Council of the European Union

**Brussels, 2 June 2021**
**(OR. en)**

**9440/21**

**HYBRID 31**
**DISINFO 14**
**AG 47**
**FREMP 159**
**PE 59**
**AUDIO 59**
**DIGIT 66**
**SOC 375**

**COVER NOTE**

| | |
|---|---|
| From: | Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director |
| To: | Mr Jeppe TRANHOLM-MIKKELSEN, Secretary-General of the Council of the European Union |
| No. Cion doc.: | COM(2021) 262 final |
| Subject: | COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS European Commission Guidance on Strengthening the Code of Practice on Disinformation |

Delegations will find attached document COM(2021) 262 final.

Encl.: COM(2021) 262 final

EUROPEAN
COMMISSION

Brussels, 26.5.2021
COM(2021) 262 final

# COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

## European Commission Guidance on Strengthening the Code of Practice on Disinformation

## 1 INTRODUCTION

The COVID-19 crisis has starkly illustrated the threats and challenges disinformation poses to our societies. The 'infodemic' – the rapid spread of false, inaccurate or misleading information about the pandemic – has posed substantial risks to personal health, public health systems, effective crisis management, the economy and social cohesion. The pandemic has also elevated the role digital technology plays in our lives, making it increasingly central to how we work, learn, socialise, provide for material needs, and participate in the civic discourse. It has raised the stakes to ensure that the online ecosystem is a safe space, and it has shown that, despite considerable efforts made to date, there is an urgent need to step-up efforts to fight disinformation[1].

From its inception[2], the EU approach to countering disinformation has been grounded in the protection of freedom of expression and other rights and freedoms guaranteed under the EU Charter of Fundamental Rights. In line with those rights and freedoms, rather than criminalising or prohibiting disinformation as such, the EU strategy aims to make the online environment and its actors more transparent and accountable, making content moderation practices more transparent, empowering citizens and fostering an open democratic debate[3]. To this end, the EU has sought to mobilise all relevant stakeholders, including public authorities, businesses, media, academics and civil society.

A centrepiece of EU efforts has been the self-regulatory Code of Practice on Disinformation[4]. In force since October 2018, the Code's signatories now comprise major online platforms active in the EU as well as, *inter alia*, major trade associations representing the European advertising sector. The Commission considers the Code to be a substantial, first-of-its-kind achievement. It has provided an innovative tool for ensuring greater transparency and accountability of online platforms, as well as a structured framework for monitoring and improving the platforms' policies on disinformation.

Nevertheless, the Commission's Assessment of the Code of Practice in 2020[5] has revealed significant shortcomings. These include inconsistent and incomplete application of the Code across platforms and Member States, limitations intrinsic to the self-regulatory nature of the Code, as well as gaps in the coverage of the Code's commitments. The assessment also highlighted the lack of an appropriate monitoring mechanism, including key performance indicators (KPIs), lack of commitments on access to platforms' data for research on disinformation and limited participation from stakeholders, in particular from the advertising sector. Therefore, the Commission announced in the European Democracy Action Plan[6] (EDAP) that it will issue guidance for strengthening the Code, as part of comprehensive actions to address disinformation in

---

[1] Joint Communication on Tackling COVID-19 Disinformation – Getting the facts right (JOIN (2020) 8 final).
[2] In the Action Plan against Disinformation (JOIN (2018) 36 final), the European Commission and the High Representative set out a comprehensive strategy to counter disinformation in the EU.
[3] While online platforms' terms and conditions may cover also content which is harmful but not illegal, when disinformation constitutes illegal content (e.g. hate speech or terrorist content), the relevant legislative remedies apply).
[4] https://ec.europa.eu/digital-single-market/en/code-practice-disinformation
[5] SWD (2020) 180 final.
[6] COM (2020) 790 final.

the online environment, and that it will present specific legislation on the transparency of political advertising.

To step up the fight against disinformation, the Digital Services Act[7] (DSA) proposed by the Commission sets out a co-regulatory framework through Codes of Conduct for addressing systemic risks linked to disinformation. Furthermore, it introduces wide-ranging transparency measures around content moderation and advertising, and proposes binding and enforceable legal obligations for very large online platforms[8] to assess and address systemic risks for fundamental rights or presented by the intentional manipulation of their service.

The Guidance is based on the Commission's experience to date in monitoring and evaluating the Code[9] and on the Commission's report on the 2019 elections[10]. It also contributes to the Commission's response to the December 2020 European Council conclusions[11]. To collect input to the Guidance, the Commission organised multi-stakeholder discussions[12] as well as a workshop for Member States.

This Guidance sets out the Commission's views on how platforms and other relevant stakeholders should step up their measures to address gaps and shortcomings in the Code and create a more transparent, safe and trustworthy online environment. One area, in particular, where the Code has failed to achieve sufficient progress is in the demonetisation of disinformation, where online advertisements still continue to incentivise the dissemination of disinformation[13]. Online platforms and all other players of the online advertising ecosystem should thus take responsibility and work together to defund disinformation. Furthermore, the revised Code should step up commitments to limit manipulative behaviour, strengthen user empowerment tools, increase the transparency of political advertising, and further empower the research and fact-checking community. The Guidance also lays out the cornerstones for an improved, robust framework for the monitoring of the strengthened Code. The strengthened Code should also aim to achieve a broader participation with new signatories, including additional online platforms active in the EU as well as other relevant players.

---

[7] Proposal for a Regulation of the European Parliament and the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM (2020) 825 final). References to the DSA in this document are to be understood as to the text as proposed by the Commission.

[8] The DSA proposal defines very large platforms in Art. 25 as online platforms which provide their services to a number of average monthly active recipients of the service in the Union corresponding to 10% of the Union's population.

[9] Commission's September 2020 Assessment (SWD (2020) 180 final)

[10] Report on the 2019 elections to the European Parliament (SWD (2020) 113 final) https://ec.europa.eu/info/files/com_2020_252_en.pdf_en

[11] https://www.consilium.europa.eu/media/47296/1011-12-20-euco-conclusions-en.pdf

[12] A summary of the discussions with stakeholder is available here: https://digital-strategy.ec.europa.eu/en/library/summary-multi-stakeholder-discussions-preparation-guidance-strengthen-code-practice-disinformation

[13] Evidence also shows that revenues from online advertisements still contribute significantly to the monetisation of disinformation websites, including advertising from large brands unwittingly placed next to disinformation content (e.g. Global Disinformation Index report https://disinformationindex.org/2020/03/why-is-ad-tech-giving-millions-to-eu-disinformation-sites/ and Avaaz report https://secure.avaaz.org/campaign/en/youtube_climate_misinformation/)

Strengthening the Code offers an early opportunity for stakeholders to design appropriate measures in view of the adoption of the proposed DSA. Notably, the Guidance also aims at evolving the existing Code of Practice towards a 'Code of Conduct' as foreseen in its Article 35. Very large platforms[14] in particular, will benefit from participating in the strengthened Code in anticipation of new obligations applicable to them under the proposed DSA, in particular with regard to risk assessment, risk mitigation, user empowerment, and transparency around advertising. Smaller platforms and other stakeholders will also benefit from subscribing to appropriate commitments under the strengthened Code to gain from its best practices and to protect themselves against reputational risks presented by the misuse of their systems to spread disinformation.

Without prejudice to the final agreement of the co-legislators on the DSA or on the Commission's legislative initiative on the transparency of political advertising, the strengthened Code of Practice can serve as a tool for online platforms to improve their policies and mitigate risks linked to disinformation that their services present to democracy.

The strengthening of the Code is not only a provisional step. This Guidance calls for developing the Code into a strong, stable, flexible instrument that makes online platforms more transparent, accountable and responsible by design.

## 2 COVID-19 MONITORING – RESULTS AND LESSONS LEARNED

In addition to the lessons learned through the evaluation of the Code of Practice, new insights have been gathered under the monitoring programme set up following the Joint Communication on Tackling COVID-19 disinformation[15], during which online platform signatories to the Code have been reporting monthly on actions taken to combat COVID-19 disinformation in the EU.

The monitoring programme has not only provided an in-depth overview of the actions taken to counter disinformation around COVID-19 based on the Code's commitments, it has also put the Code through a 'stress test'.

The platforms' reports show that the Code's commitments have been implemented through effective actions in various areas, such as increased visibility of authoritative sources on their services; development and deployment of new tools and services to facilitate access to reliable information; actions to address content containing false or misleading information likely to cause physical harm or impair the effectiveness of public health policies; expressly prohibiting advertising that exploits the crisis or spreads disinformation about COVID-19.

Overall, the programme has demonstrated that the Code provides an agile, structured framework that can be deployed and translated into decisive action by signatories to fight disinformation in crisis situations and which is complementary to obligations under applicable regulatory frameworks. The Code also provided a useful structure for monitoring these measures in an extraordinary situation, dynamically shifting the focus as the crisis evolved (e.g. to focus on disinformation around COVID-19 vaccines).

---

[14] In the sense of Art. 25 of the DSA as proposed by the Commission. For the definition, see footnote 8.
[15] Joint Communication on Tackling COVID-19 Disinformation – Getting the facts right (JOIN (2020) 8 final).

At the same time, the COVID-19 programme highlighted a number of shortcomings of the existing monitoring framework of the Code of Practice:

- *Quality of reporting.* There are substantial variations in the consistency, quality and level of detail of the reporting. The lack of sufficiently granular data, particularly at Member State level, meant that the information provided often did not reveal whether reported actions were implemented across all Member States or in all EU languages. Moreover, the lack of a common, agreed reporting template remains an obstacle for more efficient monitoring and cross-platform comparisons.
- *KPIs*. While the quality and the granularity of the reporting improved over time, the data provided is still not always adequate and sufficiently detailed to measure the extent to which commitments are implemented or the effect of the actions taken.
- *Independent assessment*. The COVID-19 monitoring has confirmed the need for independent verification of the signatories' reports, in particular whether reported policies and actions have been implemented at Member State level and in all EU languages, and whether the reporting sufficiently addresses disinformation concerns at national level[16].
- *Lack of sufficient fact-checking coverage.* During the COVID-19 'infodemic' signatories have increased fact-checking activities on their services which are becoming available also to users of private messaging apps. However, content labelled as false by independent fact-checkers tends to resurge across platforms due to the lack of a centralised fact-checks repository.
- *Continued monetisation of disinformation through advertisement placements.* Despite actions to limit the monetisation of disinformation, relevant research shows that problems persist in this area[17].

# 3 HORIZONTAL ISSUES TO BE ADDRESSED

## 3.1 Reinforced commitments to achieve the Code's objectives

The commitments of the current Code of Practice are not sufficiently effective in providing a comprehensive response to the disinformation phenomena. There is a need for stronger and more specific commitments in all areas of the Code to address gaps and shortcomings, including new and emerging risks. To ensure that the Code stays a living instrument, signatories should set up a permanent mechanism for its regular adaptation.

## 3.2 Expanded scope

The 'infodemic' around the COVID-19 pandemic has demonstrated that misinformation[18] (false or misleading information spread without a malicious intent) can also pose

[16] As foreseen in the June 2020 Communication, the European Regulators Group for Audiovisual Media Services is assisting the Commission with the COVID-19 monitoring programme.

[17] GDI research in January and February 2021 on France, Germany, Italy and Spain highlights that the majority of ad tech companies do not have specific COVID-19 disinformation content policies or that those policies are violated and continue to fund news sites flagged publicly as purveyors of disinformation: https://disinformationindex.org/2021/02/ad-funded-covid-19-conspiracy-sites-a-look-at-the-eu/. Avaaz research in August 2020 highlighted that content from the top 10 websites spreading health misinformation had almost four times as many estimated views on Facebook as equivalent content from the websites of 10 leading health institutions: https://secure.avaaz.org/campaign/en/facebook_threat_health/.

substantial public harm if it becomes viral. While the main target remains disinformation in the narrow sense[19], in the strengthened Code signatories should commit to have in place appropriate policies and take proportionate actions to mitigate the risks posed by misinformation, when there is a significant public harm dimension and with proper safeguards for the freedom of speech. Users need to be empowered to contrast this information with authoritative sources and be informed where the information they are seeing is verifiably false. In line with this, depending on their nature, not all commitments of the Code would apply to misinformation.

The present Guidance uses – for the ease of reference – the overarching term 'disinformation' to refer to the different phenomena to be addressed, while clearly acknowledging the important differences between them[20]. Disinformation in this sense includes disinformation in the narrow sense, misinformation, as well as information influence operations[21] and foreign interference[22] in the information space, including from foreign actors, where information manipulation is used with the effect of causing significant public harm.

### 3.3 Broadened participation

The current Code's signatories include major online platforms operating in the EU. However, wider participation from both established and emerging platforms could provide a more comprehensive and coordinated response to the spread of disinformation. Potential new signatories may include providers of online services which disseminate information to the public, such as smaller social media or search services (e.g. players offering services at national or regional level or on a specialised/topical basis). Given the relevant compliance burdens, including reporting obligations, commitments under the strengthened Code should take into account the size of the signatories' services. While very large online platforms will need to take robust measures to address the relevant systemic risks under the proposed DSA, the measures applicable to smaller or emerging services should not impose a disproportionate burden on them.

Private messaging services can also be misused to fuel disinformation and misinformation, as observed in recent electoral campaigns and during the COVID-19 pandemic[23]. Such service providers could be signatories of the Code, committing to specific measures appropriate for this type of services, without any weakening of the encryption often used by this type of services, and with due regard to the protection of privacy and the right to private and family life including communications.

---

[18] EDAP defines misinformation as follows: *'misinformation is false or misleading content shared without harmful intent though the effects can be still harmful, e.g. when people share false information with friends and family in good faith'*.

[19] EDAP defines disinformation as follows: '*disinformation is false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm'*.

[20] Where relevant, the Guidance distinguishes between the different subcategories.

[21] As defined in EDAP: 'information *influence operation refers to coordinated efforts by either domestic or foreign actors to influence a target audience using a range of deceptive means, including suppressing independent information sources in combination with disinformation*'.

[22] As defined in EDAP: '*foreign interference in the information space, often carried out as part of a broader hybrid operation, can be understood as coercive and deceptive efforts to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents*'.

[23] 'Stop the virus of disinformation', United Nations Interregional Crime and Justice Research Institute (UNICRI), http://www.unicri.it/sites/default/files/2020-11/SM%20misuse.pdf

In order to increase the Code's impact on the demonetisation of disinformation, a broader participation of stakeholders from the advertising ecosystem beyond the circle of the Code's current signatories (European and national associations from the advertising sector) is key. The Code would benefit in particular from more involvement of brands (in particular those with substantial online advertisement spending) as well as other participants of the online advertising sector (e.g. ad exchanges, ad-tech providers, communication agencies) and other players providing services that may be used to monetise disinformation (e.g. e-payment services, e-commerce platforms, crowd-funding/donation systems)[24].

New signatories could also include other stakeholders that can have a significant impact through their tools, instruments, solutions or relevant specific expertise, including fact-checkers, organisations providing ratings relating to disinformation sites or assessing disinformation, as well as providers of technological solutions that can support the efforts to address disinformation. Such organisations can contribute considerably to the efficient implementation of the Code and its success.

### 3.4 Tailored commitments

To facilitate broader participation, the strengthened Code should include tailored commitments that correspond to the diversity of services provided by signatories and the particular roles they play in the ecosystem.

Signatories should sign up to the commitments that are relevant for their services. While participation in the Code and subscription to its commitments remains voluntary, in order to ensure the Code's effectiveness as a risk mitigation tool, signatories should not, in principle, opt out of commitments that are relevant for their services. Where signatories opt not to subscribe to a particular commitment relevant for their services, they should provide a public justification, in the spirit of recital 68 of the proposed DSA. Signatories that are providing tools, instruments or solutions to fight disinformation could subscribe to appropriate commitments and support other signatories of the Code with their expertise. Any reporting requirements for such organisations should be adapted to their mission.

### 3.5 European Digital Media Observatory

To provide an effective contribution to addressing the issue of disinformation, it is crucial to have the support of a multidisciplinary community including fact-checkers, academic researchers and other relevant stakeholders. To contribute to the creation of such community and facilitate its work, the European Digital Media Observatory (EDMO)[25] was established. By providing support to independent researchers and fact-checkers, EDMO and its national hubs will increase their capacity to detect and analyse disinformation campaigns. EDMO can play an important role in achieving several of the Code's objectives. It is thus expected that signatories of the Code will cooperate with EDMO as appropriate.

---

[24] 'How COVID-19 conspiracists and extremists use crowdfunding platforms to fund their activities', EUDisinfoLab https://www.disinfo.eu/publications/how-covid-19-conspiracists-and-extremists-use-crowdfunding-platforms-to-fund-their-activities/

[25] https://edmo.eu/

### 3.6 Rapid Alert System

As outlined in the 2018 Action Plan against Disinformation[26], online platforms should cooperate with the EU Rapid Alert System, which connects all EU Member States and relevant EU Institutions to enable joint responses to disinformation by information sharing and providing timely alerts on disinformation campaigns. Building on this, the strengthened Code should explore opportunities for reinforcing such cooperation, notably by facilitating an informal exchange between the signatories to present their work and findings, as well as to ensure close, streamlined and coherent links on a national level between all the Member States and the signatories as appropriate. This should also take into account the cooperation with EDMO, as mentioned above.

## 4 SCRUTINY OF AD PLACEMENTS

As explained, decisive action to demonetise the purveyors of disinformation is key for the Code's success. The strengthened Code's commitments should therefore take more granular, tailored action to address disinformation risks linked to the distribution of online advertising, keeping in mind upcoming regulatory requirements in the proposed DSA applicable to all online advertising, including political and issue-based advertising and, to the extent applicable, the announced initiative on political advertising.

### 4.1 Demonetising disinformation

The Code should strengthen commitments aimed at defunding the dissemination of disinformation on signatories' own services or on third-party websites[27]. To improve transparency and accountability around ad placements, signatories participating in ad placements, including ad-tech companies[28], should identify the criteria they use to place ads, and adopt measures that enable verification of the landing/destination place of ads, with the aim of avoiding the placement of advertising next to disinformation content or in places that are known for repeated publication of disinformation. Platforms should commit, in particular, to tighten eligibility requirements and content review processes for content monetisation and ad revenue share programmes on their services to bar participation by actors that systematically post content debunked as disinformation[29]. Furthermore, platforms should also commit to strengthen relevant policies and exercise due diligence with a view to excluding participation in the ad networks or ad exchanges of websites that persistently purvey disinformation content.

Commitments in this area should also build on and improve the availability and uptake of brand safety tools, which should integrate information and analysis from fact-checkers, researchers and other relevant stakeholders providing information e.g. on the sources of disinformation campaigns. Supported by such information and tools, brand owners and other advertisers should commit to do their utmost to avoid the placement of their

---

[26] JOIN (2018) 36 final.

[27] Evidence also shows that revenues from online advertisements still contribute significantly to the monetisation of disinformation websites, including advertising from large brands unwittingly placed next to disinformation content. For example, the Global Disinformation Index estimates that around $ 76 million dollars per year in ad revenues flow to disinformation sites targeting Europe: https://disinformationindex.org/2020/03/why-is-ad-tech-giving-millions-to-eu-disinformation-sites/.

[28] A limited number of ad-tech companies has already adopted such policies.

[29] See for instance Avaaz's 2020 Report, 'Why is YouTube Broadcasting Climate Misinformation to Millions?': https://secure.avaaz.org/campaign/en/youtube_climate_misinformation/.

advertising next to disinformation content or in places that repeatedly publish disinformation.

### 4.2 Improving cooperation between relevant players

Achieving tangible results requires the close cooperation of different players within the advertising ecosystem. To this end, as set out in Section 3.3, a broader participation of stakeholders from the advertising ecosystem is key. The strengthened Code should provide a framework for such widened participation strengthening the cooperation of all relevant actors and further facilitating ongoing cross-industry initiatives in this area[30].

As part of the strengthened Code, all actors involved in buying, selling and placing digital advertising should commit to exchange best practices and strengthen cooperation. Such cooperation should facilitate the integration and flow of information across the whole advertising value chain, in particular information relevant for identifying purveyors of disinformation in full respect of all relevant data protection rules.

Cross-platform cooperation could also include the exchange of information on disinformation ads refused by one platform to prevent their appearance on other platforms – for example, by the creation of a common repository of rejected ads – for awareness of other platforms whose services may also be affected.

Actions to defund disinformation should be broadened by the participation of players active in the online monetisation value chain, such as online e-payment services, e-commerce platforms and relevant crowd-funding/donation systems.

### 4.3 Commitments to address advertising containing disinformation

Under the strengthened Code, signatories should commit to design appropriate and tailored advertising policies that address the misuse of their advertising systems for propagating disinformation[31]. They should enforce these policies consistently and effectively. To this end, signatories should cooperate with fact-checkers to identify ads that contain disinformation which has been fact-checked and debunked. To ensure consistent implementation, signatories should commit to adapt their current ad verification and review systems to ensure that ads placed through or on their services comply with their advertising policies in respect of disinformation. Signatories should also commit to explain clearly to advertisers which advertising policies have been violated when they reject or remove disinformation ads or disable advertising accounts[32].

---

[30] The Global Alliance for Responsible Media, launched in June 2019 under the auspices of the World Federation of Advertisers (WFA), includes platform and advertising sector signatories of the Code, as well other notable stakeholders across the advertising ecosystem. It is developing a set of industry-wide common definitions and standards for how harmful content is categorised across platforms, approved by advertisers, and implemented by platforms in their advertising products and brand safety tools. Notably, the Alliance is pursuing a separate category for disinformation and misinformation to be included in the set. See WFA 'Interim Report on Activities related to the EU Code of Practice on Disinformation', September 2020, p. 2: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=69683

[31] Evidence shows the persistence of online ads containing disinformation that fact-checkers have identified and debunked. See 'Facebook Approved Ads With Coronavirus Misinformation': https://www.consumerreports.org/social-media/facebook-approved-ads-with-coronavirus-misinformation/.

[32] As the Commission has noted, platforms' policies pursue a range of objectives, some of which are not specifically tailored to tackle disinformation – e.g. unsupported commercial claims, deceptive business practices. See SWD (2020) 180 final.

## 5 POLITICAL ADVERTISING AND ISSUE-BASED ADVERTISING

'Political advertising' and 'issues based advertising'[33] play an important role in shaping political campaigns and public debates around key societal issues. Such online paid-for content can have a decisive role in forming the public opinion and influence the outcome of elections. The organisation of elections in the EU is largely regulated at Member State level, with various relevant rules affecting political advertising including their transparency. In EDAP, the Commission announced legislation to strengthen the transparency of political advertising. To ensure the adequate level of transparency and accountability in this area, the Code's commitments need further strengthening, in support of the wider legal framework.

The revision of the Code in this area will need to take into account the Commission's upcoming legislative proposal on the transparency of sponsored political content and the relevant provisions of the proposed DSA. A strengthened Code will serve as an important vehicle to deliver tangible progress to support the existing legal framework, as well as to pave the way towards strengthened legislation and through the new legislative framework once it is in place and to devise industry-led solutions to support its implementation and achieve continued progress in this area.

For a consistent and effective application of the commitments, a shared understanding among signatories of 'political advertising' and 'issue-based advertising' is needed which adequately takes into account the existing applicable national legal frameworks. The signatories should make sure that they comply with applicable laws and align their practices with the upcoming legislation on the transparency of sponsored political content.

### 5.1 Efficient labelling of political and issue based ads

The Code should include strengthened commitments ensuring the transparency and public disclosure of both political and issue-based ads, taking into account the relevant provisions in the proposed DSA[34], the upcoming legislative initiative on transparency of political advertising, and without prejudice to existing regulatory frameworks. These ads should be clearly and effectively labelled and distinguishable as paid-for content, and users should be able to understand that the content displayed contains advertising related to political or societal issues. The strengthened Code could include a set of common criteria and examples on the marking and labelling of political and issue-based ads. Where relevant, signatories should integrate relevant research to improve the effectiveness of labels in informing users[35]. The Code should include commitments aiming at ensuring that labels remain in place when users share political or issue-based ads in an organic way[36], so that they continue to be clearly identified as ads.

---

[33] While there is currently no common definition of issue-based ads in the Code, there seems to be agreement that issue-based ads are ads that include sponsored content on societal issues or related to a debate of general interest that might have an impact on public discourse. Examples of such issues include climate change, environmental issues, immigration or COVID-19.

[34] Article 24 in particular.

[35] Dobber et al.,'Effectiveness of online political ad disclosure labels: empirical findings', March 2021: https://www.uva-icds.net/wp-content/uploads/2021/03/Summary-transparency-discloures-experiment_update.pdf.

[36] Organic content is free content that users share with each other without paying for it. This also includes situations where users share with each other sponsored content which then becomes organic content.

### 5.2 Verification and transparency commitments for political and issue-based ads

Signatories who display political and issues-based ads should ensure that the identity of the advertiser is visible to users, including a specific commitment setting out transparency obligations in line with the requirements in the proposed DSA[37].

Signatories should also make reasonable efforts to ensure, through effective identity verification and authorisation systems, that all the necessary conditions are met before allowing the placement of these types of ads.

### 5.3 Transparency in messaging platforms

The revised Code of Practice should include new, tailored commitments addressing the use of messaging platforms for the dissemination of political and issue-based ads, in full respect of the General Data Protection Regulation (GDPR) and EU requirements for privacy in electronic communications services. The abovementioned requirement that when sponsored political content is shared between users, it should continue to be labelled as paid-for content, should also apply to the extent possible to sponsored political content shared over messaging platforms. To this end, signatories should develop solutions which are compatible with the encryption technology often used by messaging platforms, without any weakening of the encryption.

### 5.4 Targeting of political ads

Micro-targeting of political advertising may raise various concerns. It raises issues of compliance with data protection rules, as micro-targeting is based on personal information and sometimes includes sophisticated psychological profiling techniques[38]. It can affect the right of voters to receive information, since micro-targeting allows political advertisers to send tailored messages to targeted audiences, while other audiences may be deprived of this information. Micro-targeting makes it difficult to fact-check or scrutinise such ads, and for individuals to assert their rights, including as regards data protection. This in turn may increase the risk of political polarisation[39].

The strengthened Code should contribute to limit or avoid the risks associated with micro-targeting of individuals with political and/or issues-based advertising. In this regard, full compliance with the GDPR and other relevant laws should be ensured, in particular acquiring valid consent where required[40]. Access to information should be facilitated to enable the competent authorities to perform their monitoring and enforcement function.

---

[37] DSA proposal, Article 30.

[38] Specific transparency obligations are included in the DSA proposal as well as in the proposal for the Digital Markets Act.

[39] See, for instance, Papakyriakopoulos et. al, 'Social media and microtargeting: Political data processing and the consequences for Germany', Big Data & Society, November 2018, doi 10.1177/2053951718811844, or Lewandowsky et al., 'Understanding the influence of online technologies on political behaviour and decision-making', EUR 30422 EN, Publications Office of the European Union, Luxembourg.

[40] For more guidance, see the European Data Protection Board Guidelines 05/2020 on consent under Regulation 2016/679 and Guidelines 08/2020 on the targeting of social media users (providing examples on when consent is required for targeted advertising).

Signatories should commit to ensure that citizens are clearly informed when they are being micro-targeted and be given meaningful information on the criteria and data used for this purpose. They should implement strong related transparency measures, including dedicated searchable ad libraries with all micro-targeted ads served to specific user groups[41], accompanied by information on targeting and delivery criteria.

### 5.5 Improved ad repositories and minimum functionalities for the application programming interfaces (APIs)

The strengthened Code should ensure that signatory platforms commit to improve the completeness and quality of the information in their repositories of political ads, so that these effectively contain all sponsored political content served. These repositories should provide current, regularly updated information on the volume and budget of political ads served by political advertisers in the Member States, the number of times each ad has been displayed online, and the targeting criteria used by the advertiser, taking into account the relevant provisions in the proposed DSA and the upcoming legislative proposal on political advertising[42].

Some platforms have developed application programming interfaces (APIs) or other interfaces enabling users and researchers to perform customised searches within their political ad repositories. However, the functionalities of these APIs are very limited. The strengthened Code should ensure that APIs for platforms' political ads repositories include a set of minimum functionalities, as well as a set of minimum search criteria that enable users and researchers to perform customised searches to retrieve real-time data in standard formats and allow for easier cross-platform comparison, research and monitoring. If repositories for issue-based ads are established, they should have comparable API functionalities and search capabilities. Commitments should also ensure wide access to APIs and that functionalities of the APIs are regularly updated to meet researchers' needs.

## 6 INTEGRITY OF SERVICES

The strengthened Code should provide for comprehensive coverage of current and emerging forms of manipulative behaviour used to spread disinformation. It should take account of the evolving nature of and the broader risks associated with the spread of disinformation, for example the fact that disinformation campaigns can be part of hybrid threats to security, in particular in combination with cyberattacks[43]. It should include tailored commitments to address vulnerabilities and ensure transparency and accountability regarding actions that signatories take to limit manipulative behaviour which, according to their relevant terms of service, are not permitted on signatories' services, also in view of the upcoming regulatory requirements set out in the proposed DSA[44].

---

[41] For instance, ad libraries, if equipped with the necessary data, can be used to verify online equal time exposure to political messages.
[42] See DSA proposal, Article 30.
[43] Joint Communication on Increasing resilience and bolstering capabilities to address hybrid threats (JOIN (2018) 16 final)
[44] Article 26(1) point c of the DSA proposal identifies the 'intentional manipulation' of services as a systemic risk, against which very large platforms must take risk mitigation measures.

### 6.1 Common understanding of impermissible manipulative behaviour

To ensure a consistent approach, the strengthened Code should ensure that signatories agree on a cross-service understanding of manipulative behaviour not permitted on their services, including 'inauthentic behaviour', without prejudice to existing EU and national laws. That understanding should be wide enough to cover the full range of behaviours through which malicious actors may attempt to manipulate services. To this end, signatories should draw up a comprehensive list of manipulative tactics, techniques and procedures (TTPs) that constitute impermissible inauthentic behaviour across their services. The techniques identified should be sufficiently defined to enable comparisons of the prevalence of impermissible behaviours across platforms, as well as the effectiveness of actions taken to counter them. The common understanding should provide a shared vocabulary for signatories, regulators, civil society and other stakeholders to discuss problems of online disinformation and manipulation both in the context of the Code of Practice and in other fora, such as the EU Rapid Alert System and Elections Cooperation Network, and in preparation of the application of the proposed DSA. This work should take into account the rapidly developing situation regarding the TTPs and reflect these possible changes when developing terminology and definitions.

### 6.2 Strengthened commitments to limit impermissible manipulative behaviour

The strengthened Code should set out new commitments in the area of impermissible manipulative behaviour, covering the full range of manipulative techniques and requiring effective responses to counter them. The commitments should require signatories to address evolving manipulative techniques, such as hack-and-leak operations, account takeovers, the creation of inauthentic groups, impersonation, deepfakes, the purchase of fake engagements or the opaque involvement of influencers. Furthermore, the commitments should not only require signatories to publish relevant policies, but should also lay down baseline elements, objectives, and benchmarks for measures deployed to counter impermissible manipulative behaviours. The strengthened Code should take into consideration the transparency obligations for AI systems that generate or manipulate content and the list of manipulative practices prohibited under the proposal for Artificial Intelligence Act[45].

### 6.3 Adjusting commitments, cooperation and transparency

To ensure its continuing relevance and adequacy, the strengthened Code should establish a mechanism through which its commitments can be adjusted over time based on the latest evidence on the conducts and TTPs employed by malicious actors.

Signatories should commit to set up channels of exchange between their respective trust, cybersecurity and safety teams. These channels of exchange should facilitate the proactive sharing of information about influence operations and foreign interference in information space on the signatories' services to prevent the resurgence of such campaigns on other platforms. Results and lessons learned should be included in the

[45] COM (2021) 206 final.

signatories' yearly monitoring reports, discussed in the permanent task-force[46], and be made available on a regular basis in common data formats[47].

Commitments shall ensure that all policies and measures are clearly communicated to the users, including via the transparency centre[48]. Signatories should also commit to make all actions against impermissible manipulative behaviour subject to an internal complaint handling system, taking into consideration the relevant provisions in the proposed DSA[49].

## 7 EMPOWERING USERS

Empowering users is key to limiting the impact of disinformation. A better understanding of the functioning of online services, as well as tools that foster more responsible behaviour online or that enable users to detect and report false and/or misleading content, can dramatically limit the spread of disinformation. The Code's commitments in this area should be widened to cover a broad range of services, including for example tailored commitments for messaging services. They should also include mechanisms to appeal against actions taken by signatories as follow-up to users' reports. Signatories should also specifically consider the situation of children who can be particularly vulnerable to disinformation.

### 7.1 Commitment to measures enhancing media literacy

Several signatories have made efforts in the area of media literacy providing users with relevant tools. Under the strengthened Code, signatories should commit to continue these efforts and commit in particular to a stronger involvement of the media literacy community in the design and implementation of tools and assessment of media literacy campaigns on their services, including to protect children. These efforts could also be aligned with the Commission's initiatives in the area of media literacy[50], including the new Digital Education Action Plan (2021-2027)[51], to exploit relevant synergies. To this end, the Commission's Media Literacy Expert Group[52] and EDMO can provide support to establish a permanent framework for discussion.

### 7.2 Commitment to 'safe design'

The design and architecture of online services have a significant impact on the behaviour of users[53]. Signatories should therefore commit to assess the risks their systems pose and design the architecture of their services in a way that it minimises risks linked[54] to the

---

[46] Regarding the Permanent Task Force, see Section 9.2.3 further below.
[47] This should also take into account the AMITT (Adversarial Misinformation and Influence Tactics and Techniques) Framework: https://cogsec-collab.org/
[48] Regarding the Transparency Centre, see Section 9.2.2 further below.
[49] Notably Article 17, which already applies to decisions incompatible with their terms and conditions, including decisions to remove or disable access to content, do suspend or terminate the provision of the service in whole or in part to the recipient or decisions to suspend or terminate the recipient's account.
[50] See in particular the actions set out in the European Democracy Action Plan, (COM (2020) 790 final) and the Media and Audiovisual Action Plan (COM (2020) 784 final).
[51] The Digital Education Action Plan (COM (2020)624 final) puts forward a proposal to develop guidelines for teachers and educators in view of tackling disinformation and promoting digital literacy through education and training.
[52] https://digital-strategy.ec.europa.eu/en/policies/media-literacy
[53] See e.g. Lewandowsky et al., 'Understanding the influence of online technologies on political behaviour and decision-making', EUR 30422 EN, Publications Office of the European Union, Luxembourg, 2020.
[54] See DSA proposal, Article 26(1) point c on related risk assessment.

spread and amplification of disinformation[55]. This could also include pre-testing of the systems' architecture. Signatories should also invest in research and develop product features and designs that enhance users' critical thinking as well as the responsible and safe use of their services.

Online platforms could also work together with providers of technological solutions to integrate in their services solutions which allow to check authenticity or accuracy or to identify the provenance or source of digital content[56].

The providers of AI-enabled online systems also should take into consideration the relevant provisions in the proposed Artificial Intelligence Act.

### 7.3 Accountability of recommender systems

By determining the order in which information is presented, recommender systems have a significant impact on what information is actually accessed by users. It is of paramount importance that signatories under the strengthened Code commit to make their recommender systems transparent regarding the criteria used for prioritising or de-prioritising information, with the option for users to customise the ranking algorithms. All this should be done with due regard to the principle of media freedom taking into account the requirements in the relevant provisions of the DSA proposal[57].

Commitments should also include concrete measures to mitigate risks of recommender systems fuelling the viral spread of disinformation, such as the exclusion from the recommended content of false and/or misleading information where it has been debunked by independent fact-checkers and of webpages, and actors that persistently spread disinformation.

### 7.4 Visibility of reliable information of public interest

The COVID-19 pandemic has underlined the importance, in particular in times of crisis, of promoting information of public interest that is reliable, such as information provided by health authorities related to measures preventing the disease or to the safety of vaccines[58]. Signatories implemented various solutions to provide users with such information and make it visible and easy to access. Building on this experience, signatories to the strengthened Code should commit to further develop and apply such

---

[55] Simple technical interventions (for example, pop-up messages asking users if they really wish to share links that they have not viewed) can prompt users to scrutinise the content before they disseminate it and thus help limit the spread of false and/or misleading information by users acting in good faith. Examples: 'Check it out before you Tweet it' prompt implemented by Twitter: https://help.twitter.com/en/using-twitter/how-to-retweet;
YouTube fact-check information panels: https://support.google.com/youtube/answer/9229632?hl=en; Facebook pop-up notice before sharing content debunked by a fact-checker: https://www.facebook.com/journalismproject/programs/third-party-fact-checking/faqs;
TikTok 'Know your Facts tool': https://newsroom.tiktok.com/en-gb/taking-action-against-covid-19-vaccine-misinformation.

[56] In Section 3.3, the Guidance invites stakeholders that can make a contribution through their tools, instruments or solutions contributing to the fight against disinformation, to become new signatories of the Code.

[57] Notably, Articles 26, 27 and 29.

[58] COVID-19 monitoring reports provide data regarding views or click-through rates of information panels and banners providing such information: https://digital-strategy.ec.europa.eu/en/library/reports-march-actions-fighting-covid-19-disinformation-monitoring-programme

specific tools (e.g. information panels, banners, pop-ups, maps and prompts) that prioritise and lead users to authoritative sources on topics of particular public and societal interest or in crisis situations.

To deepen the existing Code's commitment[59] on the prioritisation of relevant, authentic and authoritative content, signatories should also commit to publishing information outlining the methodology their recommender systems employ in this regard. This information should be included in the transparency centre. The Code's signatories should consider ensuring that this information can be verified by third parties or through an independent audit, taking into consideration also the relevant provisions in the DSA proposal.

### 7.5 Warnings issued to users that interact or have interacted with false or misleading content

The debunking of false and/or misleading information is crucial to curbing the disinformation phenomena[60]. Several signatories have established cooperation with independent fact-checkers and/or have created in-house moderation teams to provide labels for false or misleading content. However, the Code currently does not include relevant commitments. Accordingly – complementing new commitments to ensure the consistent application of fact-checking, as discussed below in Section 8.3 – signatories should commit to provide, for all EU languages in which their service is provided, systems for the regular and consistent labelling of content identified as false or misleading and for issuing targeted warnings to users that have interacted with such content. Signatories should commit to inform users why particular content or accounts have been labelled, demoted or otherwise affected by measures taken, as well as the basis for such action. Signatories should commit to design their labelling and warning systems in accordance with up-to-date scientific evidence on how to maximise the impact of such interventions, ensuring in particular that they are designed to capture users' attention[61].

### 7.6 Functionality to flag harmful false information

Although some signatories already provide a dedicated functionality for users to flag false and/or misleading information, this feature is not yet available on all services. The strengthened Code should contain a dedicated commitment requiring relevant signatories to offer user-friendly, effective procedures on their services, enabling users to flag disinformation with the potential to cause public or individual harm. This functionality should also support labelling systems and mechanisms to help the identification of resurging false information content already labelled as false in other languages or on other services, with full respect for the freedom of expression. The commitment should specify that the functionality needs to be duly protected from abuse (i.e. the tactic of 'mass-flagging' to silence other voices) and available in all EU Member State languages in which their services are provided. Actions taken by signatories on flagged content should respect the freedom of expression and not be disproportionate. Measures in this area could include applying a transparent fact-checking procedure to the flagged content with subsequent follow-up actions, such as labelling the content where relevant. Signatories should commit to provide users with follow-up information about reported

[59] See commitment 8 of the Code of Practice on Disinformation.
[60] The Debunking Handbook 2020: https://sks.to/db2020.
[61] Optimisations can for instance relate to the visual design, the point in time or the graphical presentation of the intervention.

content, such as whether the content was reviewed and, if so, the results of the assessment and any action taken with respect to the content. Users whose content or accounts have been subject to such measures should likewise be informed to understand the reasons behind the actions taken and have access to an appropriate and transparent mechanism to appeal and seek redress against the measures applied.

### 7.7 Availability of indicators for informed online navigation

It is not an aim of the strengthened Code to evaluate the veracity of editorial content. However, given the abundance of information available online, users face challenges regarding which information sources to consult and trust. Indicators of trustworthiness, focused on the integrity of the source, developed by independent third parties, in collaboration with the news media, including associations of journalists and media freedom organisations, as well as fact-checkers, can support users in making informed choices[62].

Signatories could facilitate access to such indicators providing users with the choice to use them on their services. In this case, the strengthened Code should ensure that signatories provide transparency regarding such third-party indicators, including about their methodology.

The implementation of such trustworthiness indicators should be fully in line with the principles of media freedom and pluralism. To this end, it should be left for the users to decide if they want to use such tools[63].

### 7.8 Measures to curb disinformation on messaging apps

In addition to recent initiatives developed in cooperation with fact-checkers[64], signatories that provide private messaging applications should test and implement technical features helping users to identify disinformation disseminated through such services. Such solutions should be compatible with the nature of these services and in particular the right to private communications, without any weakening of the encryption. Such features could, for example, help users to verify whether particular content they receive has been fact-checked as false. This could be achieved e.g. through solutions that make visible fact-checking labels when content from social media is disseminated over a messaging app. Signatories could also consider solutions that enable users to check content they received over a messaging application against a repository of fact-checks.

## 8 EMPOWERING THE RESEARCH AND FACT-CHECKING COMMUNITY

In view of their key contribution to an effective strategy for tackling disinformation, the strengthened Code should set out a framework for robust access to platform data by the research and fact-checking community and adequate support for their activities.

---

[62] Examples of such indicators can be the Global Disinformation Index (GDI), the Journalism Trust Initiative (JTI) or the Trust Project, as well as the service NewsGuard.

[63] Tools for assessing the trustworthiness of information sources, such as so-called trust marks, should be made available to users to consult if they so wish. Users could also be given the option of having signals relating to the trustworthiness of media sources fed into the automated systems that select and rank content appearing in their user feeds.

[64] Fact-checking organisations, supported by some providers of messaging applications, give users of messenger apps the possibility to have messages they received via such private channels fact-checked: https://faq.whatsapp.com/general/ifcn-fact-checking-organizations-on-whatsapp/?lang=en

### 8.1 Access to signatories' data for research on disinformation

By offering evidence-based analysis, researchers are essential to the proper understanding of the evolution of the risks linked to disinformation[65] and can contribute to the development of risk mitigation mechanisms. This work critically depends on access to platform data. The proposed DSA provides a regulatory mechanism for vetted researchers to have access to data for research on the risks stemming from platforms' services[66]. The strengthened Code should create a framework that, already in the interim before the DSA's adoption, allows researchers the necessary access to platform data and also facilitates in the long term the development of a specific framework for data access tailored for conducting research on the disinformation phenomena.

#### 8.1.1 General framework for access to data

For the strengthened Code, relevant signatories, in particular platforms, should commit to co-creating a robust framework for access to data for research purposes. The conditions for access should be transparent, open and non-discriminatory, proportionate and justified. Where personal data are concerned, the conditions have to be GDPR compliant. In general, access conditions to any data should respect the right to private communications and appropriately protect the rights and legitimate interests of all concerned parties.

Signatories should develop the framework in cooperation with the research community, EDMO and relevant national authorities. Commitments should include a detailed timeline for the progress expected in the design and implementation of the framework.

The framework should contemplate different access to data regimes with appropriate safeguards for i) anonymised and non-personal data and for ii) data requiring additional scrutiny, including personal data. The framework should provide for the possibility of real-time access to certain types of data, in order to enable the prompt assessment of emerging or evolving risks and the design of appropriate mitigation measures.

While the framework is in development, signatories should pilot temporary solutions. For example, the use of 'sandboxes' could provide access to relevant platform data for research on specific topics for a limited number of researchers informing the design of the framework and test operational solutions for wider access to data across platforms.

#### 8.1.2 Access to anonymised and non-personal data

The strengthened Code should include a commitment to provide, wherever practicable, continuous, real-time, stable and harmonised access to anonymised, aggregate or otherwise non-personal data for research purposes through APIs or other open and accessible technical solutions allowing full exploitation of the datasets.

Access to data solutions should facilitate the search and analysis of the data. Relevant signatories should ensure that the functionalities of access systems meet researchers' needs and are interoperable. Commitments should ensure procedures for reporting the

[65] This is as well crucial for informing signatories, the Commission, the competent national authorities and the public.
[66] Article 31 in particular.

malfunctioning of access systems, and for restoring access and repairing faulty functionalities in a reasonable time.

### 8.1.3 Access to data requiring additional scrutiny, including personal data

Data which might expose personal information, including sensitive one[67], require additional security and safeguards. Confidential information, in particular trade secrets, or data linked to the security of the platforms' services also deserves appropriate protection. At the same time, the framework for access to data should at least allow academic researchers to have access to datasets necessary to understand sources, vectors, methods and propagation patterns that characterise the disinformation phenomenon.

To this end, the Code should set up a transparent procedure involving all relevant stakeholders, in particular, platforms and the research community, to define the conditions applicable for access to these datasets. In principle, the conditions should be standardised and uniform across platforms. The procedure should regulate *inter alia* (i) the minimum standards and qualification for researchers to whom access will be granted, (ii) the minimum categories of data that will be made available, (iii) the technical and organisational security measures to be observed in the processing of such data, including purpose limitation and data minimisation; and (iv) in respect of pseudonymised data, any measures necessary to prevent reattribution[68].

### 8.1.4 Role of EDMO

In view of its independence and its coordination functions, EDMO could provide support in the area of access to data, including guidance on *inter alia* the categories of data to be made available, the purposes for which data may be processed, and appropriate security measures for the processing of personal data and for preventing the reattribution of anonymised data.

Facilitated by EDMO, work is being undertaken to explore the possibilities of a code of conduct under Article 40 of the GDPR aimed at ensuring the proper application of privacy and data protection requirements to the sharing of personal data by platforms with researchers. The GDPR provides general conditions of processing of personal data also in the form of sharing of personal data by platforms with researchers. Such a code would reduce legal uncertainties and risks for platforms providing access to data and ensure a secure and harmonised environment for processing of personal data for research purposes[69]. The strengthened Code should commit signatories to facilitate, as necessary, the development of the code of conduct under Article 40 of the GDPR.

### 8.1.5 Access to data for other stakeholders

Other stakeholders, such as civil society organisations, non-academic research centres and investigative journalists, also play important roles in the detection and analysis of disinformation campaigns, the formulation of policy responses, as well as the promotion

---

[67] In the sense of Article 9 of GDPR.
[68] As required by GDPR, when it comes to the personal data their disclosure needs to be based on a clear legal basis with appropriate safeguards, including the regime of Article 9 for the special categories of data.
[69] The stakeholder discussion showed support from the Code's signatories and the research community to this initiative: https://digital-strategy.ec.europa.eu/en/library/summary-multi-stakeholder-discussions-preparation-guidance-strengthen-code-practice-disinformation.

of public awareness and social resilience. The signatories of the Code should allow, in particular in Member States where there is not adequate academic capacity, for a sufficient level of access for such stakeholders consistent with privacy requirements and subject to reinforced control against misuses of personal data and the reattribution of pseudonymised data.

### 8.2 Framework of cooperation between signatories and researchers

To foster and empower a larger multi-disciplinary community of independent researchers, the Code should establish a framework for transparent, open, and non-discriminatory cooperation between signatories and the EU research community regarding resources and support made available to researchers. This framework should allow the research community to independently manage the funds made available by signatories for research on disinformation, defining scientific priorities and transparent allocation procedures based on scientific merit. In this regard, EDMO could assist in the allocation of such resources.

### 8.3 Collaboration with fact-checkers

Fact-checkers are important players in addressing the disinformation phenomenon[70]. They assess and verify content based on facts, evidence and contextual information, and raise user awareness about disinformation online. The strengthened Code should foresee strengthened support to their work and increase the coverage of fact-checking activities across EU Member States and languages.

#### 8.3.1 Forms of cooperation

In view of the significant gaps and uneven application of fact-checking activities across services and Member States[71], platform signatories should commit to concrete steps, with clear targets and timelines, to extend their cooperation with fact-checkers to ensure the consistent application of fact-checking in their services. Efforts should focus, in particular, on Member States and languages where fact-checking is not yet provided [72].

This could be achieved through multilateral agreements between platforms and independent fact-checking organisations that meet high ethical and professional standards. Such agreements should be based on transparent, open and non-discriminatory conditions, and ensure the independence of fact-checkers. The agreements should provide for fair remuneration to fact-checkers for work used by the platforms, foster cross-border cooperation between fact-checkers, and facilitate the flow of fact-checks across signatories' services.

In view of its role in fostering joint fact-checking activities, EDMO is well-suited to support platforms and fact-checkers in developing a framework for collaboration,

---

[70] Fact-checking organisations regularly publish nonpartisan reports on the accuracy of statements by public figures and major institutions and other widely circulated claims of interest to society. They are independent and follow strict ethical and transparency rules such the one defined by the International Fact-Checking Network (IFCN) (https://www.poynter.org/international-fact-checking-network-fact-checkers-code-principles).

[71] https://www.disinfo.eu/publications/bulgaria%3A-the-wild-wild-east-of-vaccine-disinformation/

[72] EDMO fact-checking activities map in the EU: https://edmo.eu/fact-checking-activities/

including the creation of a common interface for fact-checkers, the exchange of information between fact-checkers, and the promotion of cross-border cooperation.[73]

### 8.3.2 Use and integration of fact-checking in signatories' services

The strengthened Code should include commitments requiring more consistent use and integration of fact-checkers' work in platforms' services, including in programmatic advertising systems and in video content. Platforms should commit to employ mechanisms enabling the prompt and consistent incorporation of fact-checks into their services upon notification by fact-checkers, including swift and efficient labelling. Relevant signatories should facilitate the creation of a common repository of fact-checking articles (fact-checks) produced by fact-checkers and explore technological solutions to facilitate its efficient use across platforms and languages to prevent the resurgence of disinformation that has been debunked by fact-checkers[74].

### 8.3.3 Fact-checkers' access to relevant information

To maximise the quality and impact of fact-checking, the strengthened Code should ensure that platform signatories commit to provide fact-checkers with automated access to information on the actions they have taken with respect to fact-checked content and the fact checks. The information should quantify (i) user interactions over time (e.g. number of views, like, shares, comments before and after the fact-check)[75] with content which has been fact-checked, and (ii) the reach of the fact-check over time in the online services where they were published. Platforms and fact-checkers should agree on a common interface for fact-checking in order to ensure consistency in the way the platforms use, credit and provide feedback on the work of fact-checkers. Moreover, the Code should foresee regular exchange of information between relevant Code signatories and the fact-checking community aimed at further strengthening cooperation.

## 9 MONITORING OF THE CODE

The strengthened Code should be complemented with a robust monitoring system, building on the Commission's experience to date in monitoring the Code, including the COVID-19 programme. The improved monitoring system should provide for the regular assessment of the signatories' implementation of the Code commitments, spur improvements in their policies and actions, and enable evaluation of the Code's effectiveness as a tool for tackling disinformation. The improved monitoring system should reinforce the accountability of online platforms in the interim before the DSA's adoption, and provide a framework *inter alia* for structured dialogue with very large platforms on the development and deployment of risk assessment and mitigation measures, in anticipation of the legal obligations foreseen for them in the proposed DSA.

In view of these objectives, the Code's existing commitments on monitoring should be reinforced and extended to create a robust framework that incorporates the cornerstone

---

[73] To further support the work of European fact-checkers, their cooperation and the development of commonly agreed professional standards, the pilot project "Integrity of social media" will support the drafting of a Code for professional integrity for European fact-checkers in cooperation with EDMO. See: annual work programme, adopted under Commission Decision C (2020) 2259.

[74] Regarding the creation of a repository of fact-checks, signatories could seek synergies with EDMO.

[75] This should include also anonymised demographics and localisation of those sharing/receiving fact-checked content.

elements set out below. The strengthened Code should ensure in particular that signatories provide the information and data for the monitoring in standardised formats, with Member States breakdowns and on a timely basis.

### 9.1 Key Performance Indicators

The monitoring of the Code should be grounded on KPIs capable of measuring the implementation and effectiveness of the Code's commitments and the Code's impact on the disinformation phenomenon. To this end, two classes of KPIs are pertinent: (i) service-level indicators, which measure the results and impact of the policies implemented by signatories to fulfil their commitments under the Code, and (ii) structural indicators, which measure the overall impact of the Code on disinformation in the EU.

#### 9.1.1 Service-level indicators

Under the revised Code, signatories should commit to the formulation of concrete service-level indicators. Service-level indicators should effectively measure the implementation of the Code's commitments and the impact of signatories' policies. The indicators should be sufficiently flexible to cater to the different nature of the signatories' services while allowing for consistent reporting and comparisons across services.

The strengthened Code should require that signatories identify, report on and commit to a minimum set of qualitative and quantitative indicators aimed at evaluating *inter alia*:

- The impact of tools and features put in place to enhance user awareness and user empowerment, including user interactions with such tools and features[76].
- The impact of tools and features that display or make more visible reliable information of public interest, including user interactions with such tools and features[77].
- The number of fact checks, the percentage of fact-checked content versus content flagged by users, and funding provided for fact-checking activities.
- The impact of fact-checking activities and user interactions with information fact-checked as false or misleading[78].
- The number of appeals in relation to actions taken on content by platforms as a result of flagging of disinformation and information regarding their outcome.
- The number of pages, accounts, profiles and groups sharing disinformation subject to actions reducing their visibility[79] and the amount of such content shared.

---

[76] Impact could be measured through indicators quantifying the level of interaction (e.g. views, click-through rates, shares, etc.) of users with such tools and qualifying users' perception regarding the usefulness of such tools. Also, indicators should include data on the use of tools for flagging and reporting content perceived as false.

[77] Impact could be measured through indicators quantifying the level of interaction (e.g. views, impressions, click-through rates, shares, etc.) of users with such tools and qualifying users' perception regarding the usefulness of such tools.

[78] Impact could be measured through indicators quantifying the level of interaction (e.g. views, click-through rates, shares) with pieces of content before and after they are labelled or demoted for being fact checked as false. Other indicators could also give information on how users' interactions occur.

- The impact of identified impermissible manipulative behaviour, including instances of content or accounts removed or demoted[80].
- The number of partnerships between the Code's signatories' from the ad industry and third-party entities assessing the quality of information sources.
- The impact of measures employed for the scrutiny of ad placements[81].
- The quantity and granularity of data made available to research purposes and the number of European research organisations having access to platforms' data.
- The amount of resources made available by signatories for research on disinformation and the number of European research organisations having access to such resources.
- Information regarding the human workforce involved in fulfilling the Code's commitments[82].

### 9.1.2 Structural indicators

Signatories of the Code also should commit to contribute to the development of structural indicators that can effectively measure the overall impact of the Code on the disinformation phenomenon. As further described below, signatories should set up a permanent task-force whose duties will include developing, testing and adjusting structural indicators.

Structural indicators could, for example, be based on representative samples of users in various Member States aimed at gauging the prevalence of persistent purveyors of disinformation[83] in the online media diets of European citizens[84]. Such indicators could measure public engagement with information sources, as well as regular, standardised surveys to measure the exposure of citizens to disinformation.

Until a more stable set of structural indicators is developed, signatories and stakeholders should agree upon a minimum viable set of structural indicators that can be rapidly implemented and tested, working towards developing a stable set of effective structural indicators.

## 9.2 Monitoring framework

The monitoring framework should allow the regular assessment of the signatories' implementation of Code commitments, including changes and evolutions of pertinent

---

[79] Including measures such as down ranking content, as well as closing profiles and groups.
[80] Impact could be measured through indicators quantifying the level of interaction (e.g. views, click-through rates, shares, etc.) with content, accounts and instances before they were removed and before and after they were demoted.
[81] Impact could be measured through indicators quantifying the number of ad placements displayed on websites identified as persistently purveying disinformation and the number of ads containing disinformation that were removed.
[82] This includes the number of staff employed to carry out activities to counter disinformation and the languages covered by their activities.
[83] The identification of online purveyors of disinformation should be based on a clear and agreed methodology defined by a wider set of stakeholders, including academic researchers, fact-checkers, NGOs and civil society organisations.
[84] The measuring mechanism for structural indicators could draw inspiration from what it is done by the audiovisual sector to measure audiences.

policies and actions. To this end, the signatories should report regularly to the Commission on the implementation of their commitments, including relevant KPIs.

Following the positive experience of the monitoring programmes during the 2019 EU elections[85] and the COVID-19 pandemic, the Commission will rely on the support of the European Regulators Group for Audiovisual Media Services (ERGA) on monitoring the implementation of the Code at Member State level. EDMO and its hubs should also support the Commission in analysing information and data reported by the signatories and in assessing the impact of the Code at national and EU level.

Taking into account the expert advice and support from ERGA and EDMO, the Commission will regularly assess the progress made in the implementation of the Code, as well as the impact of the Code on the disinformation phenomenon and publish its conclusions. The Commission may also provide further guidance on how signatories should address remaining shortcomings and gaps in the Code.

### 9.2.1 Regular reporting

Reporting obligations under the strengthened Code should take into account the size of signatories and the type of services they provide. Providers of online services that are widely used at EU level and have higher risk profiles with respect to the spread of disinformation should report every six months on the implementation of the commitments they have subscribed to and should provide corresponding service-level indicators. They should also, on a yearly basis, assess the risks linked to the disinformation phenomenon. Other Code signatories should report yearly and provide data corresponding to their activities. Signatories that provide tools, instruments or solutions to fight against disinformation, or that support the Code through the provision of expertise, should also report on their activities and findings that are relevant for the implementation and effectiveness of the Code on a yearly basis. The reporting should be carried out in accordance with a defined schedule that sets out coverage periods and submission deadlines. Data used to measure the KPIs should include breakdowns at Member State level.

The reporting should be based on a harmonised template that allows, to the extent practicable, cross-platform comparisons. Moreover, signatories should agree on a set of standard and auditable formats for providing data related to the KPIs. These formats should be co-developed with relevant stakeholders from the permanent task-force and should meet standards and employ methods of the research and fact-checking community. Eventually, these formats should enable the continuous updating of a public dashboard made available through the transparency centre, as described below.

### 9.2.2 Transparency centre

To enhance transparency and accountability around the implementation of the Code, signatories should commit to create and maintain a publicly accessible transparency centre. Signatories should indicate in the transparency centre the specific policies they adopted to implement each Code commitment they have subscribed to and provide basic information about how these policies are enforced, including geographical and language coverage. It should also feature a public dashboard displaying relevant KPIs. The

[85] https://erga-online.eu/wp-content/uploads/2020/05/ERGA-2019-report-published-2020-LQ.pdf

transparency centre should be designed, in particular, with a view to enabling cross-service comparisons of the signatories' progress in implementing Code commitments and achieving measurable impacts in the fight against disinformation. Signatories should commit to keep the transparency centre regularly updated and disclose any changes to relevant policies no later than 30 days after a change is announced or implemented.

### 9.2.3 Permanent task-force

The strengthened Code should set up a permanent task-force aimed at evolving and adapting the Code in view of technological, societal, market, and legislative developments. The task-force should include Code's signatories and representatives from EDMO, ERGA and could invite relevant experts to support its work. The task force should be chaired by the Commission and include representatives of the European External Action Service. In line with the overall objective of providing input for the review and adaptation of the Code, the activities of the task force should include *inter alia*:

- Establishing a risk assessment methodology and a rapid response system to be used in special situations like elections or crises.
- Reviewing the quality and effectiveness of the harmonised reporting template, as well as the formats and methods of data disclosure for monitoring purposes.
- Optimising the quality and precision of data to be provided for the measurement of the indicators.
- Contributing to the assessment of the quality and effectiveness of service-level indicators and their relevant adaptation.
- Developing, testing and adjusting structural indicators and designing mechanisms to measure them at Member State level.
- Providing expert input and up-to-date evidence relevant to the Code's commitments, such as *inter alia* new forms of inauthentic behaviour.

## 10 CONCLUSION AND NEXT STEPS

This Guidance sets out key elements that are required, in the Commission's view, to transform the Code into a stronger instrument for addressing disinformation and creating a safer and more transparent online environment.

The Commission calls upon the signatories of the Code to convene and carry out the strengthening of the Code, in line with this Guidance. The Commission invites the signatories to provide a first draft of the revised Code in the autumn to allow for a proper discussion. It also invites potential new signatories to join the Code and take part in its revision, including established and emerging platforms, corporate actors and other participants in the online advertising sector, as well as other stakeholders that can contribute resources or expertise to the Code's effective functioning.

Since disinformation is a borderless phenomenon and in order to strengthen the real impact of the Code of Practice, actions in the European neighbourhood would be useful, such as work with civil society, cooperation with media professionals and media literacy initiatives.