in the EU?, 2023/10/24, DOI: 10.59704/c9cff90c698992fa). The Draft Guidelines confirm the important role, if not the dominance, of U.S. actors in the implementation of the DSA by emphasising the ongoing transatlantic cooperation through the EU-US Trade and Technology Council (para 5).

This strong role of U.S.-based actors is incompatible with the aim to minimise the risk of interference in European elections from third countries as set out in recommendation no. 28 of RECO 2023/2829 on inclusive and resilient electoral processes in the Union. According to recital 46 RECO 2023/2829, "donations from third countries to national political parties, political foundations, political candidates and campaign organisations, especially when left unchecked, could unduly influence democratic processes in the Union and be a vector of interference by third countries". Such donations "should therefore be limited or prohibited and in any case be subject to transparency requirements" (ibid). The standards for donations from third countries to political actors should apply all the more to private DSA risk management actors who are able to influence the digital public sphere in the EU in opaque ways. Giving a key role in moderating the European digital public sphere to third country actors, e.g. source raters such as NewsGuard, also contradicts the aim of the DSA to provide VLOP/VLOSE recipients in the Union with an online environment that effectively protects the fundamental rights enshrined in the Charter and is fully compliant with EU and Member State laws (cf. recitals 1 and 3 and Art. 2(1) DSA). It is indeed strange that the DSA imposes far-reaching obligations on U.S.-based VLOPs and VLOSEs to protect the EU's digital sovereignty, while at the same time a Guideline under this act gives a free pass to U.S. (and Chinese) Big Tech companies to cooperate with U.S. actors, who are often closely linked to U.S. government agencies (cf. Peukert, Who Decides What Counts as Disinformation in the EU?, 2023/10/24, DOI:

10.59704/c9cff90c698992fa), in the development and implementation of risk mitigation measures of utmost importance to European democracies.

Finally, paragraph 16(h)(ii), which recommends "cooperation between the relevant teams of different providers of VLOPs and VLOSEs to identify common threats and to counter cross-platform influence operations and migration of malicious actors", should be either deleted or limited to an ad-hoc information exchange in the face of a concrete FIMI/disinformation campaign. Permanent cooperation between providers of very large online platforms/search engines in the economically important and sensitive area of content moderation risks distorting competition on the markets for online platforms and search engines in violation of Art. 101 TFEU. It also increases the risk of a widespread distortion of equal active and passive voting rights and equal chances of political parties through disproportionate promotion of a particular candidate or campaign across very large services (see supra, response to Q1).

Response to Q7

No, I am not in agreement with the best practice recommendations for generative AI for two reasons.

Firstly, and contrary to what is claimed in paragraph 26, article 35(1) DSA does not establish a risk mitigation obligation regarding the "*creation* of generative AI content". Chapter III Section 5 DSA only applies to online platforms and search engines as defined in Art. 3(h) and (j) DSA. An online platform may store and disseminate AI generated content at the request of a recipient of the service, but it is not the functionality of an online platform to generate such content in the first place. For example, the "My AI" chatbot available on Snapchat is not a service covered by the DSA. The same is true when a search engine returns AI generated content as a result of a search query, because that content was available on an indexed website. If, in contrast, a so-called "conversational search engine" uses natural language predictive text to answer queries, it does not qualify as a search engine within the meaning of Art. 3(j) DSA, because it does not "*return* … results in any format in which information related to the requested content can be found". Finding existing data is not the same as creating new data. Art. 3(j) DSA targets conventional search engines like Google Search and Bing, but not so-called chatbot services like the Microsoft Copilot or Google Gemini – a type of service that triggered regulatory responses only after the adoption of the DSA. The appropriate legal basis for addressing the risks associated with the creation of generative AI content is the forthcoming AI Act, in particular the provisions on transparency obligations for AI systems that interact directly with natural persons and additional obligations for providers of general purpose AI models and systems. By including the creation of generative AI content, the Draft Guidelines confuse the scope of application of the DSA with that of the AI Act, thereby creating legal uncertainty. As a result, the Guidelines should clarify that they only regulate risks related to the dissemination, but not the creation, of generative AI content.

Secondly, the recommendation to cooperate with fact checkers (para 28(a)(ii)), should be made subject to the requirements and limitations set out in my response to Q3 (trustworthiness checks, transparency, state independence, no third country actors).

Response to Q12

No, I disagree with the recommended best practices in section 3.4 for three reasons.

Firstly, the recommendation to cooperate with private actors such as "independent experts and civil society organisations" should be made subject to the requirements and limitations set out in my response to Q3 (trustworthiness checks, transparency, state independence, no third country

actors). Contrary to what paragraph 36 seems to suggest, there should be no cooperation with "campaign organisations" that are actively involved in a forthcoming election.

Secondly, it is noteworthy (and questionable) that Section 3.4 seems to rule out that user-based solutions internal to a platform or search engine, such as the Community Note system of X, can ever constitute a sufficient risk management measure pursuant to Art. 35 DSA. If this is the Commission's view, it should be articulated.

Thirdly, all recommendations to cooperate with "responsible national authorities" should be deleted (paras 31, 33, 34). As explained in my response to Q1, the Guidelines also recommend measures against content that is in compliance with EU and Member State laws. Footnote 29 rightly stresses that orders of national judicial or administrative authorities to act against *illegal* content are subject to strict requirements set out in article 9 (not: 10) DSA. It follows, *e contrario*, that the DSA does not provide a legal basis for orders by national authorities to take action against *lawful* content, even if such content poses a systemic risk to electoral processes. If, in the context of the cooperation recommended in paragraph 34, public authorities flag lawful content and request a VLOP or VLOSE provider to take a content moderation measure that negatively affects the availability, visibility or accessibility of that content (cf. Art. 3(t) DSA), this interference may arguably be attributed to that public authority. As this interference with freedom of expression is not prescribed by law, it would be unconstitutional (cf. Peukert, The Regulation of Disinformation in the EU – Overview and Open Questions (June 30, 2023), http://dx.doi.org/10.2139/ssrn.4496691). Finally, the recommendation to communicate informally with national authorities conflicts with the exclusive powers of the Commission to supervise and enforce the risk management obligation of Art. 35 DSA (Art. 56(2) DSA).

Response Q22

The recommendation in paragraph 50 to establish contacts with European political parties, who are directly affected by election-related content moderation, should be deleted. If at all, these contacts should only take place on an ad hoc basis in the context of a specific FIMI/disinformation campaign and should be conducted on a strictly egalitarian basis. This means that all European political parties must be invited and granted access to communication exchanges on equal terms.

Response Q24

The Draft Guidelines, including paragraph 2 on Art. 35(3) DSA as the legal basis for the Guidelines, do not mention the fact that Art. 35(3) empowers the Commission to issue guidelines "in cooperation with the Digital Service Coordinators" (DSCs). This gap may be due to the fact that several Member States, including Germany, have not yet designated their DSCs. It is true that this failure of Member States complicates the monitoring and enforcement of the DSA (cf. recital 7 Commission Recommendation of 20.10.2023 on coordinating responses to incidents in particular arising from the dissemination of illegal content, ahead of the full entry into application of Regulation (EU) 2022/2065 (C(2023)7170)). However, these difficulties do not justify setting aside a DSA provision requiring cooperation with national DSCs.

In my view, Art. 35(3) DSA presupposes that the Commission first consults *all* DSCs of *all* Member States and incorporates their viewpoints in the final Guidelines. This follows from the wording of Art. 35(3) 1st sentence DSA when compared to other provisions on Commission guidelines (Arts. 22(8), 25(3), 28(4), 39(3) DSA). In contrast to Arts. 22(8), 28(4) and 39(3) DSA, the Commission need not consult the European Board for Digital Services, which can perform its tasks also if one or more Member States have not designated a DSC (Art. 62(1) DSA), and which adopts its acts by simple majority of votes (Art. 62(3) DSA). Instead, Art. 35(3) DSA requires that the Commission has to

cooperate with "*the* Digital Service Coordinator*s*", that is the plurality of all DSCs representing all Member States. Such a strict interpretation of Art. 35(3) DSA reflects the exceptional importance and sensitivity of the subject matter of Art. 35 Guidelines. While the mitigation of systemic risks for electoral processes touches on the very fabric of the European digital public sphere and the national and EU democratic systems, the issues addressed in Arts. 22, 28 and 39 DSA are of a much more limited nature. They therefore do not presuppose the involvement of all Member States. In contrast, a "whole-of-society" approach to mitigating systemic risks to election integrity in the EU implies that *all* Member States, represented by their DSCs, actively contribute to and support measures that regulate electoral processes taking place on their territory.

End of document.