EUROPEAN
COMMISSION

Brussels, XXX
[…](2024) XXX draft

ANNEX

SENSITIVE[*]
UNTIL ADOPTION

ANNEX

to the

Communication to the Commission

On the approval of the content of draft guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065

[*] Distribution only on a 'Need to know' basis - Do not read or carry openly in public places. Must be stored securely and encrypted in storage and transmission. Destroy copies by shredding or secure deletion. Full handling instructions https://europa.eu/!db43PX

ANNEX

to the

Communication to the Commission

On the approval of the content of draft guidelines for providers of Very Large Online Platforms and Very Large Online Search Engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065

1. INTRODUCTION

1.1. Purpose and Legal Basis

(1) Online platforms and search engines have become important venues for public debate and for shaping public opinion and voter behaviour. Regulation (EU) 2022/2065 ("Digital Services Act") imposes obligations on providers of very large online platforms (VLOPs) and very large online search engines (VLOSEs) ([1]) to carry out specific risk assessments and put in place reasonable, proportionate and effective risk mitigation measures including for "any actual or foreseeable negative effects on civic discourse and electoral processes" ([2]).

(2) Pursuant to Article 35(3) of Regulation (EU) 2022/2065, the Commission may issue guidelines on the risk mitigation measures providers of VLOPs and VLOSEs are required to adopt in relation to specific risks. Such guidelines may, in particular, present best practices and recommend possible measures, having due regard to the possible consequences of the measures on the fundamental rights enshrined in the Charter of Fundamental Rights of the European Union (the 'Charter') of all parties involved.

(3) A wide range of phenomena involving online platforms and search engines give rise to a heightened risk to election integrity. These include, but are not limited to the proliferation of illegal hate speech online, threats linked to foreign information manipulation and interference ("FIMI") as well as the wider phenomenon of disinformation, the spread of (violent) extremist content and such with the intent to radicalise people, as well as the spread of content generated through new technologies such as generative Artificial Intelligence ("AI") ([3]). In view of several elections planned in the EU in the months to come, including the upcoming 2024 elections to the European Parliament, this document contains guidance aimed at supporting providers of VLOPs and VLOSEs to ensure that, where appropriate, they comply with their obligation to mitigate specific risks linked to electoral

([1]) Pursuant to Article 33 of the DSA, these are providers designated by the Commission as having a number of average monthly active recipients of their service in the European Union (EU) equal to or higher than 45 million.

([2]) Article 34(1)(c) of the DSA.

([3]) Artificial intelligence capable of generating text, images, or other media, using generative models.

processes. This guidance remains generally relevant even after those elections have taken place.

(4) Measures taken by VLOPs and VLOSEs in line with Regulation (EU) 2022/2065, including all measures to mitigate negative effects on electoral processes mentioned in these guidelines, should be taken with particular consideration for the protection of fundamental rights enshrined in the Charter, including the right to human dignity, respect for private and family life, the protection of personal data, freedom of expression and information, including freedom and pluralism of the media, freedom of association and freedom to conduct a business. Providers of VLOPs and VLOSEs should pay due regard to the potential impact of the measures on the fundamental rights of all parties involved, including vulnerable groups considering accessibility and inclusiveness of the measures.

(5) These guidelines already account for forthcoming obligations imposed on providers of VLOPs and VLOSEs by the Regulation (EU) 2024/900 on the transparency and targeting of political advertising ("Regulation on Political Advertising")([4]), as well as the forthcoming Regulation laying down harmonised rules on Artificial Intelligence ("AI Act")([5]), both of which are in the process of adoption by the EU legislator, as well as the voluntary commitments undertaken by providers of VLOPs and VLOSEs under the AI Pact to adhere to the obligations laid down in the AI Act prior to its entry into application ([6]). Providers of VLOPs and VLOSEs shall be bound to comply with such legally binding rules when they enter into application, to the extent applicable to them.

(6) Providers of VLOPs and VLOSEs shall comply with their obligations under Regulation (EU) 2022/2065. These guidelines should be seen in the framework of supporting providers of VLOPs and VLOSEs to ensure compliance with the obligation under Article 35 of that Regulation vis-à-vis risks on electoral processes. In addition to the obligation to put in place reasonable, proportionate, and effective mitigation measures for risks related to electoral processes pursuant to Article 35 of Regulation (EU) 2022/2065, providers of VLOPs and VLOSEs must follow all other legal obligations in Regulation (EU) 2022/2065 which may be relevant for elections. These include, but are not limited to, Articles 14 and, 17 on Terms and Conditions and Statement of Reasons, Articles 27 and 38 on Recommender Systems, Articles 36 and 48 on Crisis Response Mechanisms and Protocols, Articles 15, 24, 37, 42 on Transparency and Independent Audits, Articles 26 and 39 on Online Advertising Transparency and Article 40 on Data Access and Scrutiny.

(7) Systemic risks for electoral processes can also manifest themselves through the amplification and potentially rapid and wide dissemination of content that is illegal under European or Member State laws, for example, threats, violent extremist and terrorist content, illegal hate speech or online harassment against political candidates or office holders, journalists, election workers or others involved in the electoral process. As such Articles 9, 10, 16, 22 of Regulation (EU) 2022/2065 on Illegal Content, covering orders to act against illegal content and to provide

([4]) EU introduces new rules on transparency and targeting of political advertising - Consilium (europa.eu)

([5]) https://digital-strategy.ec.europa.eu/en/news/commission-welcomes-political-agreement-artificial-intelligence-act

([6]) https://digital-strategy.ec.europa.eu/en/policies/ai-pact

information, as well as Notice and Action Mechanisms and the provision on Trusted Flaggers, are of particular note.

1.2. Input for guidelines and related policy initiatives

(8) These guidelines build upon a series of readiness dialogues on election integrity carried out by the Commission with several providers of VLOPs and VLOSEs after Regulation (EU) 2022/2065 entered into application for the first 19 designated services at the end of August 2023 ([7]), in cooperation with relevant national authorities. For the preparation of the final version of these guidelines, the Commission organised an exploratory consultation ([8]), which was published on 8 February 2024 and closed on 7 March 2024, as well as targeted consultations in the form of round table exchanges, including with Civil Society organisations and providers of VLOPs and VLOSEs on a draft version of the guidelines. In addition, in finalising the guidelines, the Commission cooperated with the Digital Services Coordinators through meetings of the European Board for Digital Services.

(9) To the extent relevant for compliance of VLOPs and VLOSEs with Regulation (EU) 2022/2065, the guidelines also reflect several commitments and measures to reduce the spread of online disinformation contained in the Code of Practice on Disinformation ([9]), the first worldwide industry-led framework in the digital field and a source of industry best practices to address disinformation. They also take into account the work done by the EU's institutions and the Member States on foreign information manipulation and interference ("FIMI"), notably the comprehensive framework provided by the EU FIMI Toolbox and the recent European External Action Service (EEAS) Report on FIMI Threats ([10]) focusing on responses to FIMI in the context of elections.

(10) These guidelines complement the Commission's policies in the field of democracy and free, fair and resilient elections, including the 2020 European democracy action plan ([11]), the elections and integrity package presented by the Commission in 2021 ([12]) and recently the 2023 Defence of Democracy package ([13]), and the work of the European Cooperation Network on elections ([14]) to foster cooperation

([7]) The Commission organised ad-hoc meetings with providers of VLOPs and VLOSEs, both in bilateral settings, as well as in the presence of national authorities, where elections were taking place to gather information on existing practices and ad-hoc policies in place to address elections-related risks.

([8]) There were 77 replies to the consultation, for a summary see: Public consultation on draft guidelines for Providers of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) on the Mitigation of Systemic Risks for Electoral Processes: A summary and analysis of responses.

([9]) https://disinfocode.eu/introduction-to-the-code/

([10]) https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

([11]) https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/new-push-european-democracy/protecting-democracy_en

([12]) https://commission.europa.eu/publications/reinforcing-democracy-and-integrity-elections-all-documents_en

([13]) https://commission.europa.eu/publications/defence-democracy_en

([14]) https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/eu-citizenship-and-democracy/democracy-and-electoral-rights/european-cooperation-network-elections_en

among national electoral networks of competent authorities. The Defence of Democracy package includes, among others, extensive recommendations to Member States, and national and European political parties, political foundations and campaign organisations on inclusive and resilient electoral processes in the EU and enhancing the European nature and efficient conduct of the elections to the European Parliament ([15]). As indicated in these recommendations, the Commission will report on the conduct of the European Parliamentary elections. The Commission's Communication on Defence of Democracy also provides an assessment of risks to electoral processes and the civic discourse from the perspective among others of the implementation of the European Democracy Action Plan and should be taken into account ([16]).

1.3. Outline

(11) The structure of these guidelines is as follows:

a) Section 1 sets out the purpose and legal basis, input and other related policy initiatives, and structure of these guidelines;

b) Section 2 sets out the scope of these guidelines;

c) Section 3 sets out the main substantive guidance on mitigation measures to address systemic risks related to electoral processes. Specific subsections cover reinforcing internal processes; risk mitigation measures for electoral processes; mitigations measures linked to generative AI; cooperation with EU and national authorities, independent experts and civil society organisations; the process of putting into place risk mitigation measures during and after an electoral event; and specific guidance for elections to the European Parliament;

d) Section 4 indicates next steps and conclusions.

2. SCOPE OF THESE GUIDELINES

(12) The guidelines are addressed to providers of VLOPs and VLOSEs whose services bear risks of actual or foreseeable negative effects on electoral processes stemming from the design, functioning, and use of those services within the meaning of Article 34 of Regulation (EU) 2022/2065. Pursuant to Article 35(1) of that regulation, providers of VLOPs and VLOSEs shall put in place reasonable, proportionate, and effective mitigation measures, tailored to the specific systemic risks identified.

(13) Article 35(1) of Regulation (EU) 2022/2065 provides a non-exhaustive list of mitigation measures that providers of VLOPs and VLOSEs may adopt to address the systemic risks they identify in the risk assessment process to which their service and its related systems, including algorithmic systems, give rise, or which arise from the use made of their services. These guidelines further elaborate on that list and set out best practices and recommend risk mitigating measures specifically for risks related to electoral processes.

([15]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023H2829

([16]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0630.

(14) The measures presented in these guidelines are not an exhaustive list of recommendations to providers of VLOPs and VLOSEs in all instances. The appropriate mitigation measures depend on the specific service and the specific systemic risks identified pursuant to Article 34 of Regulation (EU) 2022/2065.

(15) Providers of VLOPs and VLOSEs should apply these guidelines for electoral processes in Member States, including for national elections and for elections to the European Parliament. This should include measures during pre-electoral, electoral, and post-electoral periods ([17]). Mitigation measures should also be applied for regional and local elections or referenda, should risk assessments conclude there are actual or foreseeable negative effects for these electoral processes.

(16) The scope of these guidelines is the application of Article 35(1) of Regulation (EU) 2022/2065. Pursuant to Article 35(2) the Board, in cooperation with the Commission, shall publish comprehensive reports once a year which will include the identification and assessment of the most prominent and recurrent systemic risks reported by providers of VLOPs or VLOPSEs or identified through other information sources.

(17) In line with recital 103 of Regulation (EU) 2022/2065, these guidelines may also serve as a source of inspiration for providers of online platforms or search engines that have not been designated as VLOPs or VLOSEs and whose services give rise to similar risks. It may also serve as a reference for the continuous research into, and analysis of, the effectiveness of risk mitigation measures in response to risks related to electoral processes. Where the mitigation measures and best practices recommended in these guidelines are of application to electoral processes in general, providers of VLOPs and VLOSEs may consider keeping the measures and practices in place where appropriate to protect public debate outside of electoral processes, considering the impact this may have on fundamental rights.

3. ELECTION SPECIFIC RISK MITIGATION MEASURES

3.1. Reinforcing internal processes

(18) To tailor mitigation measures to identified risks to electoral processes, providers of VLOPs and VLOSEs should consider **reinforcing internal processes** in line with Article 35(1)(f) of Regulation (EU) 2022/2065. Mitigation measures should, amongst others, be guided by information on elements such as the presence and activity of political actors on the service, relevant discussions on, and usage of, the platform in the context of elections, the number of users in a Member State when a particular election is called in that Member State, and indications of previous instances concerning tactics, techniques, and procedures for information manipulation.

(19) Internal processes should identify and make available relevant information, analysis, and data to enable the design and calibration of measures to mitigate any actual or foreseeable risks that might stem from information on elections that is searched, shared, or accessed via the service provided by VLOPs and VLOSEs. This could include, but is not limited to, information on political parties or

([17]) The Council of Europe Electoral Cycle - Elections (coe.int)

candidates, party programmes, manifestos or other political material, or related information, to organise events such as demonstrations or rallies, campaigning, fundraising, or other related political activities. Internal processes for collecting and sharing analysis and data informing the design and calibration of risk mitigation measures that providers of VLOPs and VLOSEs put in place shall ensure compliance with relevant data protection legislation ([18]).

(20) Internal processes should be reinforced to ensure that the design and calibration of mitigation measures is appropriate for the specific regional, local, and linguistic context in which they will be employed. Therefore, providers of VLOPs and VLOSEs are encouraged, amongst others, to ensure information and analysis collected on **local context-specific risks and Member State specific information** at the national, regional and/or local level is seamlessly made available to the entities responsible for the design and calibration of risk mitigation measures.

(21) It is also recommended that providers have adequate content moderation resources with local language capacity and knowledge of the national and/or regional contexts and specificities. The Commission also recommends that providers ensure they have adequate internal processes to take into account **independent analyses** of the state of media freedom and pluralism, such as the Media Pluralism Monitor ([19]), knowledge of media literacy initiatives and indicators, and information on the existence of an enabling space for civil society organisations to participate in policy-making and civic discourse. The capacity of all relevant mitigation measures to perform effectively in the local linguistic and electoral context should also be considered.

(22) To reinforce internal processes and resources in a particular electoral context, providers of VLOPs and VLOSEs should consider setting up **a dedicated, clearly identifiable internal team** prior to each individual electoral period (see also section 3.5. 'During an electoral period'). The resource allocation for that team should be proportionate to the risks identified for the election in question, including being staffed by persons with Member State specific expertise, such as local, contextual and language knowledge. The team should cover all relevant expertise including in areas such as content moderation, fact-checking, threat disruption, hybrid threats, cybersecurity, disinformation and FIMI, fundamental rights and public participation and cooperate with relevant external experts, for example with the European Digital Media Observatory (EDMO) hubs and independent fact-checking organisations ([20]).

(23) The Commission recommends that providers of VLOPs and VLOSEs define in their terms and conditions the period during which measures and resources will be in place that are specific to the mitigation of risks for the electoral process. Certain risk mitigation measures such as additional internal processes or dedicated teams

([18]) This includes Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

([19]) https://cmpf.eui.eu/media-pluralism-monitor/

([20]) See section 3.4. on 'Cooperation with national authorities, independent experts and civil society organisations

may only be needed around a specific electoral period, depending on the risk of a given provider and the specificities of the election at stake.

(24) In addition, some Member States have a set period of time for election campaigning according to national laws, while others do not. This should be taken into account by providers of VLOPs and VLOSEs. In line with insights on expected threat progression during elections from the 2nd EEAS Report on Foreign Information Manipulation and Interference (FIMI) ([21]), the Commission recommends that, depending on the risk assessment for the particular election and taking into account the applicable electoral procedures, risk mitigation measures are in place and functioning at least one to six months before an electoral period, and continue at least one month after the elections.

(25) Depending on the specific context, mitigation measures normally be intensified during the period prior to the date of elections, taking into account national rules on elections, a heightened risk for threats, and the need to provide accurate information on voting procedures.

3.2. Risk mitigation measures for electoral processes

(26) Mitigation measures for systemic risks for electoral processes should draw, in particular, on industry standards established through the Code of Practice on Disinformation and other relevant EU industry codes, such as the Code of Conduct on Countering Hate Speech Online, and from existing best practices such as those shared by the EU Internet Forum, those documented in the Content-Agnostic Election Integrity Framework for Online Platforms ([22]) and the Election Integrity Programme of the Integrity Institute ([23]) as well as recommendations from civil society, such as those from the Civil Liberties Union for Europe and European Partnership for Democracy ([24]).

3.2.1. Specific mitigation measures

(27) Specifically, mitigation measures aimed at addressing systemic risks to electoral processes should include measures in the following areas:

a) **Access to official information on the electoral process**. To improve voter turnout and prevent the spread of misinformation, disinformation and FIMI on the electoral process itself, best practice for providers of VLOPs and VLOSEs is to facilitate access to official information concerning the electoral process, including information on how and where to vote, based on official information from the electoral authorities of the Member States concerned. Such information could be provided for example by means of information panels, banners, pop-ups, search interventions, links to websites of the electoral authorities, specific election information tabs or a dedicated part of the platform. When designing and implementing such mitigation measures, the

([21]) EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf (europa.eu)

([22]) Demorcacy By Design – Accountable Tech

([23]) Elections Program — Integrity Institute

([24]) DSA: New Risk Assessments To Protect Civic Discourse and Electoral Processes liberties.eu

Commission recommends that providers of VLOPs and VLOSEs take principles such as inclusiveness and accessibility into account.

b) **Media literacy initiatives.** Best practice for providers of VLOPs and VLOSEs is to collaborate on, implement, invest and engage in media literacy initiatives and campaigns focussing on elections to foster critical thinking and improve users' skills in recognizing disinformation and manipulation techniques, also related to generative AI. This could be achieved by:

   i. Collaborating with **local media literacy organisations**, as well as relevant associations, groups and networks, financially supporting, sharing and integrating election related initiatives and campaigns on the platform, including by developing joint initiatives. Local media literacy organisations represent a valuable resource in terms of knowledge of local contexts and target audiences. The Commission recommends the use of the network of EDMO and its hubs and the Commission's Expert Group on Media Literacy to find the relevant organisations at Member State level.

   ii. Developing and applying **inoculation measures** that pre-emptively build resilience against possible and expected disinformation narratives and manipulation techniques by informing and preparing users. Such measures should take into account the specific local context where they are carried out and should be complemented by other measures providing reliable information to users. Inoculation measures can take different forms, including e.g., gamified interventions, such as participation in online games on the generation of disinformation which encourages a critical reflection on the tactics used to influence ([25]), video or other types of content ([26]), and where feasible, should be implemented in-app to foster ease of access.

   iii. When designing media literacy campaigns, it is recommended that providers of VLOPs or VLOSEs take into account specific narratives as well as tactics, techniques and procedures (TTPs) that contribute to systemic risks that are likely to occur before, during and after an election, in line with the approach of adapting mitigation measures to the **relevant national context and target audiences**.

c) **Measures to provide users with more contextual information** on the content and accounts they engage with. Examples include:

   i. **Fact-checking labels** on identified disinformation and FIMI content provided by independent fact-checkers and fact-checking teams of independent media organisations. Fact-checking coverage should extend across the EU and its languages, inter alia through strengthening the cooperation with local fact-checkers during election periods, integrating and showcasing election-related fact-checking content as well as

([25]) Traberg, C. S., Roozenbeek, J., & van der Linden, S. (2022). Psychological Inoculation against Misinformation: Current Evidence and Future Directions. The Annals of the American Academy of Political and Social Science, 700(1), 136-151. https://doi.org/10.1177/00027162221087936

([26]) Jon Roozenbeek *et al.*, Psychological inoculation improves resilience against misinformation on social media. *Sci. Adv.***8**,eabo6254(2022).DOI:10.1126/sciadv.abo6254

employing mechanisms to help increase the impact of these on audiences. Fact-checking labels should be accessible and written in easily understandable language.

ii. **Prompts and nudges** urging users to read content and evaluate its accuracy and source before sharing it.

iii. Clear, visible, and non-deceptive **indications of official accounts,** as well as accounts providing authoritative information on the electoral process, such as the accounts of electoral authorities, including the basis on which such verification is established. The criteria that lead to an "official" label for an account should be made easily available and provided in easily understandable language, to prevent such indications from giving credibility to accounts impersonating official accounts, such as those of electoral authorities.

iv. Clear, visible, and non-deceptive **labelling of accounts** controlled by Member States, third countries and entities controlled or financed by entities controlled by third countries.

v. **Tools and information to help users assess the trustworthiness** of information sources, such as trust marks focused on the integrity of the source based on transparent methodologies and developed by independent third parties.

vi. **Other tools to assess the provenance**, edit history, authenticity, or accuracy of digital content. These help users to check the authenticity or identify the provenance or source of content related to elections.

vii. Establish effective internal measures to **counter misuse** of any of the above procedures and tools, in particular the abuse of the verification process for labelled accounts and content.

d) **Recommender systems** can play a significant role in shaping the information landscape and public opinion, as recognised in recitals 70, 84, 88, and 94, as well as Article 34(2) of Regulation (EU) 2022/2065. To mitigate the risk that such systems may pose in relation to electoral processes, providers of VLOPs and VLOSEs should consider:

i. Ensuring that recommender systems are designed and adjusted in a way that gives users meaningful choices and controls over their feeds, with due regard to media diversity and pluralism;

ii. Establishing measures to reduce the prominence of disinformation in the context of elections based on clear and transparent methods, e.g. regarding deceptive content that has been fact-checked as false or coming from accounts that have been repeatedly found to spread disinformation;

iii. Establishing measures to limit the amplification of deceptive, false or misleading content generated by AI in the context of elections through their recommender systems;

iv. Regularly assessing the performance and impact of recommender systems and addressing any emerging risks or issues related to electoral processes, including by updating and refining policies, practices, and algorithms;

v. Establishing measures to provide transparency around the design and functioning of recommender systems, in particular in relation to the data and information used in designing systems that foster media pluralism and diversity of content, to facilitate third party scrutiny and research;

vi. Engaging with external parties to conduct adversarial testing and red team exercises on these systems to identify potential risks such as risks stemming from biases, susceptibility to manipulation, or amplification of misinformation, disinformation, FIMI or other harmful content.

e) **Political advertising**. Providers of VLOPs and VLOSEs are advised to prepare for the entry into application of Regulation (EU) 2024/900 on the transparency and targeting of political advertising ("Regulation on Political Advertising") and to take particular care to consider the provision on non-discrimination (Article 5(1)) which will enter into application 20 days after the Regulation's publication on 20 March 2024 ([27]). All online platform providers are responsible for ensuring that this provision is complied with. This Regulation defines political advertising as the preparation, placement, promotion, publication, delivery, or dissemination of messages by, for or on behalf of political actors, unless they are of a purely private or a purely commercial nature; or which are liable and designed to influence voting behaviour or the outcome of an election, referendum, or a legislative or regulatory process, at EU, national, regional or local level. Providers of VLOPs and VLOSEs are encouraged to take the definitions provided by the regulation into account, when applying these guidelines. If a provider of a VLOP or VLOSE offers the possibility to place political advertisements on its service, the Commission recommends that, when complying with the obligations laid down in Article 26 of Regulation (EU) 2022/2065 and in line with the forthcoming regulation on the transparency and targeting of political advertising, these are **labelled in a clear, salient and unambiguous manner** and in real time to allow users to understand that the content displayed contains political advertising. In addition, the labels applied should remain in place when shared by users on the same platform. The Commission also recommends that providers of VLOPs and VLOSEs align their policies to the Regulation on Political Advertising in advance of its entry into application which complement the legal obligations stemming from Articles 26 and 39 of Regulation (EU) 2022/2065, and in particular in the following areas:

i. Provide users with **information** about the political advertisements they see, such as the **sponsor identity** and, where applicable, the entity ultimately controlling the sponsor; the period during which the

([27]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202400900&pk_campaign=todays_OJ&pk_source=EURLEX&pk_medium=X&pk_keyword=trasparency_of_political_advertising&pk_content=regulation&pk_cid=EURLEX_todaysOJ. Articles 3 and 5(1) enter into application on entry into force on 9 April 2024. The rest of the Regulation enters into application on 9 October 2025.

political advertisement is intended to be published, delivered or disseminated; the **aggregated amounts and the aggregated value** of other benefits received by the providers of political advertising services; as well as meaningful information about the main parameters used to determine the recipient to whom the advertisement is presented.

ii. Maintain a publicly available, searchable **repository of political ads**, updated in as close as possible to real-time. This shall include, as a minimum, the total number of recipients of the service reached and, where applicable, the aggregate numbers broken down by Member State for the group or groups of recipients that the advertisement specifically targeted, as mandated by Article 39 of Regulation (EU) 2022/2065, and could also include e.g., the aggregated amounts and the aggregated value of other benefits received by the providers, the number of impressions and the geographical areas in which the ad was presented.

iii. When they do not allow political advertising on their services, have efficient **verification systems** in place and take the necessary actions to ensure that the decision is appropriately enforced.

iv. Ensure that there are adequate policies and systems in place to **prevent the misuse of advertising systems** to disseminate misleading information, disinformation and FIMI with regards to electoral processes, including deceptive generative AI content.

f) **Influencers** can have a significant impact on the electoral choices made by recipients of the service, as they are increasingly involved in facilitating political debate online. In this regard, and in order to increase transparency, providers of VLOPs and VLOSEs should:

i. Provide a functionality to allow influencers to declare whether the content they provide is or contains political advertising, including the sponsor identity and, where applicable, the entity ultimately controlling the sponsor; the period during which the political advertisement is intended to be published, delivered or disseminated; the aggregated amounts and the aggregated value of other benefits received by the providers of political advertising services; display period, as well as meaningful information about the main parameters used to determine the recipient to whom the advertisement is presented.

ii. Ensure that other recipients of the service can identify in a clear, salient and unambiguous manner and in real time, including through prominent labelling, that the content provided is or contains political advertising, as described in the influencer's declaration.

g) **Demonetisation of disinformation content.** The Commission recommends that providers of VLOPs and VLOSEs have targeted policies and systems in place to ensure that the placement of advertising does not provide financial incentives for the dissemination of disinformation and FIMI with regards to

electoral processes and hateful, (violent) extremist or radicalising content that can influence individuals in their electoral choices.

h) **Integrity of Services**. Providers of VLOPs and VLOSEs should put in place appropriate procedures to ensure the timely and effective detection and disruption of manipulation of the service when this has been identified by them as a relevant systemic risk, taking into account the best available evidence. For example, they may include in their terms and conditions specific rules against the creation of inauthentic accounts or botnets (which may include automated, partially automated, or non-automated accounts), or deceptive use of a service.

   i. The Commission recommends that providers of VLOPs and VLOSEs develop and enforce their rules, preventing deception through impersonation of candidates, the deployment of deceptive manipulated media, the use of fake engagements, non-transparent paid messages, or non-transparent promotion by influencers, as well as coordination of inauthentic content creation or behaviour.

   ii. The Commission recommends cooperation between the relevant teams of different providers of VLOPs and VLOSEs to identify common threats and to counter cross-platform disinformation campaigns, FIMI activity or hateful, (violent) extremist or radicalising activity that can influence individuals in their electoral choices and migration of malicious actors (see section 3.4 on cooperation with national authorities, independent experts and civil society organisations).

(28) Considering the evolving nature of the understanding of systemic risks to electoral processes, mitigation measures should be tied to rigorous and critical analysis, testing and review of their intended and potentially unintended impact. As such, effective mitigation measures should be based on the best available information and scientific insights. The Commission recommends that providers of VLOPs and VLOSEs pro-actively design, evaluate, and optimise conceptually valid performance metrics for the effectiveness of mitigation measures, for example via A/B testing of feature and design choices. These performance metrics should be analysed as part of providers' risk management framework and set to measure the success of relevant mitigation measures during a particular election. These metrics should be SMART (specific, measurable, achievable, relevant and time-bound) and they should be both qualitative and quantitative.

3.2.2. Third party scrutiny, research and data access

(29) Third **party scrutiny and research** into mitigation measures are important to help providers of VLOPs and VLOSEs ensure that the measures they put in place are effective and respect fundamental rights, as well as democratic principles. Stable and reliable data access for third party scrutiny is of utmost importance during electoral periods to ensure transparency and advance insights and the further development of risk mitigation measures around elections. In addition to their legal obligations under Article 40 of Regulation (EU) 2022/2065 ([28]), the Commission

([28]) Article 40.12 of the DSA already requires providers of designated VLOPs and VLOSEs to give access to eligible researchers to the information that are publicly available on their interface. Article 40(4)

recommends that providers of VLOPs and VLOSEs provide free access to data to study risks related to electoral processes, including, where necessary, those not available on the VLOP's and VLOSE's interface, to relevant third party stakeholders. In general, ad-hoc cooperation activities to design and, if necessary, swiftly adjust their risk mitigation measures in relation to electoral processes are recommended. Following documented best practice ([29]), different measures could be considered to engage in such activities with third parties,

(30) In addition to the tools and other access policies in place to comply with Article 40(12) of Regulation (EU) 2022/2065, these measures can include additional and tailor-made tools, or features, including those necessary to study and scrutinise AI models, visual dashboards, additional data points being added to existing tools or the provision of specific datasets. Access to such tools or features could be extended to a wider range of third parties, in addition to the eligible researchers under Article 40 of Regulation (EU) 2022/2065.

(31) In the area of political advertising, the Commission recommends that relevant providers of VLOPs and VLOSEs ensure that the tools and application programming interfaces (APIs) enabling research on their political advertising repositories ([30]) are fit-for-purpose and allow for meaningful research on disinformation, FIMI campaigns and hateful, (violent) extremist or radicalising content that is disseminated to influence individuals in their electoral choices during elections, including the elections to the European Parliament, in accordance with the requirements of Union law, including on the protection of personal data. This should include a set of minimum functionalities and search criteria that enable users and researchers to perform customised searches for data in as close to real time as possible during the electoral period (e.g. searches per advertiser or candidate, election, geographic area or country, language).

(32) In addition to the reports referred to in Article 42(4) of Regulation (EU) 2022/2065, the Commission recommends that providers of VLOPs and VLOSEs are as **transparent** as possible to the public about the design, functioning, and execution of mitigation measures related to electoral processes to allow for public scrutiny which in turn may impact the design of effective mitigation measures. During electoral periods, it is of particular importance that providers of VLOPs and VLOSEs show that content moderation decisions do not affect the equality of candidates or disproportionately favour or promote voices representing certain (polarised) views.

3.2.3. Fundamental rights

(33) Risk mitigation measures, taken in line with Article 35 of Regulation (EU) 2022/2065, should be taken with due regard for the protection of **fundamental rights** enshrined in the Charter of Fundamental Rights of the European Union, in particular the right to freedom of expression and of information, including media

provides for a specific data access regime for vetted researchers which will be applicable as the dedicated delegated act will be adopted.

([29]) New Guide Provides Concrete Elections Integrity Recommendations for Online Platforms — Integrity Institute

([30]) See recommendation in section 3.2.1. (e) for providers of VLOPs and VLOSEs to align their policies to the Regulation on Political Advertising in advance of its entry into application

freedom and pluralism. In line with Recital 47 of that Regulation, providers of VLOPs and VLOSEs should pay due regard to relevant international human rights standards such as the United Nations Guiding Principles on Business and Human Rights (UNGPs). Relevant independent reports ([31]) may also be considered when designing and enforcing mitigation measures.

(34) When mitigating systemic risks for electoral integrity, the Commission recommends that due regard is also given to the impact of measures to tackle illegal content such as public incitement to violence and hatred to the extent that such illegal content may inhibit or silence voices in the democratic debate, in particular those representing vulnerable groups or minorities. For example, forms of racism, or gendered disinformation and gender-based violence online including in the context of violent extremist or terrorist ideology or FIMI targeting the LGBTIQ+ community ([32]) can undermine open, democratic dialogue and debate, and further increase social division and polarization. In this respect, the Code of conduct on countering illegal hate speech online can be used as inspiration when considering appropriate action.

(35) In addition to the involvement of relevant actors during the risk assessment, as referred to in recital 90 of Regulation (EU) 2022/2065, the Commission recommends that providers of VLOPs and VLOSEs make available the fundamental rights impact assessments performed as part of the risk assessments, to civil society organisations, in particular civil society organisations consulted in this process as soon as they are concluded, i.e. possibly earlier than required under Article 42(4) of that Regulation. This could provide a space for constructive open dialogue on possible good practices and potential improvements.

3.3. Mitigation measures linked to generative AI

(36) Recent technological developments in generative AI have enabled the creation and widespread use of artificial intelligence systems capable of generating text, images, videos, or other synthetic content. While such developments may bring many new opportunities, they may lead to specific systemic risks in the context of elections. Notably, generative AI can be abused to mislead voters or to manipulate electoral processes by creating and disseminating inauthentic, biased, misleading synthetic content (including text, audio, still images and video) regarding political actors, false depiction of events, election polls, contexts or narratives. Generative AI systems can also produce incorrect, incoherent, or fabricated information, so called “hallucinations”, that misrepresent reality, and which can potentially mislead voters.

(37) Pursuant to Article 35(1) of Regulation (EU) 2022/2065, providers of VLOPs and VLOSEs should assess systemic risks in the context of elections, such as those mentioned above, and put in place reasonable, proportionate, and effective mitigation measures tailored to risks related to both the creation ( ) and

([31]) Examples include the Access Now and the European Center for Not-for-Profit Law policy paper “Towards meaningful fundamental rights impact assessments under the DSA”, Danish Institute for Human Rights, Guidance on Human Rights Impact Assessment of Digital Activities, Julian Jaursch, Josefine Bahro, Asha Allen, Claire Pershan and Katarzyna Szymielewicz, DSA risk mitigation: Current Practices, ideas and open questions

([32]) FIMI targeting LGBTIQ+ people: Well-informed analysis to protect human rights and diversity | EEAS (europa.eu)

dissemination of generative AI content, depending on the nature of their service. Best practices which may inform the relevant risk mitigation measures may be drawn already now from the AI Act and the AI Pact. Particularly relevant in this context are the obligations envisaged in the AI Act for providers of general-purpose AI models, including generative AI, requirements for labelling of 'deep fakes' and for providers of generative AI systems to use technical state-of-the-art solutions to ensure that content created by means of generative AI is marked in a machine-readable format and detectable as such, which will enable its detection by providers of VLOPs and VLOSEs. The Commission recommends that providers of VLOPs and VLOSEs align their policies to the AI Act in advance of its entry into application, in line with the AI Pact.

(38) Mitigation measures linked to generative AI should be applied by providers of VLOPs and VLOSEs, to the extent that they are technically feasible, with particular consideration to the impacts of such measures on fundamental rights protected under the Charter. The Commission also recommends cross-industry collaboration to further develop effective mitigation measures for generative AI in the context of the Codes of Practice for general-purpose AI models and transparency of AI-generated content to be developed under the AI Act.

(39) Following from the specific actual or foreseeable risks for electoral processes identified, the Commission recommends that providers of VLOPs and VLOSEs whose services can be used for the creation of deceptive, biased, false or misleading generative AI content have the following risk mitigation measures in place, to the extent this is technically feasible, and according to the current state of the art:

a) Ensure that generative AI content, and other types of synthetic and manipulated media, is detectable – notably by using sufficiently reliable, interoperable, effective and robust techniques and methods, such as **watermarks**, metadata identifications, cryptographic methods for proving provenance and authenticity of content, logging methods, fingerprints or other techniques, as may be appropriate, taking into account existing standards. This is particularly important for any generative AI content concerning candidates, politicians, or political parties. Watermarks and metadata may also be applied to content that is based on initially authentic footage (such as videos, images or audio) that subsequently has been altered through the use of generative AI;

b) Make efforts to ensure that **information** generated by AI systems is based **to the extent possible on reliable sources** in the electoral context, such as official information from relevant electoral authorities, and that any quotes or references made by the system to external sources are accurate and do not misrepresent the cited content, thus limiting the effects of 'hallucinations';

c) Warn users about potential errors in content created by generative AI systems and suggest that they **consult authoritative sources** to check the veracity of such information, as well as put safeguards in place to prevent the creation of false content that may have a strong potential to influence user behaviour;

d) Conduct and document **red-teaming** exercises and testing with a particular focus on electoral processes, with both internal teams and external experts,

before releasing generative AI systems to the public and follow a staggered release approach when doing so to better control unintended consequences;

e) Set appropriate performance metrics, including for safety and factual accuracy of answers given to questions on electoral content, and continually **monitor the performance of generative AI systems**, and take appropriate actions when needed;

f) Integrate into generative AI systems safeguards that increase their **safety**, such as prompt classifiers, content moderation and other filters, to detect and prevent prompts that go against terms of service of the provider of a VLOP or VLOSE concerning electoral processes; take other appropriate measures that seek to prevent the misuse of the generative AI system for illegal, manipulative and disinformation purposes in the context of electoral processes;

g) For text content, in particular, indicate, where possible, in the outputs generated the **concrete sources of the information used** as input data or provide other means to enable users to verify the reliability and further contextualise the information.

(40) Following from the specific actual or foreseeable risks for electoral processes identified, the Commission recommends that providers of VLOPs and VLOSEs whose services can be used to disseminate deceptive, false or misleading generative AI content consider the following risk mitigation measures, to the extent technically feasible according to the current state of the art:

a) Adapt their **terms and conditions** and ensure their enforcement, to significantly decrease the reach and impact of generative AI content that depicts disinformation or misinformation on the electoral process, such as election irregularities.

i. The Commission recommends that providers of VLOPs and VLOSEs provide clear public information on which internal processes and mitigation measures, such as labelling, marking, demoting or removing, are in place to enforce these policies;
ii. The Commission recommends that providers of VLOPs and VLOSEs cooperate and share information about such deceptive content with fact checkers to ensure that the risk of amplification in other platforms is minimised.

b) **Clearly label**, or otherwise make distinguishable through prominent markings, synthetic or manipulated images, audio or videos that appreciably resemble existing persons, objects, places, entities, events, or depict events as real that did not happen or misrepresent them, and falsely appear to a person to be authentic or truthful (i.e., **deepfakes**).

i. The Commission recommends that providers of VLOPs and VLOSEs provide users with standard and easy to use interfaces and tools to add labels to AI generated content;
ii. When labelling generative AI content, the Commission recommends that providers of VLOPs and VLOSEs apply efficient labels, easily recognised by users, taking into account aspects such as graphics,

position and timing, drawing on scientific research on the effectiveness of labels ([33]). Providers of VLOPs and VLOSEs should also test the effectiveness of such labels before release and adapt and improve them based on feedback and experience;

iii. The Commission recommends that providers of VLOPs and VLOSEs make sure the labelled generative AI content retains its label once it is shared by other users on the platform.

c) The Commission recommends that providers of VLOPs and VLOSEs adapt their advertising systems, for example by providing advertisers with options to clearly label content created with **generative AI in advertisements** or promoted posts and require in their advertising policy that this label is used when the advertisement includes generative AI content.

d) To enforce these policies, providers of VLOPs and VLOSEs should adapt their **content moderation processes and algorithmic systems** in such a way as to detect AI generated or manipulated content via watermarks, metadata identifications, cryptographic methods for proving provenance and authenticity of content, logging methods, fingerprints or other techniques.

i. In this context, providers of VLOPs and VLOSEs should cooperate with providers of generative AI systems and follow leading state of the art measures to ensure that such watermarks, metadata identifications, cryptographic methods for proving provenance and authenticity of content, logging methods, fingerprints or other techniques are detected in a reliable and effective manner; they are also recommended to support new technology innovations to improve the effectiveness and interoperability of such tools.

e) **Media literacy measures** mentioned in section 2 should also focus on generative AI systems, for instance to explain how the technology works and the possibilities for its misuse.

(41) Pursuant to Article 35(1) of the Regulation (EU) 2022/2065, when providers of VLOPs and VLOSEs address legal but harmful forms of generative AI content that can influence voters' behaviour, they should give particular consideration to the impact their policies and measures may have on fundamental rights, notably freedom of expression, including political expression, parody and satire. Such a fundamental rights impact assessment is in particular required when developing policies on what type of deceptive generative AI content a provider of a VLOP or VLOSE does not allow on their service and will remove from it.

(42) As AI generated content bears specific risks, it should be subject to heightened scrutiny, also through the development of ad hoc tools and technologies, e.g. to perform research aimed at identifying and understanding specific risks related to electoral processes. Providers of VLOPs and VLOSEs are encouraged to consider setting up dedicated tools for researchers to get access to and specifically identify and analyse AI generated content.

([33]) See for example Tom Dobber, Sanne Kruikemeier, Fabio Votta, Natali Helberger & Ellen P. Goodman (2023) The effect of traffic light veracity labels on perceptions of political advertising source and message credibility on social media, Journal of Information Technology & Politics

3.4. Cooperation with national authorities, independent experts and civil society organisations

(43) Contributing to protecting the integrity of a specific election cannot be done without knowledge of the specific national, legal, societal, and political context as well as timely reactions to real-time developments affecting the risks generated by VLOPs or VLOSEs services. Procedures and organisational structures for elections differ from Member State to Member State and even from one election to another. Providers of VLOPs and VLOSEs should be aware of the applicable national election governance structure for the elections at hand and the role of various authorities. By gaining a good understanding of specific national procedures such as the delimitation of the electoral campaign periods, timing of the official designation of election candidates, and election silence periods, providers of VLOPs and VLOSEs may design risk mitigation measures taking into account the specific aspects of the relevant Member State.

(44) To this end, the Commission recommends that providers of VLOPs and VLOSEs regularly and, where necessary, urgently, exchange information with and have contact points for competent national and European authorities, involving the Digital Services Coordinator of their Member State and, where appropriate, competent regional and local authorities, to facilitate the exchange of information, as well as the Commission, as appropriate.

(45) The goal of such interactions between providers of VLOPs and VLOSEs and competent national authorities should be limited to share information that can inform risk assessments and mitigation measures on electoral processes or can inform national authorities' actions that are within their competence to protect the integrity of electoral processes. For example, relevant national authorities can provide providers of VLOPs and VLOSEs with official information on the voting process that can be integrated in their services, and where possible and appropriate, provide them with information on possible risks for the electoral process, which can inform the mitigation measures providers of VLOPs and VLOSEs put in place. In return, information on the risks providers of VLOPs and VLOSEs mitigate on their service can be relevant for competent national authorities' work in protecting the integrity of electoral processes. To the extent that such interactions do not fall within the scope of the transparency reporting obligations under Regulation (EU) 2022/2065, the Commission recommends that national authorities and providers of VLOPSs and VLOSEs transparently report about them , for example in public documents in which national authorities evaluate the electoral process, or in transparency reporting that follows from Regulation (EU) 2022/2065.

(46) The Digital Services Coordinators designated under Regulation (EU) 2022/2065 in each Member State may serve as contact points for providers of VLOPs or VLOSEs, should it not be clear which national authority is competent for issues related to risk mitigation on electoral processes. As Digital Services Coordinators function as the single contact point with regard to all matters related to the application of Regulation (EU) 2022/2065 in a Member State, the Commission recommends that the Digital Services Coordinators are involved in the exchanges between providers of VLOPs and VLOSEs and competent national authorities on the electoral process. Additionally, the Commission recommended to Member

States to strengthen their national election networks ([34]) and to facilitate their cooperation with relevant stakeholders ([35]). These national election networks can also be a relevant contact point for providers of VLOPs and VLOSEs.

(47) Alongside cooperation with national authorities, providers of VLOPs and VLOSEs are also recommended to establish strong cooperation with relevant non-state actors as such actors play a key role in protecting electoral processes. Prior to the elections, providers of VLOPS and VLOSEs may organise meetings as well as establish channels of regular communication with non-state actors active in electoral processes such as academics, independent experts, civil society organisations and representatives of various communities, and invite them to share their independent expertise, insights and observations that can help identify risks that may require mitigation measures and contribute to the development of such mitigation measures.

(48) Establishing channels for communication during the election campaign with non-state actors, including campaign organisations and election observers, will help providers of VLOPs and VLOSEs to better understand the context of the elections so as to react promptly in emergency situations, to design and calibrate risk mitigation measures and to understand better how their mitigation measures work in the local context. The Working Group on Elections of the Code of Practice – and its rapid response system – is a good example of such an existing and active multistakeholder forum, including NGOs and fact-checkers with important election specific experience. The EDMO Task-force on Elections – composed of independent fact-checkers, academics, and media literacy specialists – as well as the EDMO hubs across the EU can also provide important input in this respect.

(49) The availability of trustworthy information from pluralistic sources is crucial for well-functioning democratic electoral processes. It warrants not only protection from external commercial and political interference, but also from potential misapplication of the internal processes of VLOPs and VLOSEs, as recognised by Article 17 of the proposed European Media Freedom Act ([36]). Journalists and media service providers fulfil a vital role in gathering, processing, and reporting information to the public, a role even more critical during election times. Independent news media service providers and organisations with well-established internal editorial standards and procedures are widely regarded as trusted sources of information. Providers of VLOPs and VLOSEs should, therefore, collaborate with independent media organisations, regulatory authorities, civil society and grassroots organisations, fact-checkers, academia, and other relevant stakeholders on initiatives to enhance the identification of trustworthy information and users' accessibility to pluralistic news media content related to elections from trusted sources.

(50) Considering the important role in judging the veracity of information that such organisations have, the Commission recommends that providers of VLOPs and VLOSEs collaborate with independent fact-checking organisations that adhere to

([34]) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018H0234

([35]) 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

[36] Texts adopted - European Media Freedom Act - Wednesday, 13 March 2024 (europa.eu)

high standards of methodology, ethics and transparency, for example by being a member of the European Fact-Checking Standards Network (EFCSN) and following its Code of Standards ([37]). The Commission recommends that such collaboration is transparent. For example, some signatories of the Code of Practice on Disinformation list the fact-checking organisations they have agreements with.

3.5. During an electoral period

(51) During the electoral period, in which measures and resources will be in place that are specific to the mitigation of risks for the electoral process, the Commission recommends that providers of VLOPs and VLOSEs pay specific attention to risk mitigation measures that reduce the impact of incidents that can have a significant impact on the election outcome or turnout.

(52) This includes providing users with access to reliable, timely and intelligible information from official sources on how to vote as well as on the voting process or measures like those mentioned in section 3.3 to reduce the potential harm of high impact issues such as manipulated images, voice recordings or deepfakes, for example of political actors contending in elections. Providers of VLOPs and VLOSEs should also ensure that are able to react rapidly to manipulation of their service aimed at undermining the electoral process and attempts to use disinformation and information manipulation to suppress voters.

(53) Incidents occurring on- or off- platform during an electoral period can have rapid and high-impact consequences for the integrity of elections or public security. The Commission recommends, as a result, that providers of VLOPs and VLOSEs put in place an **internal incident response mechanism**, involving also the senior leadership, as well as a mapping of the stakeholders involved within the organisation in responding to the incident. This procedure should be set-up, agreed-upon and tested, including through red teaming exercises, beforehand so it can be applied quickly. This procedure also needs to be consistent, repeatable and auditable, and produce well-documented decisions and outcomes, so that providers of VLOPs and VLOSEs can review their responses after high impact events.

(54) Considering the need for the rapid application of mitigation measures, the Commission also recommends that providers of VLOPs and VLOSEs establish cooperation and swift and efficient exchange of information cross-platform and with relevant non-state actors that have knowledge and expertise relevant for elections; these actors could include stakeholders from civil society organisations, academia and researchers, independent media and others. Considering the cross-platform nature of illegal and/or harmful content, as well as of disinformation and FIMI activity, cooperation amongst VLOPs and VLOSEs themselves to share relevant information, as well as their cooperation with smaller platforms and services is crucial to mitigate these risks effectively. This will help providers of VLOPs and VLOSEs to react more swiftly to emerging issues and incidents, better understand the context, adapt their mitigation measures, and help them assess the effectiveness of their actions taken. The efficiency of this cooperation and this exchange of information is particularly essential due to the time-sensitive nature of such events. It therefore should include reactions from providers of VLOPs and

([37]) EFCSN | European Fact-Checking Standards Network Project – European Fact-Checking Standards Network Project

VLOSEs and meaningful feedback to relevant non-state actors involved – within a reasonable timeframe – allowing assessment of the efficiency and impact of this cooperation and exchange.

(55) The rapid response system to be established by the signatories of the Code of Practice on Disinformation is a good example of such a forum for cooperation during elections, feeding into the platforms incident response mechanisms. Providers of VLOPs and VLOSEs should set out, together with the other signatories, the procedural framework for cooperation and coordination between them during elections, including a rapid feedback mechanism with the need of swift, efficient, and appropriate follow-up by platforms.

(56) Another example on how to organise the work on responses to FIMI and disinformation can be found in the second EEAS Report on FIMI Threats ([38]) which puts forward a "Response Framework" effectively linking analysis to evidence-based responses while highlighting the importance of cooperation between various stakeholders. Inspiration could also be drawn from initiatives like the Information Sharing and Analysis Center on Foreign Information Manipulation and Interference (FIMI-ISAC) ([39]). Such a FIMI-ISAC aims to promote the sharing of information between all stakeholders about root causes, incidents and threats, and the sharing of experience, knowledge and analysis.

(57) A timely response to incidents is often key. The Commission recommends that providers of VLOPs and VLOSEs consider a 'follow the sun' model in which offices around the world would be able to cover all time zones.

(58) To react in a timely manner, providers of VLOPs and VLOSEs should integrate their possible collaboration with electoral authorities and relevant non-state actors in incident response mechanisms.

3.6. After an electoral period

(59) After an electoral period, the Commission recommends that providers of VLOPs and VLOSEs conduct a **post-election review** including an assessment of the effectiveness of the risk mitigation measures employed in that context with a view to adapting the measures, if necessary. This internal report should include an assessment of whether the internal performance metrics and any other assessment criteria were met before, during and after the elections, lessons learned and areas for improvement.

(60) The Commission recommends that providers of VLOPs and VLOSEs take into account specific contributions from independent researchers, Civil Society Organisations, and independent fact-checkers on the impact of VLOPs and VLOSEs mitigation measures in the election review exercise. In addition, providers of VLOPs and VLOSEs may engage with established independent election observer groups who may be able to provide information on the use and impact of their services in that context.

([38]) EEAS-2nd-Report on FIMI Threats-January-2024_0.pdf (europa.eu)

([39]) https://fimi-isac.org/

(61) In particular, the post-election report should include information on the average and distribution of response time for terms and conditions violations, the average and distribution of the response time to flagged content by users and non-state actors, the average and distribution of the reach and engagement of content acted upon, the number of violations of certain policies pertaining to elections, instances of information manipulation and the reach of certain measures such as media literacy initiatives and authoritative initiatives. The Commission may require such reports in a confidential manner ([40]).

(62) The Commission recommends that providers of VLOPs and VLOSEs publish a public version of such post-election review documents. This should include information on actions taken by the provider of VLOPs or VLOSEs and any incidents that might have occurred, as well as information on cooperation and information exchanges that took place with relevant non-state actors during the electoral campaign period. This should include details on actions taken, efficiency and timeliness of such cooperation. This also aims at gathering public feedback on how to improve the risk mitigation measures in place or share successful measures with other providers. As a further example for election related reporting, signatories of the Code of Practice on Disinformation have developed a reporting template through which they will report ahead of and after elections on their measures taken and relevant metrics regarding their impact.

3.7. Specific guidance for the elections to the European Parliament

(63) As stated in the Communication on the Defence of Democracy package ([41]) the upcoming elections to the European Parliament will be a crucial test case for the resilience of our democratic processes, also in the face of hybrid threats including not only disinformation and FIMI but also cyberattacks. In that context, and due to their unique cross-border nature, providers of VLOPs and VLOSEs are recommended to put in place robust mitigation measures for the elections to the European Parliament taking place from 6 to 9 June 2024.

(64) This means that providers of VLOPs and VLOSEs are recommended to ensure **sufficient resources** and risk mitigation measures are available and **distributed** in a way that is proportionate to the risk assessments and include access to relevant national expertise across the EU – both at EU and Member State level.

(65) For elections to the European Parliament no predetermined campaigning period exists. This means that in Member States the campaigns for these elections can start and end at different points in time. Providers of VLOPs and VLOSEs are encouraged to take this into account when planning their risk mitigation measures for election to the European Parliament and engage with Member States in preparation of such elections.

(66) Providers of VLOPs and VLOSEs should also take into account the **unique cross-border and European dimension of these elections**, when assigning appropriate risk mitigation resources. Campaigning will not only be national and the debate

([40]) DSA Article 84

([41]) COM(2023) 630 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Defence of Democracy

will occur across borders. In addition to establishing contact with the relevant national authorities, the Commission recommends that providers of VLOPs and VLOSEs establish contact with EU-level authorities before the elections. The European Parliament plays a key role in the European elections and should be a key interlocutor for VLOPs and VLOSEs ahead of these elections. EU-wide networks of national experts in the areas of disinformation and FIMI, elections and cybersecurity such as the EU Rapid Alert System, European Cooperation Network on Elections and the NIS Cooperation Group could be relevant networks for providers of VLOPs and VLOSEs in case of cross-border incidents, including those of a hybrid nature, during the electoral period that require a rapid response and deployment of risk mitigating measures.

(67) Mitigation measures that might have to take into account related threats of a different nature aiming to destabilize or discredit the democratic processes, including cyberattacks, appropriate cooperation across these domains should be ensured. In case of cyber-enabled disinformation or FIMI activity, providers of VLOPs and VLOSEs are encouraged to establish adequate contact with national cybersecurity authorities; where such activity concerns the EU as a whole or the EU institutions, bodies and agencies, contacts with the EU Agency for Cybersecurity (ENISA) and the Computer Emergency Response Team for EU institutions, bodies and agencies (CERT-EU)[42] should be considered. Furthermore, and in line with what was proposed for national elections, the Commission recommends establishing contact and access to communication with the European Parliament's administration and European political parties on equal terms before elections to the European Parliament.

(68) Providers of VLOPs and VLOSEs who are signatories of the Code of Practice on Disinformation should engage fully in the work related to the elections to the European Parliament, including through effective participation in the rapid response system and feedback mechanism with appropriate and timely follow-up actions. They should also provide – ahead of and after the elections - targeted reporting on the measures put in place to reduce the spread of disinformation, information manipulation and FIMI in relation to the elections to the European Parliament, including relevant metrics on their impact (based on commitments 37.2 and 42). They should - based on the inputs of fact-checkers and civil society signatories - take stock after the elections of the lessons learned, assessing also the efficiency and timeliness of the cooperation – to improve the efficiency of the system for future elections.

(69) Section 3.6 on post-electoral review also applies to the European Parliament elections and should account for the particular nature of these elections.

(70) To tailor their risk mitigation measures for elections to the European Parliament, the Commission recommends that providers of VLOPs and VLOSEs establish contact and cooperate in particular with the EDMO Task Force on the elections to the European Parliament. For the 2024 elections to the European Parliament, this Task Force will produce reports and regular updates about the main disinformation trends, challenges, and phenomena. This should inform providers of VLOPs and VLOSEs actions and mitigating measures.

[42] https://cert.europa.eu/

4. NEXT STEPS AND CONCLUSION

(71) The Commission is committed to vigorously enforcing Regulation (EU) 2022/2065, including in the area of elections. These guidelines help providers of VLOPs and VLOSEs with the application of Article 35 of that regulation, in particular in relation to how to assess and mitigate systemic risks for electoral processes that stem from their service or use thereof. In view of numerous upcoming elections and not least those to the European Parliament, the Commission strongly encourages providers of VLOPs and VLOSEs to implement these guidelines quickly and comprehensively and welcomes assessments from researchers and civil society organisations on the effectiveness of the risk mitigation measures taken by the providers of these VLOPs and VLOSEs in the EU.

(72) At the same time, in particular given the early stage of implementation of Regulation (EU) 2022/2065, and the specific nature of systemic risks to electoral processes, the Commission stands ready to engage with providers of VLOPs and VLOSEs concerning the design and functioning of their services and related systems to ensure harm to electoral processes in the EU is avoided.

(73) In this context, the Commission is available to facilitate a periodic review of the risk mitigation measures adopted by providers of VLOPs and VLOSEs on a voluntary basis. This could take the form of ex ante and ex post reviewing after specific elections. The feedback provided by the Commission in that context will be based on the information provided by the providers of VLOPs and VLOSEs and would not constitute a fully-fledged assessment of the compliance measures they had adopted. As such, it is without prejudice to the Commission's investigatory and enforcement powers pursuant to Regulation (EU) 2022/2065.

(74) Under Article 64 of Regulation (EU) 2022/2065, the Commission will continue to develop expertise and capabilities on systemic and emerging issues across the EU. Information from VLOPs and VLOSEs is crucial in this regard. The Commission expects providers of such services to engage with the Commission in the frame of the enforcement of Regulation (EU) 2022/2065 in readiness dialogues on election integrity and other cooperation structures set up by the Commission services responsible for the enforcement of Regulation (EU) 2022/2065 for these purposes, to be able to respond quickly to urgent requests for information in particular on emerging issues and incidents that can have a significant impact on the election outcome or turnout. This does not preclude engagement in any other established cooperation mechanisms or protocols that may exist.

(75) As mentioned in section 1.1. in more detail, the risk-mitigation measures identified in these guidelines are based on previous readiness dialogues on election integrity with providers of VLOPs and VLOSEs, the experience gained with the Code of Practice on Disinformation and the EU FIMI Toolbox, the exploratory consultation, various round tables and input from Digital Services Coordinators. As such, the measures outlined in the guidelines can be considered as best practices at this moment in time.

(76) While the objective of this guidance is to support providers of VLOPs and VLOSEs in ensuring compliance with their obligations under Article 35 of Regulation (EU) 2022/2065, the Commission's understanding of the issues at stake

in the interpretation and implementation of Article 35 of that Regulation may evolve with further experience.

(77) In addition, the fast-evolving landscape in which providers of VLOPs and VLOSEs operate, and the tactics of malicious actors are constantly changing, thereby requiring constant updates and adjustments to respond to the ever-changing and newly emerging challenges. Moreover, once assessed by the Commission and the European Board for Digital Services, the Code of Practice on Disinformation is expected to be converted into a Code of Conduct tying it to the legal framework of Regulation (EU) 2022/2065. In this context, the Commission expects signatories to continue implementing their commitments to address disinformation under the Code of Practice on Disinformation. At the same time, additional pieces of EU legislation are set to come into force in the months to come and complement this Regulation with specific rules relevant for the subject matter of these guidelines, notably the Regulation on Political Advertising and the AI Act (the relevant content of which has been taken into account in these guidelines, in particular when it constitutes, already now, best practice in a specific area).

(78) The Commission may review these guidelines in view of practical experience gained and the pace of technological, societal and regulatory developments in this area. During such a review the Commission may decide to withdraw or amend the present Communication. The Commission encourages providers of VLOPs and VLOSEs, Digital Services Coordinators, the research community and civil society organisations to contribute to this process.